ID: 356833
Sample Name:
SecuriteInfo.com.Trojan.Siggen12.2497.1023.964
Cookbook: default.jbs
Time: 17:33:21
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

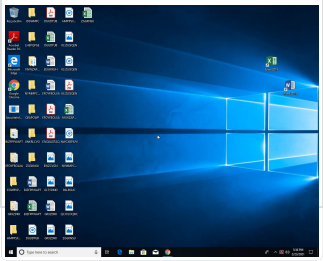
Analysis Report SecuriteInfo.com.Trojan.Siggen12.2497…

Overview

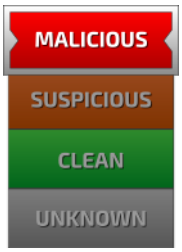
General Information

Sample Name:	SecuriteInfo.com.Trojan.Siggen12.2497.1023.964 (renamed file extension from 964 to exe)
Analysis ID:	356833
MD5:	9e74c1841ab5ec..
SHA1:	d37d7026c09dc6..
SHA256:	d367eca88434cb..
Infos:	

Most interesting Screenshot:



Detection

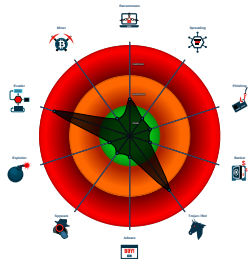


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Multi AV Scanner detection for subm…
- Binary contains a suspicious time st…
- Connects to a pastebin service (like…
- Hides threads from debuggers
- Machine Learning detection for samp…
- May check the online IP address of …
- PE file contains section with special…
- Query firmware table information (lik…
- Tries to detect sandboxes / dynamic…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe (PID: 4196 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe' MD5: 9E74C1841AB5EC50DD43819AABA20C0B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

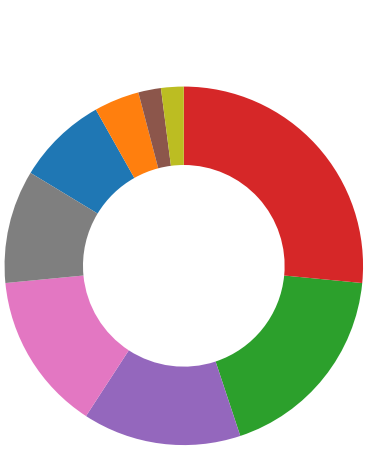
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses insecure TLS / SSL version for HTTPS connection

Binary contains paths to debug symbols

Networking:

Connects to a pastebin service (likely for C&C)

May check the online IP address of the machine

System Summary:

PE file contains section with special chars

Data Obfuscation:

Detected unpacking (changes PE section rights)

Binary contains a suspicious time stamp

Malware Analysis System Evasion:

Query firmware table information (likely to detect VMs)

Tries to detect sandboxes / dynamic malware analysis system (registry check)

Anti Debugging:

