ID: 321286
Sample Name:
SecuriteInfo.com.Trojan.PackedNET.461.20928.18265
Cookbook: default.jbs
Time: 19:25:18
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report SecuriteInfo.com.Trojan.PackedNET.461.20928.18265 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Signature Overview 5
AV Detection: 5
Networking: 5
System Summary: 5
Malware Analysis System Evasion: 5
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 11
Public 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASN 14
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 16
General 16
File Icon 16
Static PE Info 16
General 16
Entrypoint Preview 17
Data Directories 18
Sections 19

Resources 19
Imports 19
Network Behavior 19
Network Port Distribution 19
TCP Packets 19
UDP Packets 21
DNS Queries 22
DNS Answers 22
HTTPS Packets 23
SMTP Packets 24
Code Manipulations 24
Statistics 24
Behavior 24
System Behavior 24
Analysis Process: SecuriteInfo.com.Trojan.PackedNET.461.20928.exe PID: 488 Parent PID: 5552 25
General 25
File Activities 25
File Created 25
File Written 25
File Read 26
Analysis Process: RegAsm.exe PID: 5912 Parent PID: 488 26
General 26
File Activities 27
File Created 27
File Deleted 27
File Written 27
File Read 28
Registry Activities 29
Disassembly 29
Code Analysis 29

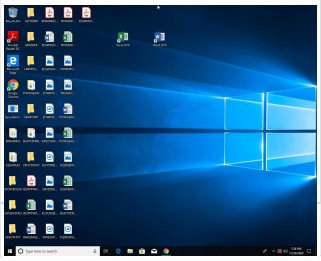
Analysis Report SecuriteInfo.com.Trojan.PackedNET.46…

Overview

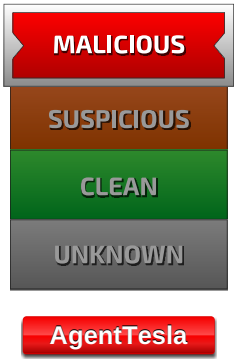
General Information

Sample Name:	SecuriteInfo.com.Trojan.PackedNET.461.20928.18265 (renamed file extension from 18265 to exe)
Analysis ID:	321286
MD5:	0daef62b8a4b65f..
SHA1:	f7151675eca0e85.
SHA256:	d859634791d000..
Tags:	AgentTesla

Most interesting Screenshot:



Detection

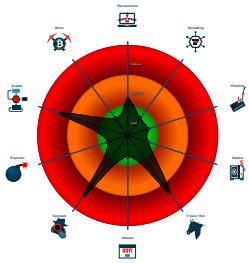


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: RegAsm connects …
- Yara detected AgentTesla
- .NET source code contains very larg…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- May check the online IP address of …
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to harvest and steal Putty / Wi…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Trojan.PackedNET.461.20928.exe (PID: 488 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.461.20928.exe' MD5: 0DAEF62B8A4B65F7CE2021E21941E32E)
  - RegAsm.exe (PID: 5912 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "=0AzrlsA",
  "URL: ": "https://2IzKMJMMUb1a8c.org",
  "To: ": "kurumsal@onurturizm.com",
  "ByHost: ": "smtp.yandex.com:587",
  "Password: ": "=0AZGzYhj",
  "From: ": "kurumsal@onurturizm.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.244849667.000000000116 1000.00000004.00000020.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.492905850.0000000002C9 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.492905850.0000000002C9 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000002.493036568.0000000002CE 5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.493036568.0000000002CE5000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 6 entries				

Unpacked PEs

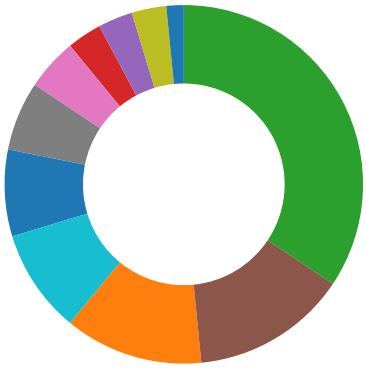
Source	Rule	Description	Author	Strings
1.2.RegAsm.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Trojan.PackedNET.461.20928.exe.55a0000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: RegAsm connects to smtp port

Signature Overview



- AV Detection
- 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:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

May check the online IP address of the machine

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

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)

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Writes to foreign memory regions

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)

