ID: 249929
Sample Name:
SecuriteInfo.com.Generic.mg.5930091b65aed962.29544
Cookbook: default.jbs
Time: 08:08:28
Date: 23/07/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

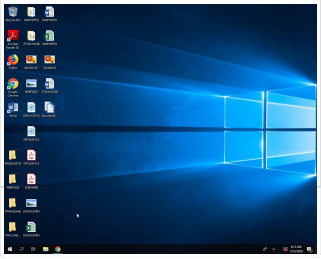
Analysis Report SecuriteInfo.com.Generic.mg.5930091b…

Overview

General Information

Sample Name:	SecuriteInfo.com.Generic.mg.5930091b65aed962.29544 (renamed file extension from 29544 to exe)
Analysis ID:	249929
MD5:	5930091b65aed9..
SHA1:	1e6ee2e805e21c..
SHA256:	91beb7c43da3dd..

Most interesting Screenshot:



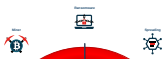
Detection

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected Trickbot
- Allocates memory in foreign process…
- Delayed program exit found
- Machine Learning detection for samp…
- Tries to detect virtualization through…
- Writes to foreign memory regions
- Contains functionality for execution …
- Contains functionality to access load…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Generic.mg.5930091b65aed962.exe (PID: 3124 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.5930091b65aed962.exe' MD5: 5930091B65AED9627DD1A4E86458B72F)
  - wermgr.exe (PID: 3092 cmdline: C:\Windows\system32\wermgr.exe MD5: FF214585BF10206E21EA8EBA202FACFD)
- **cleanup**

Malware Configuration

Threatname: Trickbot

```
{
  "gtag": "tot773",
  "C2 list": [
    "10.232.76.39:449",
    "12.50.6.122:449",
    "110.50.84.5:449",
    "36.91.45.10:449",
    "185.90.61.9:443",
    "5.1.81.68:443",
    "185.99.2.66:443",
    "45.6.16.68:449",
    "185.99.2.65:443",
    "181.129.104.139:449",
    "91.235.129.20:443",
    "190.136.178.52:449",
    "36.89.182.225:449",
    "182.253.113.67:449",
    "134.119.191.21:443",
    "51.81.112.144:443",
    "103.111.83.246:449",
    "194.5.250.121:443",
    "192.3.247.123:443",
    "36.66.218.117:449",
    "36.92.19.205:449",
    "85.204.116.216:443",
    "122.50.6.122:449",
    "78.108.216.47:443",
    "134.119.191.11:443",
    "185.14.31.104:443",
    "95.171.16.42:443",
    "110.232.76.39:449",
    "36.89.243.241:449",
    "131.161.253.190:449",
    "200.107.35.154:449",
    "85.204.116.100:443",
    "181.112.157.42:449",
    "80.210.32.67:449",
    "121.100.19.18:449",
    "103.12.161.194:449",
    "107.175.72.141:443",
    "181.129.134.18:449",
    "110.93.15.98:449"
  ],
  "modules": [
    "pwgrab",
    "mcconf"
  ]
}
```


Yara Overview

Memory Dumps

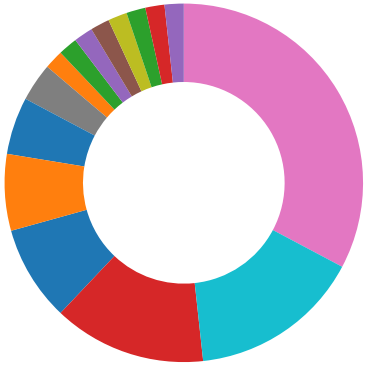
Source	Rule	Description	Author	Strings
00000001.00000002.1225534063.00000211666 4E000.00000004.00000020.sdmp	JoeSecurity_Trickbot_1	Yara detected Trickbot	Joe Security	
Process Memory Space: wermgr.exe PID: 3092	JoeSecurity_Trickbot_1	Yara detected Trickbot	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing



- E-Banking Fraud
- 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 domain / URL
- Multi AV Scanner detection for submitted file
- Yara detected Trickbot
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

E-Banking Fraud:

- Yara detected Trickbot

Malware Analysis System Evasion:

- Delayed program exit found
- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

- Allocates memory in foreign processes
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected Trickbot