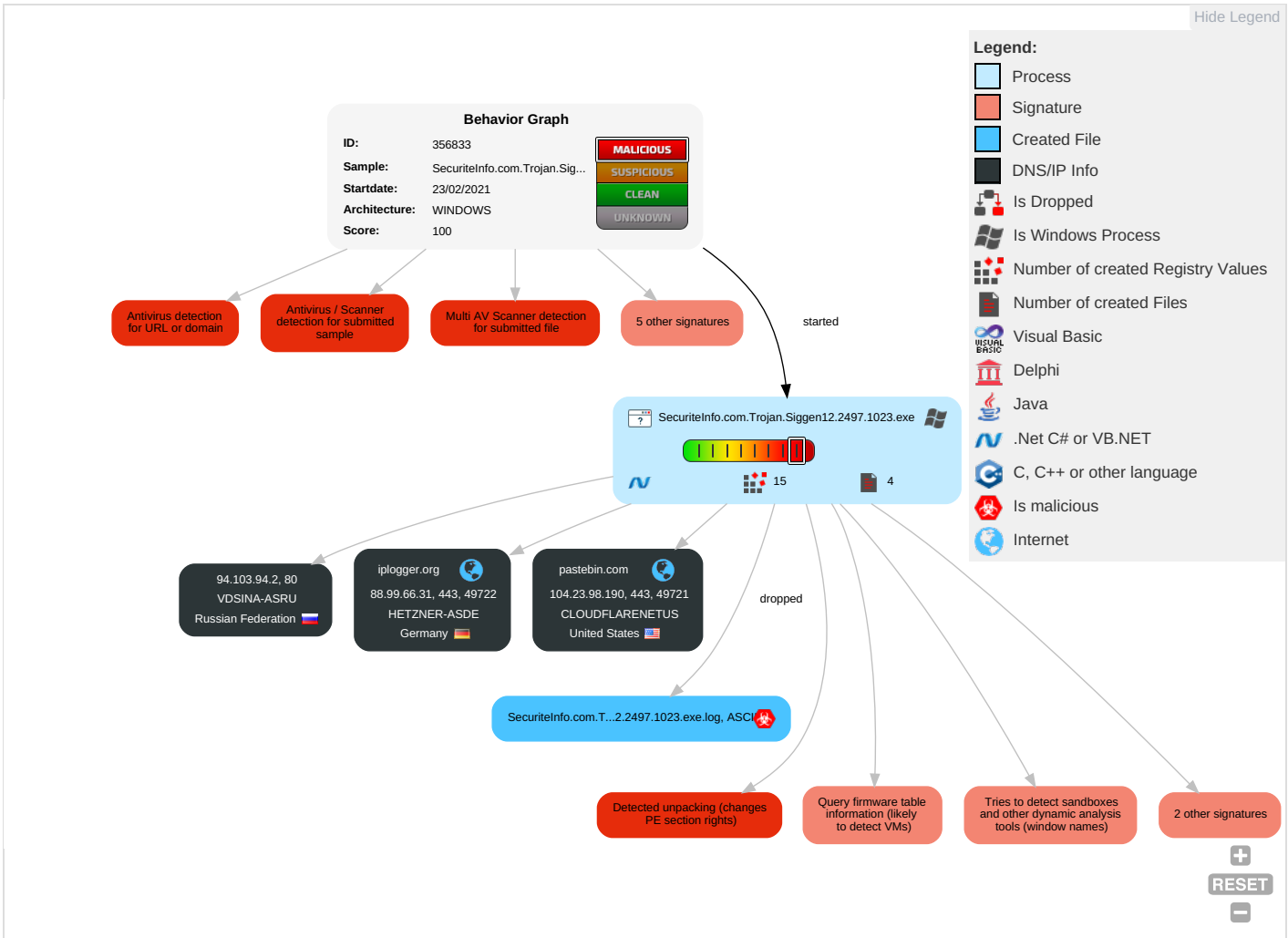
Hides threads from debuggers

Tries to detect sandboxes and other dynamic analysis tools (window names)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	Security Software Discovery 4 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Web Service 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3 4	LSASS Memory	Virtualization/Sandbox Evasion 3 4	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 1 2	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Remote System Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	System Network Configuration Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 1	LSA Secrets	System Information Discovery 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

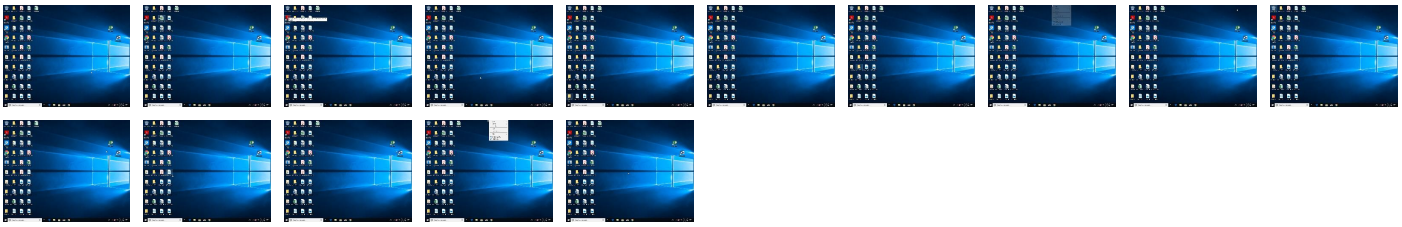
Behavior Graph



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.Siggen12.2497.1023.exe	54%	Virustotal		Browse
SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe	59%	ReversingLabs	Win32.Trojan.Zenpak	
SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe	100%	Avira	TR/Crypt.XPACK.Gen	
SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://94.103.94.2/gucci.exe	100%	Avira URL Cloud	malware	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://94.103.94.2/tnf.exe	100%	Avira URL Cloud	malware	
http://94.103.94.2	0%	Avira URL Cloud	safe	
http://94.103.94.24	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