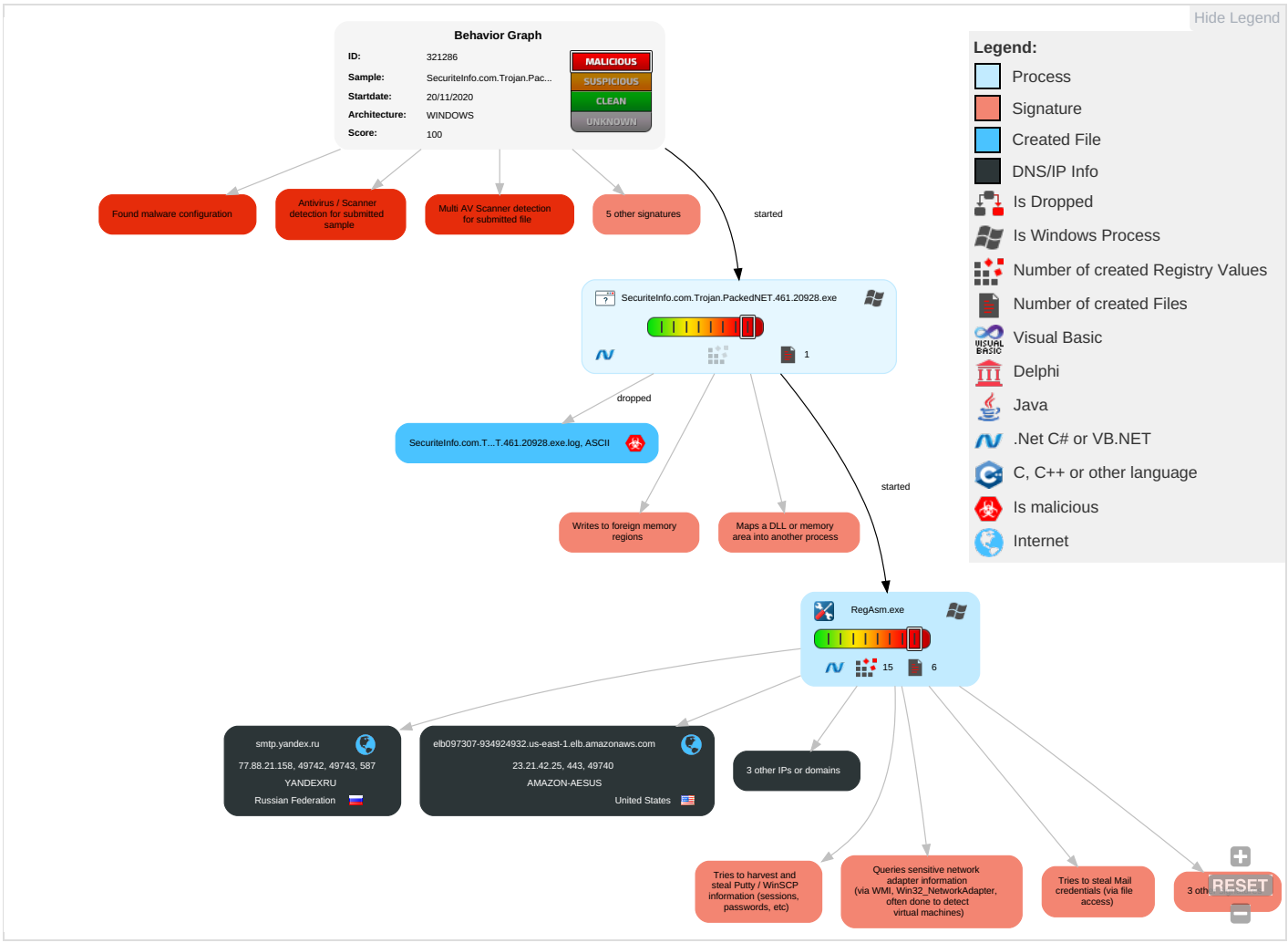
Remote Access Functionality:

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	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 2 1 2	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Security Software Discovery 1 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Virtualization/Sandbox Evasion 1 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 2 1 2	Proc Filesystem	System Network Configuration Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

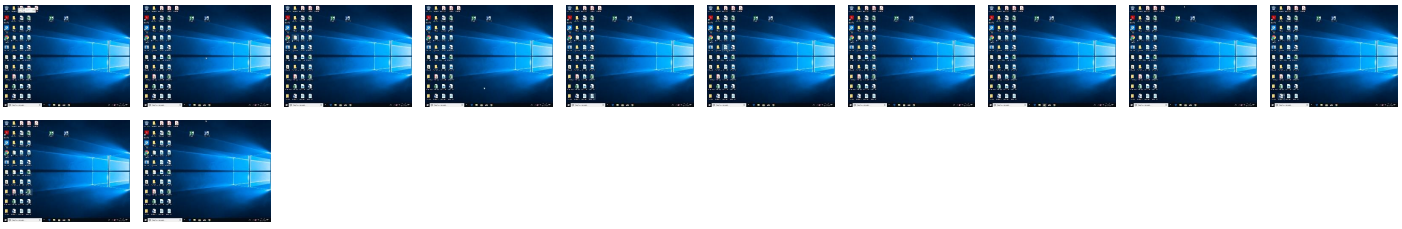
Behavior Graph



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.PackedNET.461.20928.exe	51%	Virustotal		Browse
SecuriteInfo.com.Trojan.PackedNET.461.20928.exe	52%	ReversingLabs	Win32.Trojan.Ymacco	
SecuriteInfo.com.Trojan.PackedNET.461.20928.exe	100%	Avira	TR/AD.AgentTesla.fqgqw	
SecuriteInfo.com.Trojan.PackedNET.461.20928.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.SecuriteInfo.com.Trojan.PackedNET.461.20928.exe.55a0000.1.unpack	100%	Avira	HEUR/AGEN.1138205		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	
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://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://2IzKMJMMUb1a8c.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://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	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://repository.certuqN	0%	Avira URL Cloud	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://soEqfW.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	23.21.42.25	true	false		high
smtp.yandex.ru	77.88.21.158	true	false		high
smtp.yandex.com	unknown	unknown	false		high
api.ipify.org	unknown	unknown	false		high

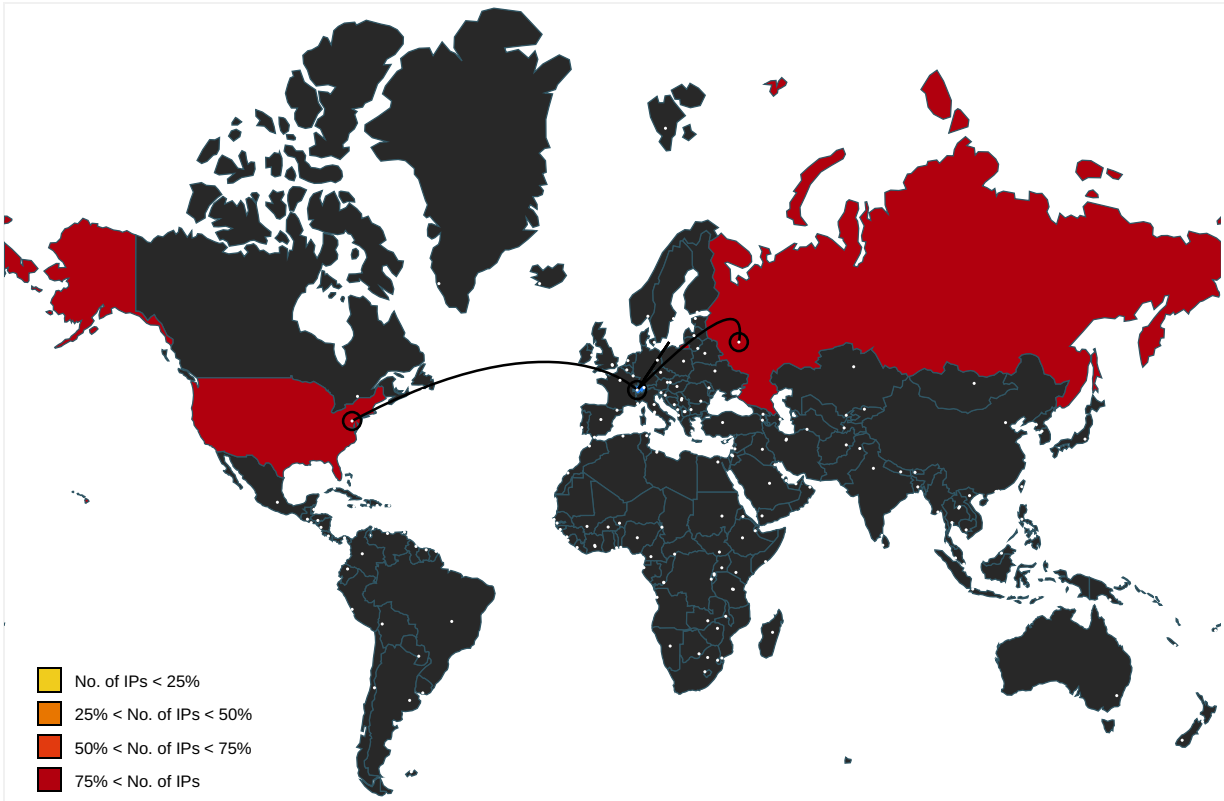
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	RegAsm.exe, 00000001.00000002.492905850.0000000002C91000.00000004.00000001.sdmp	false		high
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 00000001.00000002.492905850.0000000002C91000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegAsm.exe, 00000001.00000002.492905850.0000000002C91000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.certum.pl/ctnca.cer09	RegAsm.exe, 00000001.00000002.499365269.0000000005D8F000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegAsm.exe, 00000001.00000002.492905850.0000000002C91000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.certum.pl/ctnca.crl0k	RegAsm.exe, 00000001.00000002.499239848.0000000005D40000.00000004.00000001.sdmp	false		high
http://https://2IzKMJMMUb1a8c.org	RegAsm.exe, 00000001.00000002.493036568.0000000002CE5000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://yandex.crl.certum.pl/ycasha2.crl0q	RegAsm.exe, 00000001.00000002.499239848.0000000005D40000.00000004.00000001.sdmp	false		high
http://https://www.certum.pl/CPS0	RegAsm.exe, 00000001.00000002.499239848.0000000005D40000.00000004.00000001.sdmp	false		high
http://smtp.yandex.com	RegAsm.exe, 00000001.00000002.495319989.0000000002F49000.00000004.00000001.sdmp	false		high
http://yandex.ocsp-responder.com03	RegAsm.exe, 00000001.00000002.499239848.0000000005D40000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	RegAsm.exe, 00000001.00000002.492905850.0000000002C91000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://subca.ocsp-certum.com0.	RegAsm.exe, 00000001.00000002.499239848.0000000005D40000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://management.azure.com/Chttps://login.microsoftonline.com	SecuriteInfo.com.Trojan.PackedNET.461.20928.exe	false		high
http://repository.certum.pl/ca.cer09	RegAsm.exe, 00000001.00000002.499239848.0000000005D40000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org	RegAsm.exe, 00000001.00000002.492905850.0000000002C91000.00000004.00000001.sdmp	false		high
http://repository.certum.pl/ctnca.cer0	RegAsm.exe, 00000001.00000002.499239848.0000000005D40000.00000004.00000001.sdmp	false		high
http://https://login.microsoftonline.com	SecuriteInfo.com.Trojan.PackedNET.461.20928.exe	false		high
http://https://management.azure.com/subscriptions/	SecuriteInfo.com.Trojan.PackedNET.461.20928.exe	false		high
http://crls.yandex.net/certum/ycasha2.crl0-	RegAsm.exe, 00000001.00000002.499239848.0000000005D40000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/	SecuriteInfo.com.Trojan.PackedNET.461.20928.exe, 00000000.00000002.246909828.0000000004A46000.00000004.00000001.sdmp, RegAsm.exe, 00000001.00000002.489442244.0000000000402000.00000040.00000001.sdmp	false		high
http://subca.ocsp-certum.com01	RegAsm.exe, 00000001.00000002.499365269.0000000005D8F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://management.azure.com/	SecuriteInfo.com.Trojan.PackedNET.461.20928.exe	false		high
http://repository.certuqN	RegAsm.exe, 00000001.00000002.499239848.0000000005D40000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.certum.pl/ca.crl0h	RegAsm.exe, 00000001.00000002.499239848.0000000005D40000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	RegAsm.exe, 00000001.00000002.492905850.0000000002C91000.00000004.00000001.sdmp	false		high
http://https://secure.comodo.com/CPS0	RegAsm.exe, 00000001.00000002.499365269.0000000005D8F000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	RegAsm.exe, 00000001.00000002.492905850.0000000002C91000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	SecuriteInfo.com.Trojan.PackedNET.461.20928.exe, 00000000.00000002.246909828.0000000004A46000.00000004.00000001.sdmp, RegAsm.exe, 00000001.00000002.489442244.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certum.pl/CPS0	RegAsm.exe, 00000001.00000002.499239848.0000000005D40000.00000004.00000001.sdmp	false		high
http://soEqfW.com	RegAsm.exe, 00000001.00000002.492905850.0000000002C91000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://repository.certum.pl/ycasha2.cer0	RegAsm.exe, 00000001.00000002.499239848.0000000005D40000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.21.42.25	unknown	United States		14618	AMAZON-AESUS	false
77.88.21.158	unknown	Russian Federation		13238	YANDEXRU	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321286
Start date:	20.11.2020
Start time:	19:25:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 9s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	SecuriteInfo.com.Trojan.PackedNET.461.20928.18265 (renamed file extension from 18265 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.spyw.evad.winEXE@3/2@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.8% (good quality ratio 0.4%) • Quality average: 36.1% • Quality standard deviation: 39.1%
HCA Information:	• Successful, ratio: 100% • 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): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 13.88.21.125, 23.210.248.85, 51.104.139.180, 20.54.26.129, 8.253.95.120, 8.248.147.254, 8.248.119.254, 8.241.121.126, 8.248.115.254, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): fs.microsoft.com, arc.msn.com.nsatc.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skypedataprdcoleus17.cloudapp.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, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.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
19:26:30	API Interceptor	821x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.21.42.25	908.exe	Get hash	malicious	Browse	• api.ipify.org/
	0Oen62zpot.exe	Get hash	malicious	Browse	• api.ipify.org/
	Catalogue.exe	Get hash	malicious	Browse	• api.ipify.org/
	zMhsjuuCLk.exe	Get hash	malicious	Browse	• api.ipify.org/
77.88.21.158	CdmgSj4BO8.exe	Get hash	malicious	Browse	
	rURZ9qp1cE.exe	Get hash	malicious	Browse	
	kaeHibiTa3.exe	Get hash	malicious	Browse	
	ZBldmfU3KWpJB3r.exe	Get hash	malicious	Browse	
	RFQs.xlsm	Get hash	malicious	Browse	
	nnab.exe	Get hash	malicious	Browse	
	Purchase Order903882772.exe	Get hash	malicious	Browse	
	6266715850.xlsx	Get hash	malicious	Browse	
	Request for Quotation Commercial Offer and Official PriceList for 2020.exe	Get hash	malicious	Browse	
	cL6qhldO7O.exe	Get hash	malicious	Browse	
	PSR002330 - DURSTONE CADE S L.xlsx	Get hash	malicious	Browse	
	SWIFT.exe	Get hash	malicious	Browse	
	c9o0CtTIYT.exe	Get hash	malicious	Browse	
	MD6J6Opim9.exe	Get hash	malicious	Browse	
	New Business Inquiry Request for Quotation (MOQ and Payment Delivery Terms and Ports).exe	Get hash	malicious	Browse	
	ZYJY-2020110010 Uruguay packing list Zhongyu an.exe	Get hash	malicious	Browse	
	PI.exe	Get hash	malicious	Browse	
	Gy0RBDCf7b.exe	Get hash	malicious	Browse	
	y56pQ944uR.exe	Get hash	malicious	Browse	
	mQZgYDbf6K.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.yandex.ru	CdmgSj4BO8.exe	Get hash	malicious	Browse	• 77.88.21.158
	rURZ9qp1cE.exe	Get hash	malicious	Browse	• 77.88.21.158
	kaeHibiTa3.exe	Get hash	malicious	Browse	• 77.88.21.158
	ZBldmfU3KWpJB3r.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQs.xlsm	Get hash	malicious	Browse	• 77.88.21.158
	nnab.exe	Get hash	malicious	Browse	• 77.88.21.158
	Purchase Order903882772.exe	Get hash	malicious	Browse	• 77.88.21.158
	Proof Of Payment...Absa.exe	Get hash	malicious	Browse	• 77.88.21.158
	6266715850.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	Request for Quotation Commercial Offer and Official PriceList for 2020.exe	Get hash	malicious	Browse	• 77.88.21.158
	cL6qhldO7O.exe	Get hash	malicious	Browse	• 77.88.21.158
	PSR002330 - DURSTONE CADE S L.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	SWIFT.exe	Get hash	malicious	Browse	• 77.88.21.158
	c9o0CtTIYT.exe	Get hash	malicious	Browse	• 77.88.21.158
	MD6J6Opim9.exe	Get hash	malicious	Browse	• 77.88.21.158
	New Business Inquiry Request for Quotation (MOQ and Payment Delivery Terms and Ports).exe	Get hash	malicious	Browse	• 77.88.21.158
	ZYJY-2020110010 Uruguay packing list Zhongyu an.exe	Get hash	malicious	Browse	• 77.88.21.158
	PI.exe	Get hash	malicious	Browse	• 77.88.21.158
	Gy0RBDCf7b.exe	Get hash	malicious	Browse	• 77.88.21.158
	Xz5t2YlvYP.exe	Get hash	malicious	Browse	• 77.88.21.158
elb097307-934924932.us-east-1.elb.amazonaws.com	Defender-update-kit-x86x64.exe	Get hash	malicious	Browse	• 54.225.153.147
	http://https://largemail.r1.rpost.net/files/7xU97qcFgCvB3Uv1wDC4qvS2ZriLfublohKWA5V3/ln/en-us	Get hash	malicious	Browse	• 54.225.66.103
	ORDER.exe	Get hash	malicious	Browse	• 54.235.142.93

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Bill # 2.xlsx	Get hash	malicious	Browse	• 23.21.42.25
	PO1.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	a7UZzCVWKO.exe	Get hash	malicious	Browse	• 54.204.14.42
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 50.19.252.36
	sAPuJAvs52.exe	Get hash	malicious	Browse	• 54.243.161.145
	JlgyVmPWZr.exe	Get hash	malicious	Browse	• 174.129.214.20
	EIUOzWW2JX.exe	Get hash	malicious	Browse	• 174.129.214.20
	RVAgYSH2qh.exe	Get hash	malicious	Browse	• 54.235.142.93
	yCyc4rN0u8.exe	Get hash	malicious	Browse	• 54.235.83.248
	9cXAnovmQX.exe	Get hash	malicious	Browse	• 54.225.66.103
	T2HDck1Mmy.exe	Get hash	malicious	Browse	• 54.235.142.93
	Purchase Order.exe	Get hash	malicious	Browse	• 54.225.66.103
	Payment Advice Note from 19.11.2020.exe	Get hash	malicious	Browse	• 23.21.126.66
	phy__1__31629__2649094674__1605642612.exe	Get hash	malicious	Browse	• 23.21.126.66
	BBVA confirming Aviso de pago Eur5780201120.exe	Get hash	malicious	Browse	• 54.204.14.42
	Ejgvvuwuu8.exe	Get hash	malicious	Browse	• 54.225.169.28
	PO N0.1500243224._PDF.exe	Get hash	malicious	Browse	• 54.204.14.42

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
YANDEXRU	CdmgSj4BO8.exe	Get hash	malicious	Browse	• 77.88.21.158
	rURZ9qp1cE.exe	Get hash	malicious	Browse	• 77.88.21.158
	kaeHibiTa3.exe	Get hash	malicious	Browse	• 77.88.21.158
	ZBldmfU3KWpJB3r.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQs.xlsm	Get hash	malicious	Browse	• 77.88.21.158
	nnab.exe	Get hash	malicious	Browse	• 77.88.21.158
	Purchase Order903882772.exe	Get hash	malicious	Browse	• 77.88.21.158
	6266715850.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	Request for Quotation Commercial Offer and Official PriceList for 2020.exe	Get hash	malicious	Browse	• 77.88.21.158
	cL6qhldO7O.exe	Get hash	malicious	Browse	• 77.88.21.158
	PSR002330 - DURSTONE CADE S L.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	SWIFT.exe	Get hash	malicious	Browse	• 77.88.21.158
	c9o0CtTIYT.exe	Get hash	malicious	Browse	• 77.88.21.158
	MD6J6Opim9.exe	Get hash	malicious	Browse	• 77.88.21.158
	New Business Inquiry Request for Quotation (MOQ and Payment Delivery Terms and Ports).exe	Get hash	malicious	Browse	• 77.88.21.158
	ZYJY-2020110010 Uruguay packing list Zhongyuan.exe	Get hash	malicious	Browse	• 77.88.21.158
	PI.exe	Get hash	malicious	Browse	• 77.88.21.158
	Gy0RBDCf7b.exe	Get hash	malicious	Browse	• 77.88.21.158
	y56pQ944uR.exe	Get hash	malicious	Browse	• 77.88.21.158
	mQZgYDbf6K.exe	Get hash	malicious	Browse	• 77.88.21.158
AMAZON-AESUS	Defender-update-kit-x86x64.exe	Get hash	malicious	Browse	• 54.225.153.147
	http://https://largemail.r1.rpost.net/files/7xU97qcFgCvB3Uv1wDC4qvS2ZriLfublohKWA5V3/ln/en-us	Get hash	malicious	Browse	• 54.225.66.103
	ORDER.exe	Get hash	malicious	Browse	• 54.235.142.93
	http://s1022.t.en25.com/e/er?s=1022&lid=2184&elqTrackId=BEDFF87609C7D9DEAD041308DD8FFFB8&lb_email=bkirwer%40farbestfoods.com&elq=b095bd096fb54161953a2cf8316b5d13&elqaid=3115&elqat=1	Get hash	malicious	Browse	• 52.1.99.77
	Bill # 2.xlsx	Get hash	malicious	Browse	• 23.21.42.25
	http://https://ubereats.app.link/cwmLFZfMz5?%243p=a_custom_354088&%24deeplink_path=promo%2Fapply%3FpromoCode%3DRECONFORT7&%24desktop_url=tracking.spectrumemp.com/el?aid=8feeb968-bdd0-11e8-b27f-22000be0a14e&rid=50048635&pid=285843&cid=513&dest=overlordscan.com/cmV0by5tZXR6bGVyQGlzb2x1dGlvbnMuY2g=%23#kkowfocjoyuynaip#	Get hash	malicious	Browse	• 35.170.181.205
	BANK ACCOUNT INFO!.exe	Get hash	malicious	Browse	• 107.22.223.163
	PO1.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	http://https://rebrand.ly/zkp0y	Get hash	malicious	Browse	• 54.227.164.140
	AccountStatements.html	Get hash	malicious	Browse	• 18.209.113.162
	a7UZzCVWKO.exe	Get hash	malicious	Browse	• 54.204.14.42
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 50.19.252.36
	sAPuJAvs52.exe	Get hash	malicious	Browse	• 54.243.161.145

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	JlgyVmPWZr.exe	Get hash	malicious	Browse	• 174.129.214.20
	EIUOzWW2JX.exe	Get hash	malicious	Browse	• 174.129.214.20
	RVAgYSH2qh.exe	Get hash	malicious	Browse	• 54.235.142.93
	yCyc4rN0u8.exe	Get hash	malicious	Browse	• 54.235.83.248
	9cXAnovmQX.exe	Get hash	malicious	Browse	• 54.225.66.103
	T2HDck1Mmy.exe	Get hash	malicious	Browse	• 54.235.142.93
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 52.71.133.130

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	ARjQJiNmBs.exe	Get hash	malicious	Browse	• 23.21.42.25
	1piS4PBvBp.exe	Get hash	malicious	Browse	• 23.21.42.25
	ORDER.exe	Get hash	malicious	Browse	• 23.21.42.25
	a7UZzCVWKO.exe	Get hash	malicious	Browse	• 23.21.42.25
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 23.21.42.25
	sAPuJAvs52.exe	Get hash	malicious	Browse	• 23.21.42.25
	JlgyVmPWZr.exe	Get hash	malicious	Browse	• 23.21.42.25
	EIUOzWW2JX.exe	Get hash	malicious	Browse	• 23.21.42.25
	yCyc4rN0u8.exe	Get hash	malicious	Browse	• 23.21.42.25
	9cXAnovmQX.exe	Get hash	malicious	Browse	• 23.21.42.25
	T2HDck1Mmy.exe	Get hash	malicious	Browse	• 23.21.42.25
	Payment Advice Note from 19.11.2020.exe	Get hash	malicious	Browse	• 23.21.42.25
	PO N0.1500243224._PDF.exe	Get hash	malicious	Browse	• 23.21.42.25
	zRHI9DJ0YKIPfBX.exe	Get hash	malicious	Browse	• 23.21.42.25
	chib(1).exe	Get hash	malicious	Browse	• 23.21.42.25
	dede.exe	Get hash	malicious	Browse	• 23.21.42.25
	obi(1).exe	Get hash	malicious	Browse	• 23.21.42.25
	frc(1).exe	Get hash	malicious	Browse	• 23.21.42.25
	knitted yarn documents.exe	Get hash	malicious	Browse	• 23.21.42.25
	ano.exe	Get hash	malicious	Browse	• 23.21.42.25

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.PackedNET.461.20928.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.461.20928.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	315
Entropy (8bit):	5.350410246151501
Encrypted:	false
SSDEEP:	6:Q3La/xwcE73FKDLIP12MUAvvr3tDLIP12MUAvvR+uTL2LDY3U21v:Q3La/hg1KDLI4M9tDLI4MWuPk21v
MD5:	EE0BB4B63A030A0BF7087CB0AEBD07BC
SHA1:	9A4ADFB6336E22D49503B4B99FFC25A7882AE202
SHA-256:	6CBBAF20B7871B931A8A0B1D54890DC0E6C9ED78E7DEC5E2AB2F6D12DF349DFF
SHA-512:	47644A669A15A83D0BAA1F801BB34E36B1F8FE700E5C7A4396D684FE85AFFF6B32F511AEDD0E304DB48383E04A5044CA1B313D559737F5CD967CC00F8FDFC38B
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..

C:\Users\user\AppData\Roaming\2algnkt3.aiu\Chrome\Default\Cookies	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped

C:\Users\user\AppData\Roaming\2algnkt3.aiu\Chrome\Default\Cookies	
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	moderate, very likely benign file
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):	7.864453649536543
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SecuriteInfo.com.Trojan.PackedNET.461.20928.exe
File size:	586240
MD5:	0daef62b8a4b65f7ce2021e21941e32e
SHA1:	f7151675eca0e8523ed49af966c2d794b058517e
SHA256:	d859634791d000b01f18b3e4edc144cfb67ad9983f39d771f18ca2a4d749323b
SHA512:	413e1b44433e4c190a9dc7a29e715fb56756cb109f2a9680ad19f364805dba3587fc18aa682fd31103637358bcc3212e3c4ace2000617270d30abe31d8c88762
SSDEEP:	12288:lULVIwRue80CaPOYfBQolH/tEvoii6QxFhlCiULqyBP9DA8JHKRDT:Ur180Ca2kBfB1EAii3FhlLUXBlDA8tKR
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...|. ._..... ... .@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x49080e
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:	0x5FB4EA7C [Wed Nov 18 09:33:48 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319

General

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

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
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	0x907bc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x92000	0x242	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x94000	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

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x8e814	0x8ea00	False	0.935190827673	SysEx File - Kurzweil/Future Retro Bank 1, Channel 9	7.8686198737	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x92000	0x242	0x400	False	0.3076171875	data	3.56273769009	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x94000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

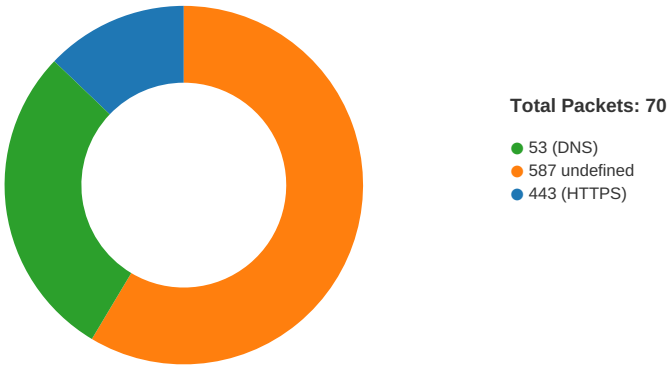
Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x92058	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 19:27:50.564285994 CET	49740	443	192.168.2.3	23.21.42.25
Nov 20, 2020 19:27:50.666688919 CET	443	49740	23.21.42.25	192.168.2.3
Nov 20, 2020 19:27:50.666794062 CET	49740	443	192.168.2.3	23.21.42.25
Nov 20, 2020 19:27:50.705985069 CET	49740	443	192.168.2.3	23.21.42.25
Nov 20, 2020 19:27:50.808331013 CET	443	49740	23.21.42.25	192.168.2.3
Nov 20, 2020 19:27:50.808360100 CET	443	49740	23.21.42.25	192.168.2.3
Nov 20, 2020 19:27:50.808373928 CET	443	49740	23.21.42.25	192.168.2.3
Nov 20, 2020 19:27:50.808386087 CET	443	49740	23.21.42.25	192.168.2.3
Nov 20, 2020 19:27:50.808402061 CET	443	49740	23.21.42.25	192.168.2.3
Nov 20, 2020 19:27:50.808476925 CET	49740	443	192.168.2.3	23.21.42.25
Nov 20, 2020 19:27:50.808545113 CET	49740	443	192.168.2.3	23.21.42.25
Nov 20, 2020 19:27:50.809530973 CET	443	49740	23.21.42.25	192.168.2.3
Nov 20, 2020 19:27:50.858505011 CET	49740	443	192.168.2.3	23.21.42.25

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 19:27:50.961071014 CET	443	49740	23.21.42.25	192.168.2.3
Nov 20, 2020 19:27:51.004965067 CET	49740	443	192.168.2.3	23.21.42.25
Nov 20, 2020 19:27:51.676534891 CET	49740	443	192.168.2.3	23.21.42.25
Nov 20, 2020 19:27:51.820050955 CET	443	49740	23.21.42.25	192.168.2.3
Nov 20, 2020 19:27:52.083458900 CET	443	49740	23.21.42.25	192.168.2.3
Nov 20, 2020 19:27:52.130053043 CET	49740	443	192.168.2.3	23.21.42.25
Nov 20, 2020 19:27:58.382222891 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:27:58.435096025 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:27:58.435312033 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:27:58.574459076 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:27:58.575035095 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:27:58.627809048 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:27:58.627840996 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:27:58.628179073 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:27:58.681076050 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:27:58.681808949 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:27:58.736090899 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:27:58.736134052 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:27:58.736150980 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:27:58.736164093 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:27:58.736346006 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:27:58.781280994 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:27:58.834579945 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:27:58.850642920 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:27:58.903578997 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:27:58.905662060 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:27:58.958583117 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:27:58.959599018 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:27:59.029395103 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:27:59.030926943 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:27:59.093538046 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:27:59.093965054 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:27:59.150490999 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:27:59.151074886 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:27:59.203895092 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:27:59.205261946 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:27:59.205394983 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:27:59.205503941 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:27:59.205594063 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:27:59.258128881 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:27:59.258172989 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:00.158128977 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:00.208794117 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.045981884 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.099844933 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.099869013 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.107911110 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.111928940 CET	49742	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.112834930 CET	49743	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.164813995 CET	587	49742	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.167136908 CET	587	49743	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.170943022 CET	49743	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.300329924 CET	587	49743	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.300682068 CET	49743	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.354933023 CET	587	49743	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.354954004 CET	587	49743	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.355289936 CET	49743	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.409542084 CET	587	49743	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.410200119 CET	49743	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.465679884 CET	587	49743	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.465708017 CET	587	49743	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.465719938 CET	587	49743	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.465733051 CET	587	49743	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.465833902 CET	49743	587	192.168.2.3	77.88.21.158

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 19:28:01.470885992 CET	49743	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.525501966 CET	587	49743	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.528270006 CET	49743	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.582700968 CET	587	49743	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.583427906 CET	49743	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.637752056 CET	587	49743	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.638557911 CET	49743	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.736917019 CET	587	49743	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.805296898 CET	587	49743	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.805823088 CET	49743	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.860151052 CET	587	49743	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.871032953 CET	587	49743	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.871562958 CET	49743	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.932570934 CET	587	49743	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.933108091 CET	49743	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.987540960 CET	587	49743	77.88.21.158	192.168.2.3
Nov 20, 2020 19:28:01.989283085 CET	49743	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.989430904 CET	49743	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.989531040 CET	49743	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.989633083 CET	49743	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.989804983 CET	49743	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.989907026 CET	49743	587	192.168.2.3	77.88.21.158
Nov 20, 2020 19:28:01.989984035 CET	49743	587	192.168.2.3	77.88.21.158

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 19:26:09.126458883 CET	53195	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:26:09.153629065 CET	53	53195	8.8.8.8	192.168.2.3
Nov 20, 2020 19:26:10.941152096 CET	50141	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:26:10.968161106 CET	53	50141	8.8.8.8	192.168.2.3
Nov 20, 2020 19:26:11.726533890 CET	53023	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:26:11.762157917 CET	53	53023	8.8.8.8	192.168.2.3
Nov 20, 2020 19:26:13.240852118 CET	49563	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:26:13.268037081 CET	53	49563	8.8.8.8	192.168.2.3
Nov 20, 2020 19:26:14.097101927 CET	51352	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:26:14.124253988 CET	53	51352	8.8.8.8	192.168.2.3
Nov 20, 2020 19:26:15.263859987 CET	59349	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:26:15.290884018 CET	53	59349	8.8.8.8	192.168.2.3
Nov 20, 2020 19:26:16.464489937 CET	57084	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:26:16.491749048 CET	53	57084	8.8.8.8	192.168.2.3
Nov 20, 2020 19:26:17.558891058 CET	58823	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:26:17.586014986 CET	53	58823	8.8.8.8	192.168.2.3
Nov 20, 2020 19:26:36.424998999 CET	57568	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:26:36.465370893 CET	53	57568	8.8.8.8	192.168.2.3
Nov 20, 2020 19:26:37.404459953 CET	50540	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:26:37.431592941 CET	53	50540	8.8.8.8	192.168.2.3
Nov 20, 2020 19:26:53.655304909 CET	54366	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:26:53.682466030 CET	53	54366	8.8.8.8	192.168.2.3
Nov 20, 2020 19:26:57.386756897 CET	53034	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:26:57.424304008 CET	53	53034	8.8.8.8	192.168.2.3
Nov 20, 2020 19:27:11.445118904 CET	57762	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:27:11.472172976 CET	53	57762	8.8.8.8	192.168.2.3
Nov 20, 2020 19:27:15.825259924 CET	55435	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:27:15.862520933 CET	53	55435	8.8.8.8	192.168.2.3
Nov 20, 2020 19:27:48.603758097 CET	50713	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:27:48.630809069 CET	53	50713	8.8.8.8	192.168.2.3
Nov 20, 2020 19:27:50.072036028 CET	56132	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:27:50.099030972 CET	53	56132	8.8.8.8	192.168.2.3
Nov 20, 2020 19:27:50.115535021 CET	58987	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:27:50.142608881 CET	53	58987	8.8.8.8	192.168.2.3
Nov 20, 2020 19:27:54.529968023 CET	56579	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:27:54.565705061 CET	53	56579	8.8.8.8	192.168.2.3
Nov 20, 2020 19:27:58.301122904 CET	60633	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 19:27:58.336817980 CET	53	60633	8.8.8.8	192.168.2.3
Nov 20, 2020 19:27:58.344650030 CET	61292	53	192.168.2.3	8.8.8.8
Nov 20, 2020 19:27:58.380335093 CET	53	61292	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 19:27:50.072036028 CET	192.168.2.3	8.8.8.8	0xc48a	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:50.115535021 CET	192.168.2.3	8.8.8.8	0xa752	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:58.301122904 CET	192.168.2.3	8.8.8.8	0x5c2b	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:58.344650030 CET	192.168.2.3	8.8.8.8	0xb5c2	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
Nov 20, 2020 19:27:50.099030972 CET	8.8.8.8	192.168.2.3	0xc48a	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 19:27:50.099030972 CET	8.8.8.8	192.168.2.3	0xc48a	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 19:27:50.099030972 CET	8.8.8.8	192.168.2.3	0xc48a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.42.25	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:50.099030972 CET	8.8.8.8	192.168.2.3	0xc48a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:50.099030972 CET	8.8.8.8	192.168.2.3	0xc48a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:50.099030972 CET	8.8.8.8	192.168.2.3	0xc48a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.204.14.42	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:50.099030972 CET	8.8.8.8	192.168.2.3	0xc48a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.28	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:50.099030972 CET	8.8.8.8	192.168.2.3	0xc48a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:50.099030972 CET	8.8.8.8	192.168.2.3	0xc48a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.182.194	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:50.099030972 CET	8.8.8.8	192.168.2.3	0xc48a	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:50.142608881 CET	8.8.8.8	192.168.2.3	0xa752	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 19:27:50.142608881 CET	8.8.8.8	192.168.2.3	0xa752	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 19:27:50.142608881 CET	8.8.8.8	192.168.2.3	0xa752	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 19:27:50.142608881 CET	8.8.8.8	192.168.2.3	0xa752	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.161.145	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:50.142608881 CET	8.8.8.8	192.168.2.3	0xa752	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.28	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:50.142608881 CET	8.8.8.8	192.168.2.3	0xa752	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		184.73.247.141	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:50.142608881 CET	8.8.8.8	192.168.2.3	0xa752	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:50.142608881 CET	8.8.8.8	192.168.2.3	0xa752	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:50.142608881 CET	8.8.8.8	192.168.2.3	0xa752	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:50.142608881 CET	8.8.8.8	192.168.2.3	0xa752	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.42.25	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:58.336817980 CET	8.8.8.8	192.168.2.3	0x5c2b	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 19:27:58.336817980 CET	8.8.8.8	192.168.2.3	0x5c2b	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)
Nov 20, 2020 19:27:58.380335093 CET	8.8.8.8	192.168.2.3	0xb5c2	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 19:27:58.380335093 CET	8.8.8.8	192.168.2.3	0xb5c2	No error (0)	smtp.yandex.ru		77.88.21.158	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
Nov 20, 2020 19:27:50.809530973 CET	23.21.42.25	443	192.168.2.3	49740	CN=*.ipify.org, OU=PositiveSSL Wildcard, OU=Domain Control Validated CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jan 24 01:00:00 CET 2018 Wed Feb 12 01:00:00 CET 2014 Tue Jan 19 01:00:00 CET 2010	Sun Jan 24 00:59:59 CET 2021 Mon Feb 12 00:59:59 CET 2029 Tue Jan 19 00:59:59 CET 2038	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Feb 12 01:00:00 CET 2014	Mon Feb 12 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 19 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		

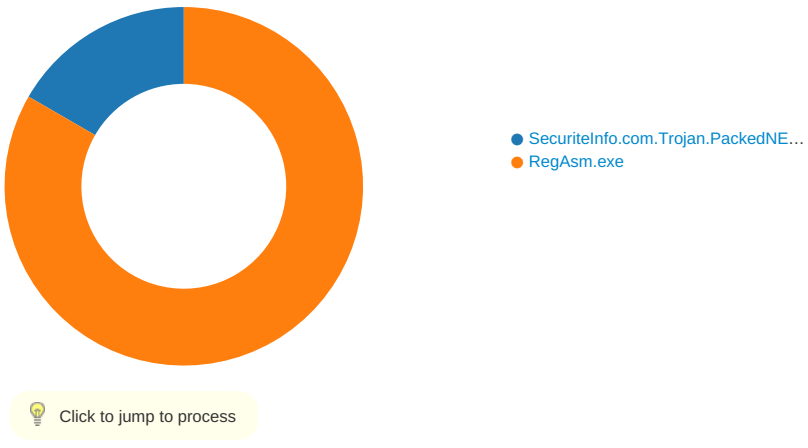
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 20, 2020 19:27:58.574459076 CET	587	49742	77.88.21.158	192.168.2.3	220 iva4-bca95d3b11b1.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru)
Nov 20, 2020 19:27:58.575035095 CET	49742	587	192.168.2.3	77.88.21.158	EHLO 287400
Nov 20, 2020 19:27:58.627840996 CET	587	49742	77.88.21.158	192.168.2.3	250-iva4-bca95d3b11b1.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 42991616 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Nov 20, 2020 19:27:58.628179073 CET	49742	587	192.168.2.3	77.88.21.158	STARTTLS
Nov 20, 2020 19:27:58.681076050 CET	587	49742	77.88.21.158	192.168.2.3	220 Go ahead
Nov 20, 2020 19:28:01.300329924 CET	587	49743	77.88.21.158	192.168.2.3	220 vla5-47b3f4751bc4.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru)
Nov 20, 2020 19:28:01.300682068 CET	49743	587	192.168.2.3	77.88.21.158	EHLO 287400
Nov 20, 2020 19:28:01.354954004 CET	587	49743	77.88.21.158	192.168.2.3	250-vla5-47b3f4751bc4.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 42991616 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Nov 20, 2020 19:28:01.355289936 CET	49743	587	192.168.2.3	77.88.21.158	STARTTLS
Nov 20, 2020 19:28:01.409542084 CET	587	49743	77.88.21.158	192.168.2.3	220 Go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.PackedNET.461.20928.exe PID: 488 Parent PID: 5552

General

Start time:	19:26:14
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.461.20928.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PackedNET.461.20928.exe'
Imagebase:	0xa50000
File size:	586240 bytes
MD5 hash:	0DAEF62B8A4B65F7CE2021E21941E32E
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: 00000000.00000002.244849667.0000000001161000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.246909828.0000000004A46000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.248059193.00000000055A2000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.PackedNET.461.20928.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E19C78D	CreateFileW

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.PackedNET.461.20928.exe.log	unknown	315	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 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 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 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	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_3	success or wait	1	6E19C907	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	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE65705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE6CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDC03DE	ReadFile

Analysis Process: RegAsm.exe PID: 5912 Parent PID: 488

General

Start time:	19:26:21
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x7d0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
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: 00000001.00000002.492905850.0000000002C91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.492905850.0000000002C91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.493036568.0000000002CE5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.493036568.0000000002CE5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.489442244.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

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	6DE8CF06	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	6DE8CF06	unknown
C:\Users\user\AppData\Roaming\2algnkt3.aiu	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CCDBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\2algnkt3.aiu\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	6CCDBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\2algnkt3.aiu\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	6CCDBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\2algnkt3.aiu\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	6CCDDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\2algnkt3.aiu\Chrome\Default\Cookies	success or wait	1	6CCD6A95	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\Roaming\2algnkt3.aiu\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 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	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6CCDDD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE65705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6DE6CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6DE6CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE6CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6CCD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6CCD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6DE65705	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CCD1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CCD1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CCD1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CCD1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\9213d628-6bf6-4a90-a728-1f854fb2c264	unknown	4096	success or wait	1	6CCD1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CCD1B4F	ReadFile
C:\Users\user\AppData\Roaming\2algnkt3.aiu\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CCD1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis