ID: 356597
Sample Name:
SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.2561
Cookbook: default.jbs
Time: 11:56:28
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

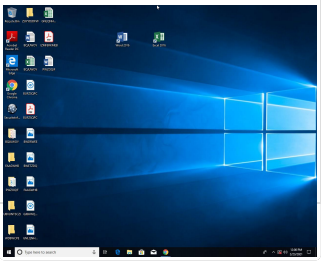
Analysis Report SecuriteInfo.com.Trojan.GenericKDZ.73…

Overview

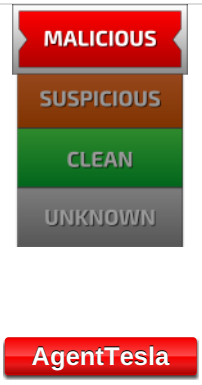
General Information

Sample Name:	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.2561 (renamed file extension from 2561 to exe)
Analysis ID:	356597
MD5:	ed6841cbc52069..
SHA1:	3b51ff4aa0b8d39..
SHA256:	0381c68c02579e..
Tags:	AgentTesla

Most interesting Screenshot:



Detection

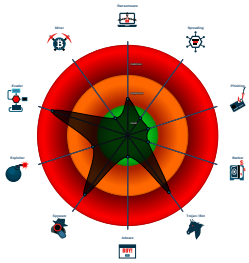


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe (PID: 6952 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe' MD5: ED6841CBC5206942DD2E812F7855B156)
  - SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe (PID: 7020 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe MD5: ED6841CBC5206942DD2E812F7855B156)
  - SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe (PID: 7080 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe MD5: ED6841CBC5206942DD2E812F7855B156)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "6WLmA2S8h7",
  "URL: ": "https://GsKwOmvIezHndSQmIcyS.com",
  "To: ": "armyscheme@yandex.com",
  "ByHost: ": "smtp.yandex.com:587",
  "Password: ": "UM9UHPz8BDmgDL",
  "From: ": "armyscheme@yandex.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.652337158.000000000367 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.911990568.00000000029C 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.651915801.000000000267 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.910118958.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.651977760.00000000026A B000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 4 entries				

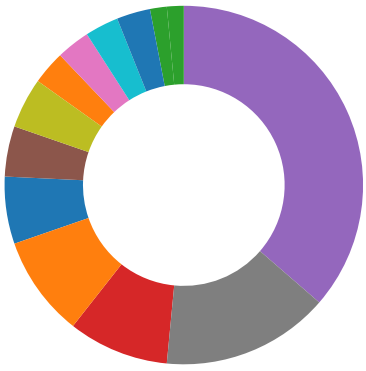
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.Trojan.GenericKDZ.73120.3552. exe.3944ca0.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.SecuriteInfo.com.Trojan.GenericKDZ.73120.3552. exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Trojan.GenericKDZ.73120.3552. exe.269986c.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.2.SecuriteInfo.com.Trojan.GenericKDZ.73120.3552. exe.3944ca0.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Trojan.GenericKDZ.73120.3552. exe.38447f0.5.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 2 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

Yara detected AntiVM_3

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

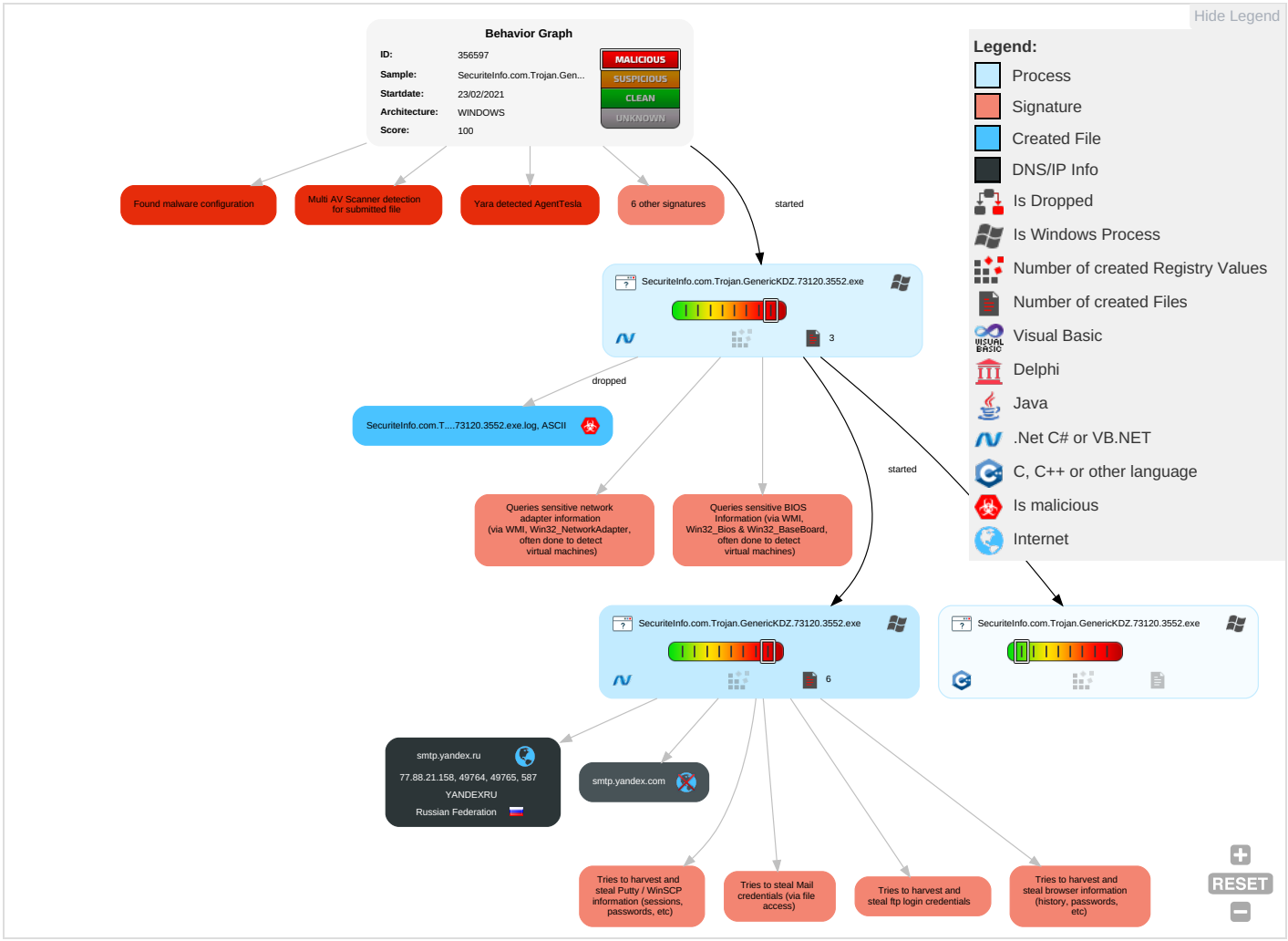
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 3	Credentials in Registry 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

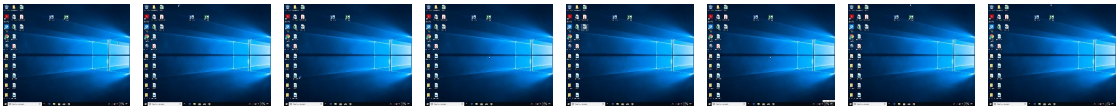
Behavior Graph



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.GenericKDZ.73120.3552.exe	37%	Virustotal		Browse
SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe	33%	ReversingLabs	Win32.Trojan.AgentTesla	
SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://tTAnFc.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://GsKwOmvIezHndSQmIcyS.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://yandex.ocsp-responder.com03	0%	URL Reputation	safe	
http://yandex.ocsp-responder.com03	0%	URL Reputation	safe	
http://yandex.ocsp-responder.com03	0%	URL Reputation	safe	
http://yandex.ocsp-responder.com03	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://crl.certum.plWq	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.yandex.ru	77.88.21.158	true	false		high
smtp.yandex.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://GsKwOmvIezHndSQmIcyS.com	true	• Avira URL Cloud: safe	unknown