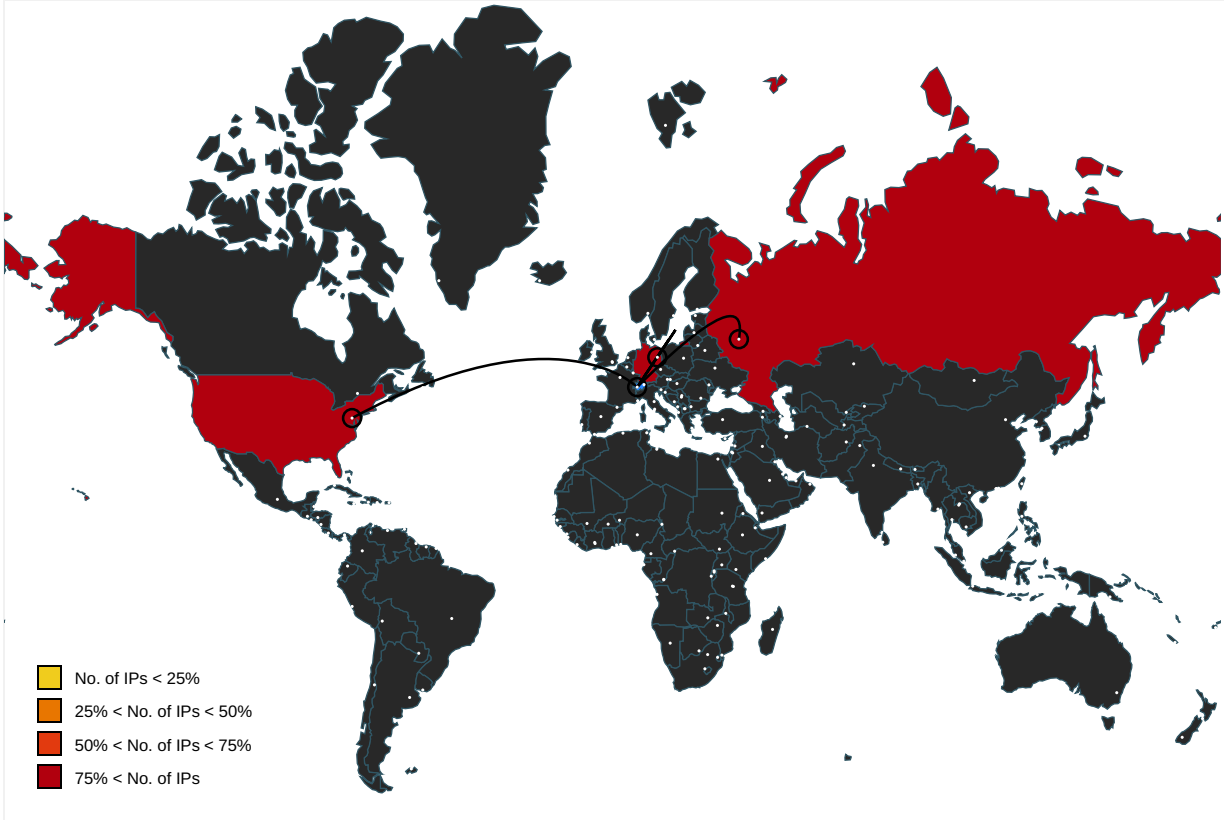
Name	IP	Active	Malicious	Antivirus Detection	Reputation
iplogger.org	88.99.66.31	true	false		high
pastebin.com	104.23.98.190	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe, 00000001.00000002.282397937.00000000031EF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iplogger.org	SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe, 00000001.00000002.282397937.00000000031EF000.00000004.00000001.sdmp	false		high
http://https://sectigo.com/CPS0	SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe, 00000001.00000002.282397937.00000000031EF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pastebin.com/raw/ZdmQ9Ych	SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe, 00000001.00000002.280165219.00000000002B2000.00000020.00020000.sdmp	false		high
http://94.103.94.2/gucci.exe	SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe, 00000001.00000002.282335767.00000000031580000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.thawte.com/ThawteTimestampingCA.crl0	SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe	false		high
http://ocsp.sectigo.com0	SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe, 00000001.00000002.282397937.00000000031EF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://94.103.94.2/tnf.exe	SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe, 00000001.00000002.282335767.00000000031580000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://94.103.94.2	SecuriteInfo.com.Trojan.Siggen 12.2497.1023.exe, 00000001.000 00002.282452543.00000000032490 00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://94.103.94.24	SecuriteInfo.com.Trojan.Siggen 12.2497.1023.exe, 00000001.000 00002.282381526.00000000031C00 00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.thawte.com0	SecuriteInfo.com.Trojan.Siggen 12.2497.1023.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pastebin.com/raw/ZdmQ9YchT	SecuriteInfo.com.Trojan.Siggen 12.2497.1023.exe, 00000001.000 00002.282272751.00000000031110 00.00000004.00000001.sdmp	false		high
http://https://pastebin.com/raw/LpGZbDTX	SecuriteInfo.com.Trojan.Siggen 12.2497.1023.exe, 00000001.000 00002.280165219.00000000002B20 00.00000020.00020000.sdmp, Sec uriteInfo.com.Trojan.Siggen12. 2497.1023.exe, 00000001.000000 02.282272751.0000000003111000. 00000004.00000001.sdmp	false		high
http://https://iplogger.org/1nzde7	SecuriteInfo.com.Trojan.Siggen 12.2497.1023.exe, 00000001.000 00002.282335767.00000000031580 00.00000004.00000001.sdmp, Sec uriteInfo.com.Trojan.Siggen12. 2497.1023.exe, 00000001.000000 02.280165219.00000000002B2000. 00000020.00020000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Trojan.Siggen 12.2497.1023.exe, 00000001.000 00002.282272751.00000000031110 00.00000004.00000001.sdmp	false		high
http://https://iplogger.org	SecuriteInfo.com.Trojan.Siggen 12.2497.1023.exe, 00000001.000 00002.282335767.00000000031580 00.00000004.00000001.sdmp	false		high
http://https://pastebin.com	SecuriteInfo.com.Trojan.Siggen 12.2497.1023.exe, 00000001.000 00002.282272751.00000000031110 00.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
88.99.66.31	unknown	Germany		24940	HETZNER-ASDE	false
104.23.98.190	unknown	United States		13335	CLOUDFLARENETUS	false
94.103.94.2	unknown	Russian Federation		48282	VDSINA-ASRU	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356833
Start date:	23.02.2021
Start time:	17:33:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.Siggen12.2497.1023.964 (renamed file extension from 964 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
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.evad.winEXE@1/1@2/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 23.211.6.115, 13.64.90.137, 168.61.161.212, 52.255.188.83, 23.218.208.56, 51.104.139.180, 20.54.26.129, 67.26.83.254, 67.26.75.254, 8.253.204.249, 67.26.73.254, 8.248.139.254, 51.103.5.159, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:34:36	API Interceptor	1x Sleep call for process: SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
88.99.66.31	Zy7qKW0uYZ.exe	Get hash	malicious	Browse	• 2no.co/1v22h7.html
	buran.exe	Get hash	malicious	Browse	• iplogger.ru/1Oh8E.jpeg
	6fAjRmbM4P.exe	Get hash	malicious	Browse	• 2no.co/1v22h7.html
	Buran.exe	Get hash	malicious	Browse	• iplogger.org/1YN4g7.tgz
	MC6YwfvkvS.exe	Get hash	malicious	Browse	• iplogger.org/1DRd77.gz
	TrustedInstaller.exe	Get hash	malicious	Browse	• iplogger.org/1yekr7.gz
	zeppelin.exe	Get hash	malicious	Browse	• iplogger.org/1D2XM6.tgz
	cli.exe	Get hash	malicious	Browse	• ezstat.ru/1BiQt7.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	R7w74RKW9A.exe	Get hash	malicious	Browse	• ezstat.ru /1BiQt7.html
	pqSZtQiuRy.exe	Get hash	malicious	Browse	• iplogger. org/14mvt7.gz
	3MndTUzGQn.exe	Get hash	malicious	Browse	• iplogger. org/14qK87
	fEBNeNkRYI.doc	Get hash	malicious	Browse	• iplogger. org/1cyy87.jpg
	Delivery-77426522.doc	Get hash	malicious	Browse	• iplogger. org/1cyy87.jpg
	mesager43.exe	Get hash	malicious	Browse	• iplogger. org/1cyy87.jpg
	hci0xn0zip.exe	Get hash	malicious	Browse	• iplogger. org/1cyy87.jpg
	DOC001.exe	Get hash	malicious	Browse	• 2no.co/1Lan77
	DOC001 (3).exe	Get hash	malicious	Browse	• 2no.co/1Lan77
	urgently.exe	Get hash	malicious	Browse	• iplogger. org/1Uu547.tgz
	SecuriteInfo.com.Generic.mg.e26982b170856ca8.exe	Get hash	malicious	Browse	• iplogger. org/1Uu547.tgz
	trwf3446.doc	Get hash	malicious	Browse	• iplogger. org/1Uu547.tgz

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
pastebin.com	1vuet1S3tI.exe	Get hash	malicious	Browse	• 104.23.98.190
	RkoKlvuLh6.exe	Get hash	malicious	Browse	• 104.23.99.190
	i0fOtOV8v0.exe	Get hash	malicious	Browse	• 104.23.99.190
	zLyXzE7WZi.exe	Get hash	malicious	Browse	• 104.23.99.190
	wLy18x5e2o.exe	Get hash	malicious	Browse	• 104.23.99.190
	QJ2UZbJWDS.exe	Get hash	malicious	Browse	• 104.23.99.190
	SWW8Mmeq6o.exe	Get hash	malicious	Browse	• 104.23.99.190
	BIb5AQZOu9.exe	Get hash	malicious	Browse	• 104.23.98.190
	7XJCrOkoIy.exe	Get hash	malicious	Browse	• 104.23.98.190
	fNOZjHL61d.exe	Get hash	malicious	Browse	• 104.23.98.190
	Ru8jlqio70.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	• 104.23.99.190
	8WjU4jrBIr.exe	Get hash	malicious	Browse	• 104.23.98.190
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 104.23.99.190
	CN-Invoice-XXXXX9808-19011143287992.exe	Get hash	malicious	Browse	• 104.23.98.190
	NitroGenerator.exe	Get hash	malicious	Browse	• 104.23.98.190
	Invoice467972.jar	Get hash	malicious	Browse	• 104.23.99.190
	Invoice467972.jar	Get hash	malicious	Browse	• 104.23.98.190
	REVISED_INVOICE_Company_BankDetails_fle_doc.xlsx.exe	Get hash	malicious	Browse	• 104.23.99.190
	MT0128.jar	Get hash	malicious	Browse	• 104.23.98.190
iplogger.org	1vuet1S3tI.exe	Get hash	malicious	Browse	• 88.99.66.31
	seed.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Variant.Zusy.368685.25375.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Variant.Zusy.368685.25618.exe	Get hash	malicious	Browse	• 88.99.66.31
	8WjU4jrBIr.exe	Get hash	malicious	Browse	• 88.99.66.31
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 88.99.66.31
	ydQ0ICWj5v.exe	Get hash	malicious	Browse	• 88.99.66.31
	r4yGYPyWb7.exe	Get hash	malicious	Browse	• 88.99.66.31
	aif9fEvN5g.exe	Get hash	malicious	Browse	• 88.99.66.31
	bZ9avvcHvE.exe	Get hash	malicious	Browse	• 88.99.66.31
	CmJ6qDTzvM.exe	Get hash	malicious	Browse	• 88.99.66.31
	RRLrVfeAXb.exe	Get hash	malicious	Browse	• 88.99.66.31
	m3eJIFyc68.exe	Get hash	malicious	Browse	• 88.99.66.31
	m8kdtboA0T.exe	Get hash	malicious	Browse	• 88.99.66.31
	jdAbDsECEE.exe	Get hash	malicious	Browse	• 88.99.66.31
	m8kdtboA0T.exe	Get hash	malicious	Browse	• 88.99.66.31
	IVCkMokXk8.exe	Get hash	malicious	Browse	• 88.99.66.31
	i9WK2pIYWG.exe	Get hash	malicious	Browse	• 88.99.66.31