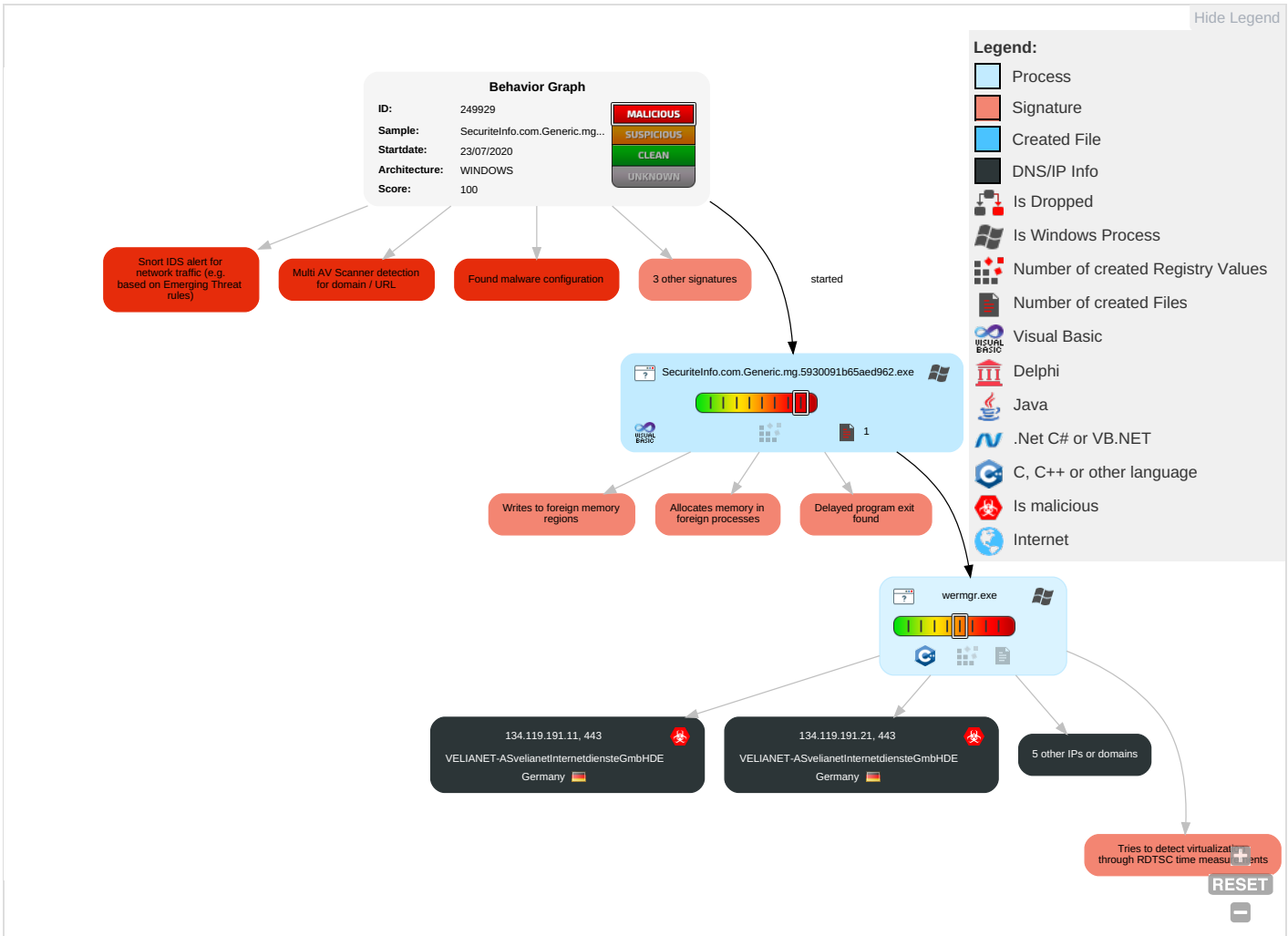
Remote Access Functionality:

- Yara detected Trickbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effe
Valid Accounts	Windows Remote Management	Winlogon Helper DLL	Access Token Manipulation 1	Virtualization/Sandbox Evasion 1	Input Capture 1	Virtualization/Sandbox Evasion 1	Application Deployment Software	Input Capture 1	Data Encrypted 1	Uncommonly Used Port 1	Eave Inse Netv Com
Replication Through Removable Media	Service Execution	Port Monitors	Process Injection 2 1 2	Access Token Manipulation 1	Network Sniffing	Process Discovery 2	Remote Services	Data from Removable Media	Exfiltration Over Other Network Medium	Standard Cryptographic Protocol 1 2	Expl Red Call
External Remote Services	Windows Management Instrumentation	Accessibility Features	Path Interception	Process Injection 2 1 2	Input Capture	Application Window Discovery 1	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Standard Application Layer Protocol 1	Expl Trac Loca
Drive-by Compromise	Scheduled Task	System Firmware	DLL Search Order Hijacking	Obfuscated Files or Information 2	Credentials in Files	Security Software Discovery 1 1 1	Logon Scripts	Input Capture	Data Encrypted	Multiband Communication	SIM Swa
Exploit Public-Facing Application	Command-Line Interface	Shortcut Modification	File System Permissions Weakness	Masquerading	Account Manipulation	System Network Configuration Discovery 1	Shared Webroot	Data Staged	Scheduled Transfer	Standard Cryptographic Protocol	Man Dev Com
Spearphishing Link	Graphical User Interface	Modify Existing Service	New Service	DLL Search Order Hijacking	Brute Force	File and Directory Discovery 2	Third-party Software	Screen Capture	Data Transfer Size Limits	Commonly Used Port	Jam Den Serv
Spearphishing Attachment	Scripting	Path Interception	Scheduled Task	Software Packing	Two-Factor Authentication Interception	System Information Discovery 1 1 2	Pass the Hash	Email Collection	Exfiltration Over Command and Control Channel	Uncommonly Used Port	Rog Acc

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.Generic.mg.5930091b65aed962.exe	20%	Virustotal		Browse
SecuriteInfo.com.Generic.mg.5930091b65aed962.exe	19%	ReversingLabs		
SecuriteInfo.com.Generic.mg.5930091b65aed962.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.SecuriteInfo.com.Generic.mg.5930091b65aed962.exe.2180000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.SecuriteInfo.com.Generic.mg.5930091b65aed962.exe.21b0000.3.unpack	100%	Avira	HEUR/AGEN.1002615		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.myhomepage.com	0%	Virustotal		Browse
http://https://134.119.191.11//	10%	Virustotal		Browse
http://https://sectigo.com/CPS0	0%	Virustotal		Browse
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://185.90.61.9/	9%	Virustotal		Browse
http://https://134.119.191.21/	9%	Virustotal		Browse
http://https://134.119.191.11/	10%	Virustotal		Browse
http://https://85.204.116.216/	8%	Virustotal		Browse
http://https://185.99.2.66/	9%	Virustotal		Browse
http://https://45.6.16.68:449/	6%	Virustotal		Browse

Domains and IPs

Contacted Domains

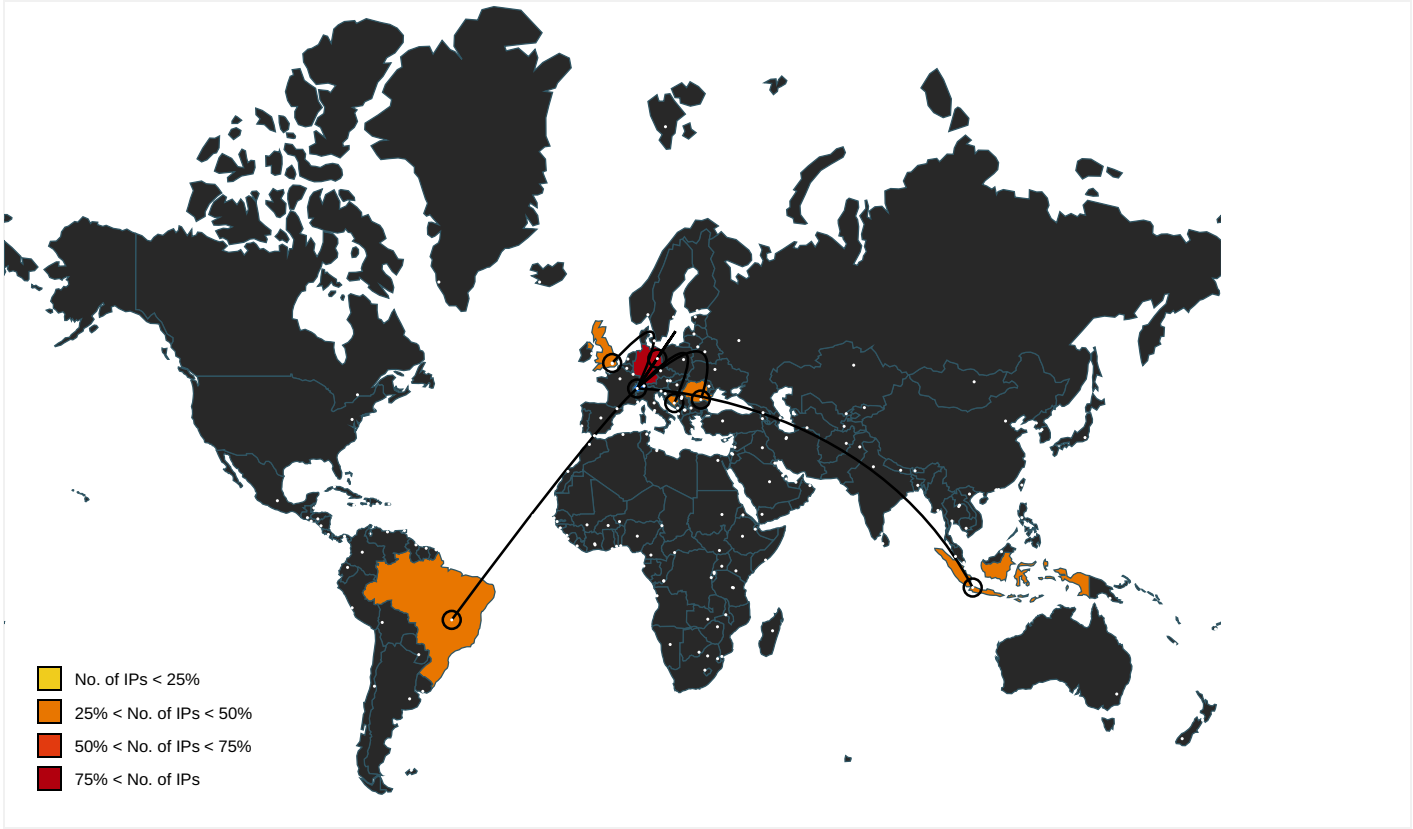
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.myhomepage.com	SecuriteInfo.com.Generic.mg.5930091b65aed962.exe	false	• 0%, Virustotal, Browse	unknown
http://https://134.119.191.11//	wermgr.exe, 00000001.00000002.1226012983.000002116682F000.00000004.00000001.sdmp	true	• 10%, Virustotal, Browse	unknown
http://https://134.119.191.21/O	wermgr.exe, 00000001.00000002.1226012983.000002116682F000.00000004.00000001.sdmp	true		unknown
http://https://134.119.191.21:443/tot773/301389_W10017134.98540ECEF76EAED1911CDE564F5F2CC7/5/spk/	wermgr.exe, 00000001.00000002.1225985319.0000021166820000.00000004.00000001.sdmp	false		unknown
http://https://45.6.16.68:449/tot773/301389_W10017134.98540ECEF76EAED1911CDE564F5F2CC7/5/spk/	wermgr.exe, 00000001.00000002.1225985319.0000021166820000.00000004.00000001.sdmp	true		unknown
http://https://sectigo.com/CPS0	wermgr.exe, 00000001.00000002.1225985319.0000021166820000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • URL Reputation: safe • URL Reputation: safe	low
http://https://185.90.61.9/	wermgr.exe, 00000001.00000002.1226012983.000002116682F000.00000004.00000001.sdmp	true	• 9%, Virustotal, Browse	unknown
http://https://134.119.191.11/7	wermgr.exe, 00000001.00000002.1226012983.000002116682F000.00000004.00000001.sdmp	true		unknown
http://https://134.119.191.11/W	wermgr.exe, 00000001.00000002.1226012983.000002116682F000.00000004.00000001.sdmp	true		unknown
http://https://185.90.61.9/s	wermgr.exe, 00000001.00000002.1226012983.000002116682F000.00000004.00000001.sdmp	true		unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://134.119.191.21/	wermgr.exe, 00000001.00000002.1226012983.000002116682F000.00000004.00000001.sdmp	true	• 9%, Virustotal, Browse	unknown
http://https://185.90.61.9/9/#	wermgr.exe, 00000001.00000002.1226012983.000002116682F000.00000004.00000001.sdmp	true		unknown
http://https://134.119.191.11/	wermgr.exe, 00000001.00000002.1226012983.000002116682F000.00000004.00000001.sdmp	true	• 10%, Virustotal, Browse	unknown
http://https://134.119.191.21/tot773/301389_W10017134.98540ECEF76EAED1911CDE564F5F2CC7/5/spk/%	wermgr.exe, 00000001.00000002.1226012983.000002116682F000.00000004.00000001.sdmp	true		unknown
http://https://85.204.116.216/	wermgr.exe, 00000001.00000002.1226012983.000002116682F000.00000004.00000001.sdmp	true	• 8%, Virustotal, Browse	unknown
http://https://185.99.2.66/	wermgr.exe, 00000001.00000002.1225942911.0000021166804000.00000004.00000001.sdmp	true	• 9%, Virustotal, Browse	unknown
http://https://134.119.191.11/tot773/301389_W10017134.98540ECEF76EAED1911CDE564F5F2CC7/5/spk/	wermgr.exe, 00000001.00000002.1225534063.000002116664E000.00000004.00000020.sdmp	true		unknown
http://https://185.90.61.9/o	wermgr.exe, 00000001.00000002.1226012983.000002116682F000.00000004.00000001.sdmp	true		unknown
http://https://134.119.191.21/tot773/301389_W10017134.98540ECEF76EAED1911CDE564F5F2CC7/5/spk/	wermgr.exe, 00000001.00000002.1225534063.000002116664E000.00000004.00000020.sdmp	true		unknown
http://https://45.6.16.68:449/	wermgr.exe, 00000001.00000002.1226012983.000002116682F000.00000004.00000001.sdmp	true	• 6%, Virustotal, Browse	unknown

Contacted IPs



Public

IP	Country	Flag	ASN	ASN Name	Malicious
45.6.16.68	Brazil		266119	FOXLINK-INTERNETEACESSORIOSLTDABR	true
110.232.76.39	Indonesia		138841	GROOVY-AS-IDPTMediaAndalanNusaID	true
185.99.2.66	Bosnia and Herzegowina		200698	GLOBALHOST-BOSNIA-ASBA	true
185.90.61.9	United Kingdom		136258	ONEPROVIDER-ASBrainStormNetworkIncCA	true

IP	Country	Flag	ASN	ASN Name	Malicious
134.119.191.21	Germany		29066	VELIANET-ASvelianetInternetdiensteGmbHDE	true
134.119.191.11	Germany		29066	VELIANET-ASvelianetInternetdiensteGmbHDE	true
85.204.116.216	Romania		48874	HOSTMAZEHOSTMAZERO	true

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	249929
Start date:	23.07.2020
Start time:	08:08:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Generic.mg.5930091b65aed962.29544 (renamed file extension from 29544 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit (version 1803) with **Office 2016**, Adobe Reader DC 19, Chrome 70, Firefox 63, Java 8.171, Flash 30.0.0.113
Number of analysed new started processes analysed:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@3/0@0/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.6% (good quality ratio 3.7%) • Quality average: 47.8% • Quality standard deviation: 29.6%
HCA Information:	• Successful, ratio: 74% • 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, wermgr.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, conhost.exe, UsoClient.exe

Simulations

Behavior and APIs

Time	Type	Description
08:10:43	API Interceptor	6x Sleep call for process: wermgr.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.6.16.68	2585a01938abgs[1].exe	Get hash	malicious	Browse	
	table_workbook_74.xls	Get hash	malicious	Browse	
185.99.2.66	Proof of Delivery_6.xls	Get hash	malicious	Browse	
185.90.61.9	Certificate.xls	Get hash	malicious	Browse	
	Bill_00062596084.xls	Get hash	malicious	Browse	
	http://https://files.constantcontact.com/5b991e10301/e57d900a-9f5d-4833-a4dd-e1f2e7df9d17.xls	Get hash	malicious	Browse	
	http://https://mapcovid.info/covidbase.jar	Get hash	malicious	Browse	
	Invoice file 356.doc	Get hash	malicious	Browse	
134.119.191.21	ZVKeVLZ.exe	Get hash	malicious	Browse	
	2585a01938abgs[1].exe	Get hash	malicious	Browse	
	Invoice file 356.doc	Get hash	malicious	Browse	
134.119.191.11	ZVKeVLZ.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ONEPROVIDER-ASBrainStormNetworkIncCA	Certificate.xls	Get hash	malicious	Browse	• 185.90.61.9
GLOBALHOST-BOSNIA-ASBA	ZVKeVLZ.exe	Get hash	malicious	Browse	• 185.99.2.65
	IRS_6880089.xls	Get hash	malicious	Browse	• 185.99.2.83
	IRS_6880089.xls	Get hash	malicious	Browse	• 185.99.2.83
	tXDaYJGfDS.xls	Get hash	malicious	Browse	• 185.99.2.83
	tXDaYJGfDS.xls	Get hash	malicious	Browse	• 185.99.2.83
	Proof of Delivery_6.xls	Get hash	malicious	Browse	• 185.99.2.66
	19SCB pmtswift0009856491011201.exe	Get hash	malicious	Browse	• 185.99.1.225
	71dhl_doc058689201711031201.exe	Get hash	malicious	Browse	• 185.99.1.225
	http://turnoutasmirsa.com/file/holanew.exe	Get hash	malicious	Browse	• 185.99.2.100
	39STATEMENT OF ACCOUNT 10-16-201.exe	Get hash	malicious	Browse	• 185.99.1.225
	69TNT.Doc557.exe	Get hash	malicious	Browse	• 185.99.1.225
	53TNT.Doc.2345x.exe	Get hash	malicious	Browse	• 185.99.1.225
	26C & F DE LA ORDE.exe	Get hash	malicious	Browse	• 185.99.1.225
VELIANET-ASvelianetInternetdiensteGmbHDE	AD.exe	Get hash	malicious	Browse	• 185.136.157.95
	http://https://is.gd/8Mrb8B	Get hash	malicious	Browse	• 92.204.167.242
	ZVKeVLZ.exe	Get hash	malicious	Browse	• 134.119.191.11
	Quotation RFQ010720-B.jar	Get hash	malicious	Browse	• 185.136.165.173
	Quotation RFQ010720-B.jar	Get hash	malicious	Browse	• 185.136.165.173
	IRS_Tax_5522181.xls	Get hash	malicious	Browse	• 134.119.191.48
	IRS_Tax_5522181.xls	Get hash	malicious	Browse	• 134.119.191.48
	http://business.comcast.com/myaccount	Get hash	malicious	Browse	• 185.19.219.27
	ReNP0w3ELZ.xls	Get hash	malicious	Browse	• 134.119.189.10
	ReNP0w3ELZ.xls	Get hash	malicious	Browse	• 134.119.189.10
	Payroll.xls	Get hash	malicious	Browse	• 134.119.189.10
	Payroll.xls	Get hash	malicious	Browse	• 134.119.189.10
	Payroll.xls	Get hash	malicious	Browse	• 134.119.189.10
	Payroll.xls	Get hash	malicious	Browse	• 134.119.189.10
	41payment invoic.exe	Get hash	malicious	Browse	• 146.0.252.20
	facture_27-06-18.exe	Get hash	malicious	Browse	• 134.119.179.55
	qBgLOEyqvk.doc	Get hash	malicious	Browse	• 134.119.189.10
	qBgLOEyqvk.doc	Get hash	malicious	Browse	• 134.119.189.10
	12Payment Transfer Slip =5419.exe	Get hash	malicious	Browse	• 37.49.224.219
	Request_592655.doc	Get hash	malicious	Browse	• 134.119.217.250

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
8916410db85077a5460817142dcbc8de	Bill_00062596084.xls	Get hash	malicious	Browse	• 185.99.2.66
	U7TR307hvX.exe	Get hash	malicious	Browse	• 185.99.2.66
	rdf.exe	Get hash	malicious	Browse	• 185.99.2.66
	aMbMD2aEat.xlsm	Get hash	malicious	Browse	• 185.99.2.66
	Info_181338267653.doc	Get hash	malicious	Browse	• 185.99.2.66
	019914252.xlsm	Get hash	malicious	Browse	• 185.99.2.66
	INV878237.doc	Get hash	malicious	Browse	• 185.99.2.66
	jucheck.exe	Get hash	malicious	Browse	• 185.99.2.66
	jer2u4ewLe.jse	Get hash	malicious	Browse	• 185.99.2.66
	jer2u4ewLe.jse	Get hash	malicious	Browse	• 185.99.2.66
	komppa.jse	Get hash	malicious	Browse	• 185.99.2.66
	target.jse	Get hash	malicious	Browse	• 185.99.2.66
	target.jse	Get hash	malicious	Browse	• 185.99.2.66
	shell.jse	Get hash	malicious	Browse	• 185.99.2.66
	TrialDesign.jse	Get hash	malicious	Browse	• 185.99.2.66
	TrialDesign.jse	Get hash	malicious	Browse	• 185.99.2.66
	TranLB.jse	Get hash	malicious	Browse	• 185.99.2.66
	ADD And 6934631.jse	Get hash	malicious	Browse	• 185.99.2.66
	ADD And 6934631.jse	Get hash	malicious	Browse	• 185.99.2.66
	9-24 without edits.jse	Get hash	malicious	Browse	• 185.99.2.66

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.827170209757444
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Generic.mg.5930091b65aed962.exe
File size:	540724
MD5:	5930091b65aed9627dd1a4e86458b72f
SHA1:	1e6ee2e805e21c007aa70217856bf31141ccc552
SHA256:	91beb7c43da3dd723c9d44629ab656b4f913c5ec111d1d362279938645f7edd3
SHA512:	f35dbf5ab53eb9f94e72e75cc068e83b8a819b215f47245431887f124fd9903e45134771252cd19beedfb0d3697781d4aeebf7f98cfb8e24eede6e399527a146
SSDEEP:	6144:QXRZwJkHAfrJoz9KnjY/F0eAcLeRpJ0ulEypWu/blRTZSMIbBkfoqpArjO:QXRZmrJoBKIqkapJDmy4uBRTQ4pD
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....]..... .....p.....Rich.....PE..L...07._..... .....0.....|H.....@....@

File Icon

Icon Hash:	7efef2faeaeae8c8

Static PE Info

General

Entrypoint:	0x40487c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5F183730 [Wed Jul 22 12:55:12 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	a9daf8a064784a80002aa6baaea5ce3b

Entrypoint Preview

Instruction
push 004080BCh
call 00007F56E479A8B5h
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], dh
add byte ptr [eax], al
add byte ptr [eax], bh
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [edx-1Eh], dl
daa

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x52b94	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x56000	0x2ef38	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1260	0x1c	.text
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	0x238	0x48	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x254	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x525e8	0x53000	False	0.277993811182	data	5.83763004179	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x54000	0x1ac4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x56000	0x2ef38	0x2f000	False	0.956028715093	data	7.89484809259	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x562e8	0x2c8	GLS_BINARY_LSB_FIRST	Greek	Greece
RT_ICON	0x565b0	0x568	GLS_BINARY_LSB_FIRST		
RT_STRING	0x56b18	0x38	data		
RT_STRING	0x56b50	0x44	data		
RT_STRING	0x56b94	0x5c	data		
RT_STRING	0x56bf0	0x28	data		
RT_STRING	0x56c18	0x16c	data		
RT_STRING	0x56d84	0x28	data		
RT_STRING	0x56dac	0x5c	data		
RT_GROUP_ICON	0x56e08	0x14	data		
RT_VERSION	0x56e1c	0x3a4	data	English	United States
RT_HTML	0x571c0	0x2dd77	data	English	United States

Imports

DLL	Import
oleaut32.dll	SysAllocStringLen
kernel32.dll	VirtualAlloc
MSVBVM60.DLL	__vbaVarSub, __vbaStrI2, _CIcos, _adj_fptan, __vbaVarMove, __vbaVarVargNofree, __vbaAryMove, __vbaFreeVar, __vbaGosubReturn, __vbaLenBstr, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaRaiseEvent, __vbaFreeObjList, _adj_fprem1, __vbaResume, __vbaCopyBytes, __vbaStrCat, __vbaLsetFixstr, __vbaSetSystemError, __vbaHresultCheckObj, __vbaLenVar, _adj_fdiv_m32, __vbaAryDestruct, __vbaExitProc, __vbaI4Abs, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaBoolVar, __vbaRefVarAry, __vbaFpR8, __vbaVarTstLt, __vbaBoolVarNull, _CIsin, __vbaErase, __vbaVargVarMove, __vbaChkstk, __vbaCyVar, __vbaGosubFree, EVENT_SINK_AddRef, __vbaStrCmp, __vbaAryConstruct2, __vbaVarTstEq, __vbaI2I4, __vbaPrintObj, DllFunctionCall, __vbaVarLateMemSt, __vbaCastObjVar, __vbaRedimPreserve, __vbaStrR4, _adj_fpatan, __vbaR4Var, __vbaFixstrConstruct, __vbaR4Cy, __vbaLateIdCallLd, __vbaRedim, EVENT_SINK_Release, __vbaUI1I2, _CIsqrt, __vbaObjIs, __vbaVarAnd, EVENT_SINK_QueryInterface, __vbaExceptHandler, __vbaStrToUnicode, _adj_fprem, _adj_fdivr_m64, __vbaGosub, __vbaFPException, __vbaInStrVar, __vbaUbound, __vbaStrVarVal, __vbaVarCat, __vbaLsetFixstrFree, __vbaI2Var, _CIlog, __vbaErrorOverflow, __vbaR8Str, __vbaVar2Vec, __vbaVarLateMemCallLdRf, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarCmpEq, __vbaVarAdd, __vbaAryLock, __vbaVarDup, __vbaStrToAnsi, __vbaFpI2, __vbaVarLateMemCallLd, __vbaVarCopy, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaCastObj, __vbaStrMove, _allmul, __vbaLateIdSt, _CItan, __vbaAryUnlock, _CIexp, __vbaI4ErrVar, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	TextFormat
FileVersion	1.00
CompanyName	Harp inc.
LegalTrademarks	Draw tables and use all features inside cells
Comments	Also text around images
ProductName	TextFormat
ProductVersion	1.00
FileDescription	Draw images by path, by handle, by resource number with any alignment
OriginalFilename	TextFormat.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map

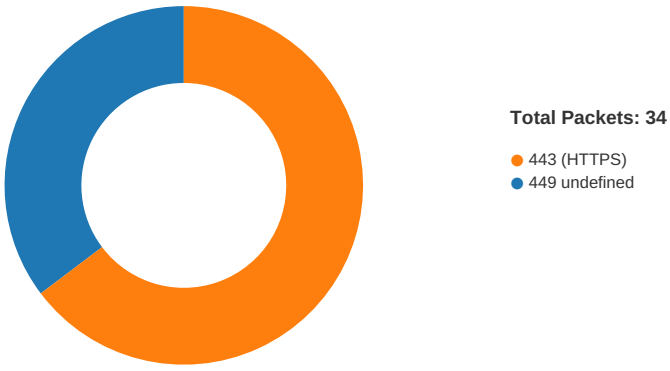
Language of compilation system	Country where language is spoken	Map
Greek	Greece	
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/23/20-08:11:36.814772	TCP	2404316	ET CNC Feodo Tracker Reported CnC Server TCP group 9	49735	443	192.168.2.5	185.90.61.9

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 23, 2020 08:10:41.390548944 CEST	49719	449	192.168.2.5	110.232.76.39
Jul 23, 2020 08:10:41.588262081 CEST	449	49719	110.232.76.39	192.168.2.5
Jul 23, 2020 08:10:42.111964941 CEST	49719	449	192.168.2.5	110.232.76.39
Jul 23, 2020 08:10:42.307502985 CEST	449	49719	110.232.76.39	192.168.2.5
Jul 23, 2020 08:10:42.810493946 CEST	49719	449	192.168.2.5	110.232.76.39
Jul 23, 2020 08:10:43.025551081 CEST	449	49719	110.232.76.39	192.168.2.5
Jul 23, 2020 08:10:44.266026020 CEST	49720	449	192.168.2.5	110.232.76.39
Jul 23, 2020 08:10:44.462061882 CEST	449	49720	110.232.76.39	192.168.2.5
Jul 23, 2020 08:10:44.966342926 CEST	49720	449	192.168.2.5	110.232.76.39
Jul 23, 2020 08:10:45.164099932 CEST	449	49720	110.232.76.39	192.168.2.5
Jul 23, 2020 08:10:45.674470901 CEST	49720	449	192.168.2.5	110.232.76.39
Jul 23, 2020 08:10:45.873655081 CEST	449	49720	110.232.76.39	192.168.2.5
Jul 23, 2020 08:10:47.090353966 CEST	49721	449	192.168.2.5	110.232.76.39
Jul 23, 2020 08:10:47.285861969 CEST	449	49721	110.232.76.39	192.168.2.5
Jul 23, 2020 08:10:47.787162066 CEST	49721	449	192.168.2.5	110.232.76.39
Jul 23, 2020 08:10:47.983171940 CEST	449	49721	110.232.76.39	192.168.2.5
Jul 23, 2020 08:10:48.487063885 CEST	49721	449	192.168.2.5	110.232.76.39
Jul 23, 2020 08:10:48.683051109 CEST	449	49721	110.232.76.39	192.168.2.5
Jul 23, 2020 08:10:50.833265066 CEST	49722	443	192.168.2.5	185.99.2.66

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 23, 2020 08:10:50.896413088 CEST	443	49722	185.99.2.66	192.168.2.5
Jul 23, 2020 08:10:50.896575928 CEST	49722	443	192.168.2.5	185.99.2.66
Jul 23, 2020 08:10:50.906559944 CEST	49722	443	192.168.2.5	185.99.2.66
Jul 23, 2020 08:10:50.969717026 CEST	443	49722	185.99.2.66	192.168.2.5
Jul 23, 2020 08:10:50.970062017 CEST	443	49722	185.99.2.66	192.168.2.5
Jul 23, 2020 08:10:50.970089912 CEST	443	49722	185.99.2.66	192.168.2.5
Jul 23, 2020 08:10:50.970107079 CEST	443	49722	185.99.2.66	192.168.2.5
Jul 23, 2020 08:10:50.970122099 CEST	443	49722	185.99.2.66	192.168.2.5
Jul 23, 2020 08:10:50.970186949 CEST	49722	443	192.168.2.5	185.99.2.66
Jul 23, 2020 08:10:50.970401049 CEST	49722	443	192.168.2.5	185.99.2.66
Jul 23, 2020 08:10:50.972846031 CEST	443	49722	185.99.2.66	192.168.2.5
Jul 23, 2020 08:10:51.021086931 CEST	49722	443	192.168.2.5	185.99.2.66
Jul 23, 2020 08:10:51.084371090 CEST	443	49722	185.99.2.66	192.168.2.5
Jul 23, 2020 08:10:51.130327940 CEST	49722	443	192.168.2.5	185.99.2.66
Jul 23, 2020 08:10:51.194247961 CEST	443	49722	185.99.2.66	192.168.2.5
Jul 23, 2020 08:10:51.194377899 CEST	443	49722	185.99.2.66	192.168.2.5
Jul 23, 2020 08:10:51.194396019 CEST	443	49722	185.99.2.66	192.168.2.5
Jul 23, 2020 08:10:51.194410086 CEST	443	49722	185.99.2.66	192.168.2.5
Jul 23, 2020 08:10:51.194423914 CEST	443	49722	185.99.2.66	192.168.2.5
Jul 23, 2020 08:10:51.194437981 CEST	443	49722	185.99.2.66	192.168.2.5
Jul 23, 2020 08:10:51.194453001 CEST	443	49722	185.99.2.66	192.168.2.5
Jul 23, 2020 08:10:51.194562912 CEST	49722	443	192.168.2.5	185.99.2.66
Jul 23, 2020 08:10:51.194576979 CEST	443	49722	185.99.2.66	192.168.2.5
Jul 23, 2020 08:10:51.194592953 CEST	443	49722	185.99.2.66	192.168.2.5
Jul 23, 2020 08:10:51.194878101 CEST	49722	443	192.168.2.5	185.99.2.66
Jul 23, 2020 08:10:51.714596987 CEST	49722	443	192.168.2.5	185.99.2.66
Jul 23, 2020 08:10:51.717784882 CEST	49723	449	192.168.2.5	45.6.16.68
Jul 23, 2020 08:10:54.727473974 CEST	49723	449	192.168.2.5	45.6.16.68
Jul 23, 2020 08:11:00.728247881 CEST	49723	449	192.168.2.5	45.6.16.68
Jul 23, 2020 08:11:14.263109922 CEST	49734	443	192.168.2.5	85.204.116.216
Jul 23, 2020 08:11:17.267854929 CEST	49734	443	192.168.2.5	85.204.116.216
Jul 23, 2020 08:11:23.276602983 CEST	49734	443	192.168.2.5	85.204.116.216
Jul 23, 2020 08:11:36.814771891 CEST	49735	443	192.168.2.5	185.90.61.9
Jul 23, 2020 08:11:39.823227882 CEST	49735	443	192.168.2.5	185.90.61.9
Jul 23, 2020 08:11:45.829137087 CEST	49735	443	192.168.2.5	185.90.61.9
Jul 23, 2020 08:11:59.348507881 CEST	49739	443	192.168.2.5	134.119.191.11
Jul 23, 2020 08:12:02.359503031 CEST	49739	443	192.168.2.5	134.119.191.11
Jul 23, 2020 08:12:08.363184929 CEST	49739	443	192.168.2.5	134.119.191.11
Jul 23, 2020 08:12:21.910532951 CEST	49740	443	192.168.2.5	134.119.191.21
Jul 23, 2020 08:12:24.911041021 CEST	49740	443	192.168.2.5	134.119.191.21
Jul 23, 2020 08:12:30.912110090 CEST	49740	443	192.168.2.5	134.119.191.21

HTTPS Packets

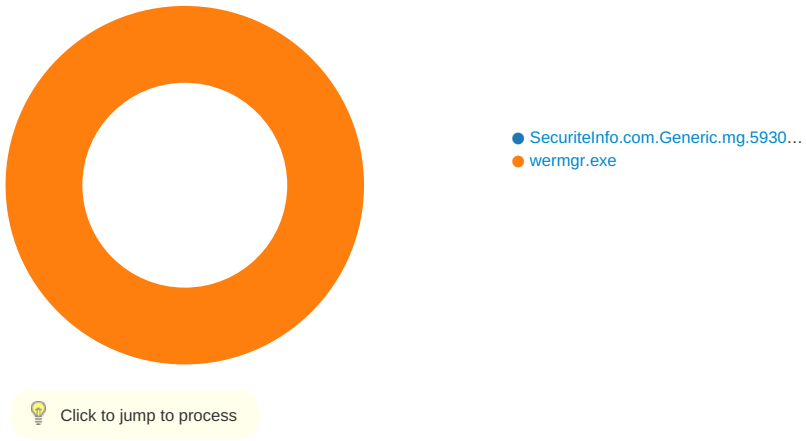
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 23, 2020 08:10:50.972846031 CEST	185.99.2.66	443	192.168.2.5	49722	CN=server.radioslon.ba CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jul 16 02:00:00 CEST 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Jul 17 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,5-10-11-13-35-23-65281,29-23-24,0	8916410db85077a5460817142dcbc8de
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		

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=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Generic.mg.5930091b65aed962.exe PID: 3124
Parent PID: 3184

General

Start time:	08:10:33
Start date:	23/07/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.5930091b65aed962.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.5930091b65aed962.exe'
Imagebase:	0x400000
File size:	540724 bytes
MD5 hash:	5930091B65AED9627DD1A4E86458B72F
Has administrator privileges:	false
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: wermgr.exe PID: 3092 Parent PID: 3124

General

Start time:	08:10:36
Start date:	23/07/2020
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0x7ff72a270000
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Trickbot_1, Description: Yara detected Trickbot, Source: 00000001.00000002.1225534063.000002116664E000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\desktop.ini	unknown	282	success or wait	1	211665D7AA7	ReadFile

Disassembly

Code Analysis