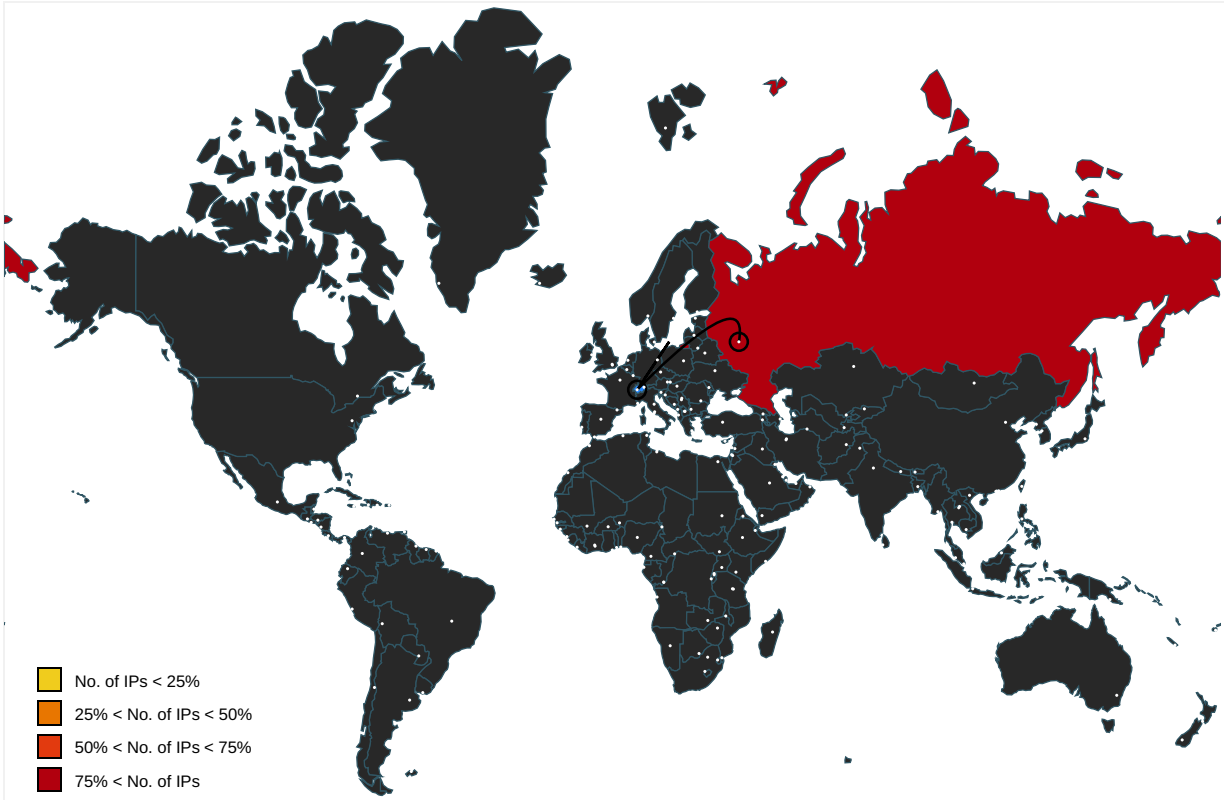
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.911990568.00000000029C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.911990568.00000000029C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://tTAnFc.com	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.911990568.00000000029C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://repository.certum.pl/ctnca.cer09	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.912711978.0000000002D64000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.911990568.00000000029C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.certum.pl/ctnca.crl0k	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.912711978.0000000002D64000.00000004.00000001.sdmp	false		high
http://yandex.crl.certum.pl/ycasha2.crl0q	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.912711978.0000000002D64000.00000004.00000001.sdmp	false		high
http://https://www.certum.pl/CPS0	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.912711978.0000000002D64000.00000004.00000001.sdmp	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000000.00000002.651915801.0000000002671000.00000004.00000001.sdmp	false		high
http://smtp.yandex.com	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.912711978.0000000002D64000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%$	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.911990568.00000000029C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://yandex.ocsp-responder.com03	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.912711978.0000000002D64000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://subca.ocsp-certum.com0.	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.912711978.0000000002D64000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.certum.pl/ca.cer09	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.912711978.0000000002D64000.00000004.00000001.sdmp	false		high
http://www.certum.pl/Ciq	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.915387308.0000000006370000.00000004.00000001.sdmp	false		high
http://crls.yandex.net/certum/ycasha2.crl0-	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.912711978.0000000002D64000.00000004.00000001.sdmp	false		high
http://subca.ocsp-certum.com01	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.912711978.0000000002D64000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.911990568.00000000029C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://crl.certum.pl/ca.crl0h	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.912711978.0000000002D64000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000000.00000002.651915801.0000000002671000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000000.00000002.652337158.0000000003679000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.910118958.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certum.pl/CPS0	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.912711978.0000000002D64000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.certum.plWq	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.915387308.0000000006370000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://repository.certum.pl/ycasha2.cer0	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe, 00000004.00000002.912711978.0000000002D64000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.88.21.158	unknown	Russian Federation		13238	YANDEXRU	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356597
Start date:	23.02.2021
Start time:	11:56:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.2561 (renamed file extension from 2561 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:	19
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@5/2@4/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.7% (good quality ratio 0.7%) • Quality average: 73% • Quality standard deviation: 24.6%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 13.64.90.137, 92.122.145.220, 168.61.161.212, 51.104.144.132, 67.26.83.254, 8.248.117.254, 8.248.131.254, 8.248.121.254, 67.26.81.254, 52.155.217.156, 20.54.26.129, 51.11.168.160, 92.122.213.247, 92.122.213.194, 51.104.139.180 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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.

Simulations

Behavior and APIs

Time	Type	Description
11:58:12	API Interceptor	767x Sleep call for process: SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
77.88.21.158	PO Contract -SCPL0882021 & sales contract ZD.1.190 22021_PDF.exe	Get hash	malicious	Browse	
	pass.exe	Get hash	malicious	Browse	
	nXKdiUgIYy.exe	Get hash	malicious	Browse	
	x4cXV3784J.exe	Get hash	malicious	Browse	
	Request For Quotation #D22022021_pdf.exe	Get hash	malicious	Browse	
	RFQ_PDRVK2200248_00667_PDF.exe	Get hash	malicious	Browse	
	emI0MqOvFw.exe	Get hash	malicious	Browse	
	ZnsXrCAriL.exe	Get hash	malicious	Browse	
	zyp9gbDQHw.exe	Get hash	malicious	Browse	
	DHL Shipment Notification.PDF.exe	Get hash	malicious	Browse	
	MI3eskSuv2.exe	Get hash	malicious	Browse	
	NUANG KONG-ON2343020-146377_PDF.exe	Get hash	malicious	Browse	
	NUANG KONG-ON2343020-146377_PDF.exe	Get hash	malicious	Browse	
	feb 16 processed.xlsx	Get hash	malicious	Browse	
	IMG_Catalogue Document.exe	Get hash	malicious	Browse	
	PO#THE786YT_pdf.exe	Get hash	malicious	Browse	
	BL_No#ONEYJKTAC6384600.exe	Get hash	malicious	Browse	
	DHL Delivery Documents.exe	Get hash	malicious	Browse	
	Scan copy.exe	Get hash	malicious	Browse	
	jmsg.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.yandex.ru	PO Contract -SCPL0882021 & sales contract ZD.1.190 22021_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	pass.exe	Get hash	malicious	Browse	• 77.88.21.158
	nXKdiUgIYy.exe	Get hash	malicious	Browse	• 77.88.21.158
	x4cXV3784J.exe	Get hash	malicious	Browse	• 77.88.21.158
	Request For Quotation #D22022021_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ_PDRVK2200248_00667_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	emI0MqOvFw.exe	Get hash	malicious	Browse	• 77.88.21.158
	ZnsXrCAriL.exe	Get hash	malicious	Browse	• 77.88.21.158
	zyp9gbDQHw.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL Shipment Notification.PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	MI3eskSuv2.exe	Get hash	malicious	Browse	• 77.88.21.158
	NUANG KONG-ON2343020-146377_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	NUANG KONG-ON2343020-146377_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	feb 16 processed.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	IMG_Catalogue Document.exe	Get hash	malicious	Browse	• 77.88.21.158
	PO#THE786YT_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	BL_No#ONEYJKTAC6384600.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL Delivery Documents.exe	Get hash	malicious	Browse	• 77.88.21.158
	Scan copy.exe	Get hash	malicious	Browse	• 77.88.21.158
	jmsg.exe	Get hash	malicious	Browse	• 77.88.21.158

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
YANDEXRU	PO Contract -SCPL0882021 & sales contract ZD.1.190 22021_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	pass.exe	Get hash	malicious	Browse	• 77.88.21.158
	nXKdiUgIYy.exe	Get hash	malicious	Browse	• 77.88.21.158
	x4cXV3784J.exe	Get hash	malicious	Browse	• 77.88.21.158
	Request For Quotation #D22022021_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ_PDRVK2200248_00667_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	emI0MqOvFw.exe	Get hash	malicious	Browse	• 77.88.21.158
	ZnsXrCAriL.exe	Get hash	malicious	Browse	• 77.88.21.158
	zyp9gbDQHw.exe	Get hash	malicious	Browse	• 77.88.21.158

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL Shipment Notification.PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	MI3eskSuv2.exe	Get hash	malicious	Browse	• 77.88.21.158
	NUANG KONG-ON2343020-146377_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	NUANG KONG-ON2343020-146377_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	feb 16 processed.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	IMG_Catalogue Document.exe	Get hash	malicious	Browse	• 77.88.21.158
	PO#THE786YT_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	BL_No#ONEYJKTAC6384600.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL Delivery Documents.exe	Get hash	malicious	Browse	• 77.88.21.158
	Scan copy.exe	Get hash	malicious	Browse	• 77.88.21.158
	jmsg.exe	Get hash	malicious	Browse	• 77.88.21.158

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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=b77a

C:\Users\user\AppData\Roaming\wqgzo1wl.s25\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Roaming\wqgzo1wl.s25\Chrome\Default\Cookies	
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.880210581673569
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe
File size:	1103872
MD5:	ed6841cbc5206942dd2e812f7855b156
SHA1:	3b51ff4aa0b8d39e6d6e2df5b19a47b06898ab21
SHA256:	0381c68c02579ec24cbc328815c87c9aa49833ae2ddc321780fe9881234a2f80
SHA512:	5ffef1b2aab994e2694d0a1a0d2e9c9866e006f34cdc838b63d8f806042ed42d7ba7965a1cd71ffa3836bfc804f402b52af4d7d63de5b41d28f3e6e0250335e1
SSDEEP:	24576:jPpPu1E6ykjcWFKDu0mcaJzi7g9aYN0g:7XjktFK5m39I
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...M.3`.....P.....L.....j.... .....@.. .....@.... .....@.....

File Icon

Icon Hash:	71e8e4a8e8f634c0

Static PE Info

General

Entrypoint:	0x50a96a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6033844D [Mon Feb 22 10:15:41 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10a918	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10c000	0x48c4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x112000	0xc	.reloc
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x108970	0x108a00	False	0.557391614017	data	6.90500904332	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x10c000	0x48c4	0x4a00	False	0.418285472973	data	4.57969847443	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x112000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x10c100	0x4228	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0x110338	0x14	data		
RT_VERSION	0x11035c	0x366	data		
RT_MANIFEST	0x1106d4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

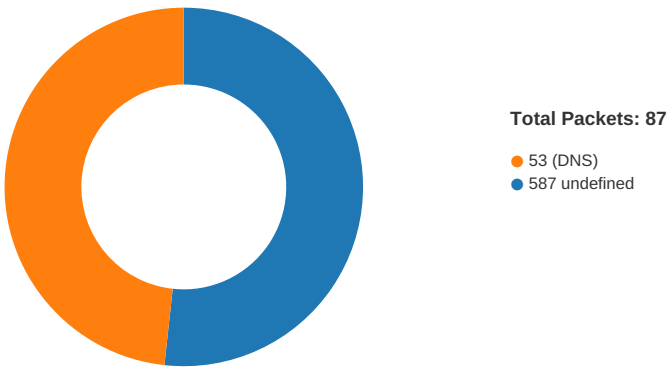
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017 Robert B. Cialdini
Assembly Version	43.338.0.0
InternalName	c.exe
FileVersion	43.338.0.0
CompanyName	Robert B. Cialdini
LegalTrademarks	
Comments	
ProductName	Thesis Nana
ProductVersion	43.338.0.0
FileDescription	Thesis Nana
OriginalFilename	c.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:58:58.106215000 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:58:58.186173916 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:58:58.186362982 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:58:58.373878002 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:58:58.375708103 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:58:58.455715895 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:58:58.455749989 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:58:58.456248999 CET	49764	587	192.168.2.4	77.88.21.158

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:58:58.538436890 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:58:58.582616091 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:58:58.615063906 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:58:58.695570946 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:58:58.695627928 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:58:58.695666075 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:58:58.695699930 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:58:58.703221083 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:58:58.771265984 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:58:58.851321936 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:58:58.895190954 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:58:59.172787905 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:58:59.251318932 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:58:59.254308939 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:58:59.332761049 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:58:59.334856987 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:58:59.431695938 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:58:59.433132887 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:58:59.519197941 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:58:59.519965887 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:58:59.608505011 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:58:59.608949900 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:58:59.687268972 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:58:59.689661026 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:58:59.689963102 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:58:59.690992117 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:58:59.691169977 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:58:59.768017054 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:58:59.769141912 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:00.415633917 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:00.457859993 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:02.183410883 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:02.262670040 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:02.262701035 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:02.262880087 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:02.401103973 CET	49764	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:02.479176044 CET	587	49764	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:03.300127029 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:03.383040905 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:03.383186102 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:03.621592999 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:03.622035027 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:03.706747055 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:03.706770897 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:03.711843014 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:03.795093060 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:03.795886040 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:03.880462885 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:03.880525112 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:03.880567074 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:03.880595922 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:03.880781889 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:03.884777069 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:03.968183994 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:03.972023964 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:04.055254936 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:04.055917025 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:04.140674114 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:04.141330004 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:04.242348909 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:04.243261099 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:04.342873096 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:04.343381882 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:04.438290119 CET	587	49765	77.88.21.158	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:59:04.438990116 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:04.521945953 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:04.523829937 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:04.524080038 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:04.524276018 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:04.524415970 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:04.524655104 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:04.524965048 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:04.525087118 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:04.525226116 CET	49765	587	192.168.2.4	77.88.21.158
Feb 23, 2021 11:59:04.607135057 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:04.607436895 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:04.608045101 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:04.608594894 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:04.649279118 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:05.229787111 CET	587	49765	77.88.21.158	192.168.2.4
Feb 23, 2021 11:59:05.270661116 CET	49765	587	192.168.2.4	77.88.21.158

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:57:06.594347000 CET	59123	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:06.643116951 CET	53	59123	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:07.803843021 CET	54531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:07.856393099 CET	53	54531	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:09.045293093 CET	49714	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:09.094345093 CET	53	49714	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:09.756489992 CET	58028	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:09.815228939 CET	53	58028	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:10.214262962 CET	53097	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:10.265885115 CET	53	53097	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:12.275666952 CET	49257	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:12.325360060 CET	53	49257	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:13.469850063 CET	62389	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:13.521256924 CET	53	62389	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:23.684297085 CET	49910	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:23.733010054 CET	53	49910	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:24.839854956 CET	55854	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:24.901241064 CET	53	55854	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:25.855124950 CET	64549	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:25.906555891 CET	53	64549	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:27.177679062 CET	63153	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:27.229803085 CET	53	63153	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:28.154551029 CET	52991	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:28.213673115 CET	53	52991	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:30.431581974 CET	53700	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:30.483865976 CET	53	53700	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:32.744935989 CET	51726	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:32.797676086 CET	53	51726	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:33.714268923 CET	56794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:33.762917042 CET	53	56794	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:35.015880108 CET	56534	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:35.094866991 CET	53	56534	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:36.185718060 CET	56627	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:36.237374067 CET	53	56627	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:37.352361917 CET	56621	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:37.401473999 CET	53	56621	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:38.845118999 CET	63116	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:38.893798113 CET	53	63116	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:39.998684883 CET	64078	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:40.050729990 CET	53	64078	8.8.8.8	192.168.2.4
Feb 23, 2021 11:57:40.403548002 CET	64801	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:57:40.452088118 CET	53	64801	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:02.191102028 CET	61721	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 11:58:02.240053892 CET	53	61721	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:02.619703054 CET	51255	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:58:02.686022997 CET	53	51255	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:03.277900934 CET	61522	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:58:03.340362072 CET	53	61522	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:03.371686935 CET	52337	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:58:03.446568012 CET	53	52337	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:03.970334053 CET	55046	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:58:04.029058933 CET	53	55046	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:04.468333006 CET	49612	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:58:04.517111063 CET	53	49612	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:04.997914076 CET	49285	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:58:05.058387995 CET	53	49285	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:05.630060911 CET	50601	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:58:05.689775944 CET	53	50601	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:06.321228027 CET	60875	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:58:06.381019115 CET	53	60875	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:07.197412014 CET	56448	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:58:07.254626036 CET	53	56448	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:08.118940115 CET	59172	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:58:08.170274973 CET	53	59172	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:08.668065071 CET	62420	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:58:08.725950003 CET	53	62420	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:16.754177094 CET	60579	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:58:16.806175947 CET	53	60579	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:16.833950043 CET	50183	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:58:16.891777039 CET	53	50183	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:22.253757954 CET	61531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:58:22.312084913 CET	53	61531	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:52.404874086 CET	49228	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:58:52.455672026 CET	53	49228	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:54.481831074 CET	59794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:58:54.546998978 CET	53	59794	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:57.843852043 CET	55916	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:58:57.903400898 CET	53	55916	8.8.8.8	192.168.2.4
Feb 23, 2021 11:58:57.920231104 CET	52752	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:58:57.981416941 CET	53	52752	8.8.8.8	192.168.2.4
Feb 23, 2021 11:59:02.791591883 CET	60542	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:59:02.850053072 CET	53	60542	8.8.8.8	192.168.2.4
Feb 23, 2021 11:59:03.247848034 CET	60689	53	192.168.2.4	8.8.8.8
Feb 23, 2021 11:59:03.298435926 CET	53	60689	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 11:58:57.843852043 CET	192.168.2.4	8.8.8.8	0x3b1b	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)
Feb 23, 2021 11:58:57.920231104 CET	192.168.2.4	8.8.8.8	0x2f23	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)
Feb 23, 2021 11:59:02.791591883 CET	192.168.2.4	8.8.8.8	0x492f	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)
Feb 23, 2021 11:59:03.247848034 CET	192.168.2.4	8.8.8.8	0x354f	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 11:58:57.903400898 CET	8.8.8.8	192.168.2.4	0x3b1b	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 11:58:57.903400898 CET	8.8.8.8	192.168.2.4	0x3b1b	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)
Feb 23, 2021 11:58:57.981416941 CET	8.8.8.8	192.168.2.4	0x2f23	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 11:58:57.981416941 CET	8.8.8.8	192.168.2.4	0x2f23	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)
Feb 23, 2021 11:59:02.850053072 CET	8.8.8.8	192.168.2.4	0x492f	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 11:59:02.850053072 CET	8.8.8.8	192.168.2.4	0x492f	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)
Feb 23, 2021 11:59:03.298435926 CET	8.8.8.8	192.168.2.4	0x354f	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 11:59:03.298435926 CET	8.8.8.8	192.168.2.4	0x354f	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)

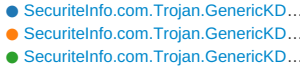
SMTP Packets

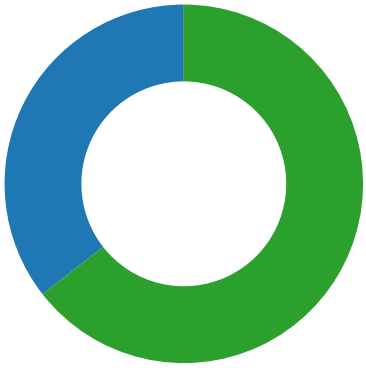
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 23, 2021 11:58:58.373878002 CET	587	49764	77.88.21.158	192.168.2.4	220 myt5-ca5ec8faf378.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru)
Feb 23, 2021 11:58:58.375708103 CET	49764	587	192.168.2.4	77.88.21.158	EHLO 405464
Feb 23, 2021 11:58:58.455749989 CET	587	49764	77.88.21.158	192.168.2.4	250-myt5-ca5ec8faf378.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 42991616 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Feb 23, 2021 11:58:58.456248999 CET	49764	587	192.168.2.4	77.88.21.158	STARTTLS
Feb 23, 2021 11:58:58.538436890 CET	587	49764	77.88.21.158	192.168.2.4	220 Go ahead
Feb 23, 2021 11:59:03.621592999 CET	587	49765	77.88.21.158	192.168.2.4	220 sas2-1cbd504aaa99.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru)
Feb 23, 2021 11:59:03.622035027 CET	49765	587	192.168.2.4	77.88.21.158	EHLO 405464
Feb 23, 2021 11:59:03.706770897 CET	587	49765	77.88.21.158	192.168.2.4	250-sas2-1cbd504aaa99.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 42991616 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Feb 23, 2021 11:59:03.711843014 CET	49765	587	192.168.2.4	77.88.21.158	STARTTLS
Feb 23, 2021 11:59:03.795093060 CET	587	49765	77.88.21.158	192.168.2.4	220 Go ahead

Code Manipulations

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe PID: 6952
Parent PID: 5876

General

Start time:	11:58:11
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe'
Imagebase:	0x1b0000
File size:	1103872 bytes
MD5 hash:	ED6841CBC5206942DD2E812F7855B156
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.652337158.0000000003679000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.651915801.0000000002671000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.651977760.00000000026AB000.00000004.00000001.sdmp, Author: Joe Security
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	6D38CF06	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	6D38CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	CreateFileW

File Written

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.GenericKDZ.73120.3552.exe.log	unknown	1314	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 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D69C907	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile

Analysis Process: SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe PID: 7020
Parent PID: 6952

General

Start time:	11:58:13

Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe
Imagebase:	0x180000
File size:	1103872 bytes
MD5 hash:	ED6841CBC5206942DD2E812F7855B156
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe PID: 7080 Parent PID: 6952

General

Start time:	11:58:14
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73120.3552.exe
Imagebase:	0x570000
File size:	1103872 bytes
MD5 hash:	ED6841CBC5206942DD2E812F7855B156
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.911990568.00000000029C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.910118958.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
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	6D38CF06	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	6D38CF06	unknown
C:\Users\user\AppData\Roaming\wqgzo1wl.s25	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\wqgzo1wl.s25\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1DBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wqgzo1wl.s25\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\wqgzo1wl.s25\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C1DDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wqgzo1wl.s25\Chrome\Default\Cookies	success or wait	1	6C1D6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wqgzo1wl.s25\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 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 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6C1DDD66	CopyFileW

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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\828336ff-45ac-41c9-ac46-f6c3d987da85	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Roaming\wqgzo1wl.s25\Chrome\Default\Cookies	unknown	16384	success or wait	2	6C1D1B4F	ReadFile

Disassembly

Code Analysis