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	1vuet1S3tI.exe	Get hash	malicious	Browse	• 172.67.199.58
	P00760000.exe	Get hash	malicious	Browse	• 104.21.19.200
	Order.doc	Get hash	malicious	Browse	• 104.21.19.200
	QUOTE.doc	Get hash	malicious	Browse	• 104.21.19.200
	Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	2070121_SN-WS.exe	Get hash	malicious	Browse	• 104.21.71.230
	purchase order.exe	Get hash	malicious	Browse	• 104.21.19.200
	9073782912,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	payment_advice.doc	Get hash	malicious	Browse	• 172.67.172.17
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	dot crypted.exe	Get hash	malicious	Browse	• 104.21.19.200
	New Order 2300030317388 InterMetro.exe	Get hash	malicious	Browse	• 172.67.172.17
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	• 172.67.172.17
	Purchase Order list.exe	Get hash	malicious	Browse	• 104.21.23.61
	RkoKlvuLh6.exe	Get hash	malicious	Browse	• 162.159.13 6.232
	i0fOtOV8v0.exe	Get hash	malicious	Browse	• 104.23.99.190
	P3knxzE7wN.exe	Get hash	malicious	Browse	• 162.159.12 8.233
	zLyXzE7WZi.exe	Get hash	malicious	Browse	• 162.159.13 8.232
	wLy18x5e2o.exe	Get hash	malicious	Browse	• 162.159.13 6.232
HETZNER-ASDE	1vuet1S3tI.exe	Get hash	malicious	Browse	• 88.99.66.31
	MV9tCJw8Xr.exe	Get hash	malicious	Browse	• 195.201.56.70
	seed.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Variant.Zusy.368685.25375.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	Get hash	malicious	Browse	• 95.216.186.40
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 195.201.22 5.248
	SecuriteInfo.com.Variant.Zusy.368685.25618.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	Get hash	malicious	Browse	• 95.216.186.40
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	• 95.216.186.40
	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 195.201.22 5.248
	8WjU4jrBIr.exe	Get hash	malicious	Browse	• 94.130.165.85
	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe	Get hash	malicious	Browse	• 188.40.67.173
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 88.99.66.31
	Order_20180218001.exe	Get hash	malicious	Browse	• 135.181.57.206
	unmapped_executable_of_polyglot_duke.dll	Get hash	malicious	Browse	• 5.9.110.84
	DHL eInvoice_Pdf.exe	Get hash	malicious	Browse	• 195.201.179.80
	Subconract 504.xlsm	Get hash	malicious	Browse	• 95.216.245.130
	ydQ0ICWj5v.exe	Get hash	malicious	Browse	• 88.99.66.31
	r4yGYPyWb7.exe	Get hash	malicious	Browse	• 88.99.66.31

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	P00760000.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31
	Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31
	purchase order.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31
	9073782912,pdf.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31
	Purchase Order.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31
	dot crypted.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31
	v2.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31
	Halkbank_Ekstre_20210223_082357_541079.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31
	FOB offer_1164087223_I0133P2100363812.PDF.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31
	(appproved)WJO-TT180,pdf.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31
	purchase order.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31
	9073782912,pdf.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31
	purchase order 1.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31
	telex transfer.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31
	GPP.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31
	DHL Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 104.23.98.190 • 88.99.66.31

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	847
Entropy (8bit):	5.35816127824051
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MxHKXwYHKhQnoPtHoxHhAHKzva
MD5:	31E089E21A2AEB18A2A23D3E61EB2167
SHA1:	E873A8FC023D1C6D767A0C752582E3C9FD67A8B0
SHA-256:	2DCCE5D76F242AF36DB3D670C006468BEEA4C58A6814B2684FE44D45E7A3F836
SHA-512:	A0DB65C3E133856C0A73990AEC30B1B037EA486B44E4A30657DD5775880FB9248D9E1CB533420299D0538882E9A883BA64F30F7263EB0DD62D1C673E7DBA881
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.9537837476311966

General

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.Siggen12.2497.1023.exe
File size:	2665184
MD5:	9e74c1841ab5ec50dd43819aaba20c0b
SHA1:	d37d7026c09dc6d93fd01dc90d7a224d22dca168
SHA256:	d367eca88434cb310aad91f251c9baa7d11fcd2ffd2c0f0cbb35595445a27698
SHA512:	7a2ce87fa40f324569d710a5163431d0ac6f1456a4b8c242e173b46a62b0effaf6f4d38617d710ebec6dd0a976475df913dc7b6ba8f9f16069257c86e768ec7d
SSDEEP:	49152:Qbp22+n3DZ3hTHi9zEtSSoTJVhurXd0btj4raluLy+p+3EIHQEwI9qY/wBdZN:Q92Ln3D7QzEESgicR4ty+mNHvp9qKwB5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....W....."...0.....X.E.. ...@....@.. .....m.....-)...`.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x858058
Entrypoint Section:	.boot
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, HIGH_ENTROPY_VA
Time Stamp:	0xAC57F2AF [Tue Aug 16 19:08:31 2061 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:	4328f7206db519cd4e82283211d98e83

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert High Assurance Code Signing CA-1, OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 6/1/2017 5:00:00 PM 7/8/2020 5:00:00 AM
Subject Chain	• CN=Kaspersky Lab, O=Kaspersky Lab, L=Moscow, C=RU
Version:	3
Thumbprint MD5:	D47ED7012E116270A767DA88438C3BA6
Thumbprint SHA-1:	3C92C9274AB6D3DD520B13029A2490C4A1D98BC0
Thumbprint SHA-256:	3606C42F2608526263AC61997AA0A83B364FB23A6882447CA787B5A5790115D8
Serial:	0F9D91C6ABA86F4E54CBB9EF57E68346

Entrypoint Preview

Instruction
call 00007FDC0C5B4870h
push ebx
mov ebx, esp
push ebx
mov esi, dword ptr [ebx+08h]
mov edi, dword ptr [ebx+10h]
cld
mov dl, 80h
mov al, byte ptr [esi]
inc esi
mov byte ptr [edi], al
inc edi
mov ebx, 00000002h
add dl, dl
jne 00007FDC0C5B4727h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jnc 00007FDC0C5B470Ch
add dl, dl
jne 00007FDC0C5B4727h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jnc 00007FDC0C5B4773h
xor eax, eax
add dl, dl
jne 00007FDC0C5B4727h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jnc 00007FDC0C5B4807h
add dl, dl
jne 00007FDC0C5B4727h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc eax, eax
add dl, dl
jne 00007FDC0C5B4727h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc eax, eax
add dl, dl
jne 00007FDC0C5B4727h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc eax, eax
add dl, dl
jne 00007FDC0C5B4727h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc eax, eax
je 00007FDC0C5B472Ah
push edi
mov eax, eax
sub edi, eax
mov al, byte ptr [edi]
pop edi
mov byte ptr [edi], al
inc edi

Instruction
mov ebx, 00000002h
jmp 00007FDC0C5B46BBh
mov eax, 00000001h
add dl, dl
jne 00007FDC0C5B4727h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc eax, eax
add dl, dl
jne 00007FDC0C5B4727h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jc 00007FDC0C5B470Ch
sub eax, ebx
mov ebx, 00000001h
jne 00007FDC0C5B474Ah
mov ecx, 00000001h
add dl, dl
jne 00007FDC0C5B4727h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
adc ecx, ecx
add dl, dl
jne 00007FDC0C5B4727h
mov dl, byte ptr [esi]
inc esi
adc dl, dl
jc 00007FDC0C5B470Ch
push esi
mov esi, edi
sub esi, ebp

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x803a	0x50	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa000	0x5cc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x287400	0x36e0	.themida
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
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
	0x2000	0x2000	0x800	False	0.97509765625	data	7.67255739846	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
	0x4000	0x5cc	0x400	False	0.9755859375	data	7.31449001732	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
	0x6000	0xc	0x200	False	0.591796875	data	4.34313215347	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.idata	0x8000	0x2000	0x200	False	0.16796875	data	1.05072803613	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xa000	0x2000	0x600	False	0.422526041667	data	4.10903222417	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.themida	0xc000	0x44c000	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.boot	0x458000	0x285a00	0x285a00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xa090	0x33c	data		
RT_MANIFEST	0xa3dc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators	English	United States

Imports

DLL	Import
kernel32.dll	GetModuleHandleA
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2019
Assembly Version	1.0.0.0
InternalName	pastebinload.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	pastebinload
ProductVersion	1.0.0.0
FileDescription	pastebinload
OriginalFilename	pastebinload.exe

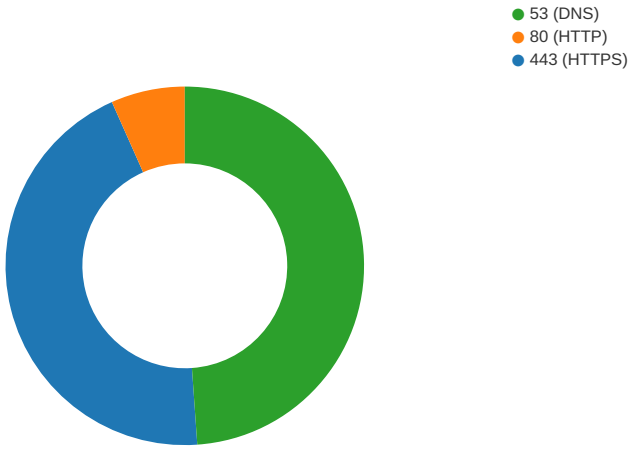
Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 45



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:34:14.869764090 CET	49721	443	192.168.2.5	104.23.98.190
Feb 23, 2021 17:34:14.913286924 CET	443	49721	104.23.98.190	192.168.2.5
Feb 23, 2021 17:34:14.913436890 CET	49721	443	192.168.2.5	104.23.98.190
Feb 23, 2021 17:34:14.983339071 CET	49721	443	192.168.2.5	104.23.98.190
Feb 23, 2021 17:34:15.024333000 CET	443	49721	104.23.98.190	192.168.2.5
Feb 23, 2021 17:34:15.028955936 CET	443	49721	104.23.98.190	192.168.2.5
Feb 23, 2021 17:34:15.028994083 CET	443	49721	104.23.98.190	192.168.2.5
Feb 23, 2021 17:34:15.029050112 CET	443	49721	104.23.98.190	192.168.2.5
Feb 23, 2021 17:34:15.029119968 CET	49721	443	192.168.2.5	104.23.98.190
Feb 23, 2021 17:34:15.033962011 CET	49721	443	192.168.2.5	104.23.98.190
Feb 23, 2021 17:34:15.076345921 CET	443	49721	104.23.98.190	192.168.2.5
Feb 23, 2021 17:34:15.076601028 CET	443	49721	104.23.98.190	192.168.2.5
Feb 23, 2021 17:34:15.210010052 CET	49721	443	192.168.2.5	104.23.98.190
Feb 23, 2021 17:34:15.241267920 CET	49721	443	192.168.2.5	104.23.98.190
Feb 23, 2021 17:34:15.282227993 CET	443	49721	104.23.98.190	192.168.2.5
Feb 23, 2021 17:34:15.296063900 CET	443	49721	104.23.98.190	192.168.2.5
Feb 23, 2021 17:34:15.296092033 CET	443	49721	104.23.98.190	192.168.2.5
Feb 23, 2021 17:34:15.296180010 CET	49721	443	192.168.2.5	104.23.98.190
Feb 23, 2021 17:34:15.309288979 CET	49721	443	192.168.2.5	104.23.98.190
Feb 23, 2021 17:34:15.361028910 CET	443	49721	104.23.98.190	192.168.2.5
Feb 23, 2021 17:34:15.361053944 CET	443	49721	104.23.98.190	192.168.2.5
Feb 23, 2021 17:34:15.361155987 CET	49721	443	192.168.2.5	104.23.98.190
Feb 23, 2021 17:34:15.434195995 CET	49722	443	192.168.2.5	88.99.66.31
Feb 23, 2021 17:34:15.505187988 CET	443	49722	88.99.66.31	192.168.2.5
Feb 23, 2021 17:34:15.505347967 CET	49722	443	192.168.2.5	88.99.66.31
Feb 23, 2021 17:34:15.505953074 CET	49722	443	192.168.2.5	88.99.66.31
Feb 23, 2021 17:34:15.576910973 CET	443	49722	88.99.66.31	192.168.2.5
Feb 23, 2021 17:34:15.579960108 CET	443	49722	88.99.66.31	192.168.2.5
Feb 23, 2021 17:34:15.579993963 CET	443	49722	88.99.66.31	192.168.2.5
Feb 23, 2021 17:34:15.580010891 CET	443	49722	88.99.66.31	192.168.2.5
Feb 23, 2021 17:34:15.580027103 CET	443	49722	88.99.66.31	192.168.2.5
Feb 23, 2021 17:34:15.580091000 CET	49722	443	192.168.2.5	88.99.66.31
Feb 23, 2021 17:34:15.580144882 CET	49722	443	192.168.2.5	88.99.66.31
Feb 23, 2021 17:34:15.612219095 CET	49722	443	192.168.2.5	88.99.66.31
Feb 23, 2021 17:34:15.684082985 CET	443	49722	88.99.66.31	192.168.2.5
Feb 23, 2021 17:34:15.708132982 CET	49722	443	192.168.2.5	88.99.66.31
Feb 23, 2021 17:34:15.789016008 CET	443	49722	88.99.66.31	192.168.2.5
Feb 23, 2021 17:34:15.791534901 CET	49723	80	192.168.2.5	94.103.94.2
Feb 23, 2021 17:34:15.922952890 CET	49722	443	192.168.2.5	88.99.66.31
Feb 23, 2021 17:34:18.923104048 CET	49723	80	192.168.2.5	94.103.94.2
Feb 23, 2021 17:34:20.047295094 CET	49722	443	192.168.2.5	88.99.66.31
Feb 23, 2021 17:34:24.923680067 CET	49723	80	192.168.2.5	94.103.94.2
Feb 23, 2021 17:34:36.969779015 CET	49721	443	192.168.2.5	104.23.98.190

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:34:03.774154902 CET	62176	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:34:03.831387043 CET	53	62176	8.8.8.8	192.168.2.5
Feb 23, 2021 17:34:04.643302917 CET	59596	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:34:04.706511974 CET	53	59596	8.8.8.8	192.168.2.5
Feb 23, 2021 17:34:05.069267988 CET	65296	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:34:05.122757912 CET	53	65296	8.8.8.8	192.168.2.5
Feb 23, 2021 17:34:06.338099957 CET	63183	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:34:06.395525932 CET	53	63183	8.8.8.8	192.168.2.5
Feb 23, 2021 17:34:07.659116030 CET	60151	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:34:07.710705996 CET	53	60151	8.8.8.8	192.168.2.5
Feb 23, 2021 17:34:09.409313917 CET	56969	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:34:09.462913036 CET	53	56969	8.8.8.8	192.168.2.5
Feb 23, 2021 17:34:10.443526983 CET	55161	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:34:10.503493071 CET	53	55161	8.8.8.8	192.168.2.5
Feb 23, 2021 17:34:12.133086920 CET	54757	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:34:12.187357903 CET	53	54757	8.8.8.8	192.168.2.5
Feb 23, 2021 17:34:14.746510029 CET	49992	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:34:14.797784090 CET	60075	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:34:14.798823118 CET	53	49992	8.8.8.8	192.168.2.5
Feb 23, 2021 17:34:14.846426964 CET	53	60075	8.8.8.8	192.168.2.5
Feb 23, 2021 17:34:15.370466948 CET	55016	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:34:15.432893991 CET	53	55016	8.8.8.8	192.168.2.5
Feb 23, 2021 17:34:16.004375935 CET	64345	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:34:16.068969965 CET	53	64345	8.8.8.8	192.168.2.5
Feb 23, 2021 17:34:16.943373919 CET	57128	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:34:16.992152929 CET	53	57128	8.8.8.8	192.168.2.5
Feb 23, 2021 17:34:30.789222956 CET	54791	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:34:30.938575983 CET	53	54791	8.8.8.8	192.168.2.5
Feb 23, 2021 17:34:35.938600063 CET	50463	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:34:35.990102053 CET	53	50463	8.8.8.8	192.168.2.5
Feb 23, 2021 17:34:56.437218904 CET	50394	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:34:56.509088039 CET	53	50394	8.8.8.8	192.168.2.5
Feb 23, 2021 17:34:58.543198109 CET	58530	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:34:58.591972113 CET	53	58530	8.8.8.8	192.168.2.5
Feb 23, 2021 17:34:59.956121922 CET	53813	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:35:00.004868031 CET	53	53813	8.8.8.8	192.168.2.5
Feb 23, 2021 17:35:01.536695957 CET	63732	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:35:01.585465908 CET	53	63732	8.8.8.8	192.168.2.5
Feb 23, 2021 17:35:08.141235113 CET	57344	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:35:08.199840069 CET	53	57344	8.8.8.8	192.168.2.5
Feb 23, 2021 17:35:40.841784954 CET	54450	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:35:40.893313885 CET	53	54450	8.8.8.8	192.168.2.5
Feb 23, 2021 17:35:41.297235012 CET	59261	53	192.168.2.5	8.8.8.8
Feb 23, 2021 17:35:41.356280088 CET	53	59261	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 17:34:14.746510029 CET	192.168.2.5	8.8.8.8	0xf65	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Feb 23, 2021 17:34:15.370466948 CET	192.168.2.5	8.8.8.8	0xe415	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:34:14.798823118 CET	8.8.8.8	192.168.2.5	0xf65	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Feb 23, 2021 17:34:14.798823118 CET	8.8.8.8	192.168.2.5	0xf65	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:34:15.432893991 CET	8.8.8.8	192.168.2.5	0xe415	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 17:34:15.029050112 CET	104.23.98.190	443	192.168.2.5	49721	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 17 02:00:00 CEST 2020	Tue Aug 17 14:00:00 CEST 2021	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:46:39 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Feb 23, 2021 17:34:15.580027103 CET	88.99.66.31	443	192.168.2.5	49722	CN=*.iplogger.org CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Nov 20 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Nov 21 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

System Behavior

Analysis Process: SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe PID: 4196 Parent PID: 5716

General

Start time:	17:34:11
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe'
Imagebase:	0x2b0000
File size:	2665184 bytes
MD5 hash:	9E74C1841AB5EC50DD43819AABA20C0B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D9BCF06	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	6D9BCF06	unknown
C:\Users\user\AppData\Local\l.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	5A9EED	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5A9EED	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\l.exe	success or wait	1	6C806A95	DeleteFileW

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\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe.log	unknown	847	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0	success or wait	1	6DCCC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	4DA93A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	4DA93A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	4DA93A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	4DA93A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	4DA93A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	4DA93A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	4DA93A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	4DA93A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	4DA93A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	4DA93A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	4DA93A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	4DA93A	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	2	success or wait	1	4DA93A	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	998	success or wait	1	4DA93A	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	2	success or wait	1	4DA93A	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis