ID: 432683
Sample Name:
SecuriteInfo.com.Trojan.Packed2.43183.29557.7257
Cookbook: default.jbs
Time: 16:57:12
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

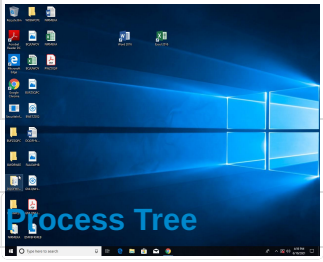
Analysis Report SecuriteInfo.com.Trojan.Packed2.43183…

Overview

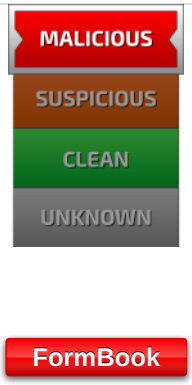
General Information

Sample Name:	SecuriteInfo.com.Trojan.Packed2.43183.29557.7257 (renamed file extension from 7257 to exe)
Analysis ID:	432683
MD5:	4e9095ceadd56b..
SHA1:	bce676ea49fb670.
SHA256:	1fe427cfa805bba..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

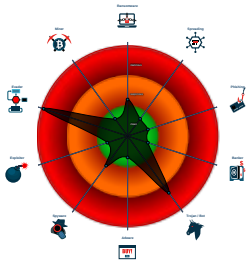


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- .NET source code contains very larg…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…

Classification



- **System is w10x64**
- SecuriteInfo.com.Trojan.Packed2.43183.29557.exe (PID: 6916 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Packed2.43183.29557.exe' MD5: 4E9095CEADD56BC68A99947AB929F691)
  - AddInProcess32.exe (PID: 6200 cmdline: C:\Users\user\AppData\Local\Temp\AddInProcess32.exe MD5: F2A47587431C466535F3C3D3427724BE)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - systray.exe (PID: 2108 cmdline: C:\Windows\SysWOW64\systray.exe MD5: 1373D481BE4C8A6E5F5030D2FB0A0C68)
        - cmd.exe (PID: 4812 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\AddInProcess32.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.roamallday.com/sadn/"
  ],
  "decoy": [
    "blessonschool.com",
    "lydialondon.com",
    "evln.xyz",
    "mychallengeiam.com",
    "stealthshop.net",
    "amybrownwhiteconsulting.info",
    "pakistanwholesaler.com",
    "authenticcase.com",
    "timothymaina.com",
    "kiem-etre.com",
    "thslot39.com",
    "tripprivee.com",
    "timeforbusinessblog.xyz",
    "afgecouncil100.com",
    "automotivesupplierdc.com",
    "thebigfoottheory.com",
    "resocoin.com",
    "healthepartner.com",
    "kkrazzybazar.com",
    "stgwxq.com",
    "tech4thelolo.com",
    "smshare2u.com",
    "mow-it-now.com",
    "seemymiamihome.com",
    "urbanadultstore.com",
    "tmvh8.com",
    "livelifelocalpublications.com",
    "blaxies3.com",
    "hotlab.info",
    "axmpjbwqh.icu",
    "lileshop.com",
    "genariofficial.com",
    "vibeofthetribe.com",
    "tldyyl.com",
    "dapurbuageung.com",
    "murrayburngundogs.com",
    "hertsandlondonknee.com",
    "mcfarline.com",
    "chicskr.com",
    "producepatties.com",
    "026lw.com",
    "humblehomeus.com",
    "accukoopje.com",
    "tantnewsgarre.website",
    "okettnet.net",
    "mattwilborne.info",
    "granthamrobotics.com",
    "theinfluenceprogram.net",
    "pointmortgageservicing.com",
    "garantiservice.com",
    "bossesbuildbusinesscredit.com",
    "oselsoft.xyz",
    "lareleverh.com",
    "mirzaissa-realtor.com",
    "tourneyphotos.com",
    "handpickednurse.com",
    "guiaconservador.com",
    "theliftquotient.com",
    "linkalto.com",
    "cosmoandcocrafts.com",
    "wzcp09.com",
    "mclpay.com",
    "jobjiihnb.club",
    "sudesheranga.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.737256043.00000000037CC000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
00000001.00000002.737256043.00000000037C C000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8190:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x851a:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1422d:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13d19:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1432f:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x144a7:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x8f32:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x12f94:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9caa:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1931f:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a3c2:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.737256043.00000000037C C000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16251:$sqlite3step: 68 34 1C 7B E1 • 0x16364:$sqlite3step: 68 34 1C 7B E1 • 0x16280:$sqlite3text: 68 38 2A 90 C5 • 0x163a5:$sqlite3text: 68 38 2A 90 C5 • 0x16293:$sqlite3blob: 68 53 D8 7F 8C • 0x163bb:$sqlite3blob: 68 53 D8 7F 8C
0000000B.00000002.803111095.0000000001290000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000B.00000002.803111095.0000000001290000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.0.AddInProcess32.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
11.0.AddInProcess32.exe.400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
11.0.AddInProcess32.exe.400000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$sqlite3step: 68 34 1C 7B E1 • 0x159bc:$sqlite3step: 68 34 1C 7B E1 • 0x158d8:$sqlite3text: 68 38 2A 90 C5 • 0x159fd:$sqlite3text: 68 38 2A 90 C5 • 0x158eb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a13:$sqlite3blob: 68 53 D8 7F 8C
11.2.AddInProcess32.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
11.2.AddInProcess32.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Copyright Joe Security LLC 2021

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)
- .NET source code contains very large array initializations

Hooking and other Techniques for Hiding and Protection:

- Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Allocates memory in foreign processes
- Injects a PE file into a foreign processes
- Maps a DLL or memory area into another process
- Modifies the context of a thread in another process (thread injection)
- Queues an APC in another process (thread injection)
- Sample uses process hollowing technique
- Writes to foreign memory regions

Stealing of Sensitive Information:

Copyright Joe Security LLC 2021

Yara detected FormBook

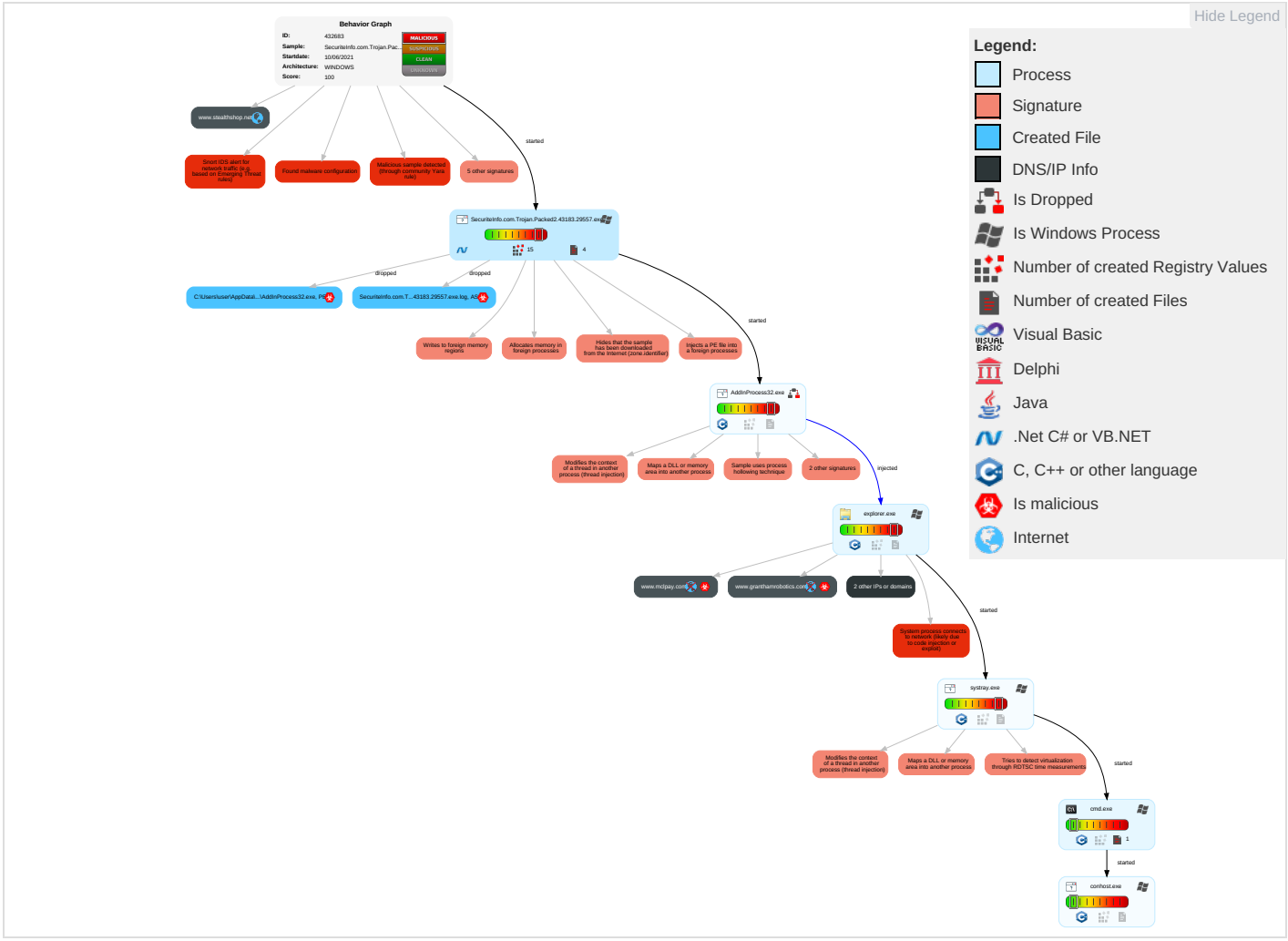
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts 1	Shared Modules 1	Valid Accounts 1	Valid Accounts 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Valid Accounts 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 8 1 2	Access Token Manipulation 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 3 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 8 1 2	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Deobfuscate/Decode Files or Information 1	DCSync	Network Sniffing	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	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Obfuscated Files or Information 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Software Packing 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols

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.Packed2.43183.29557.exe	34%	Virustotal		Browse
SecuriteInfo.com.Trojan.Packed2.43183.29557.exe	36%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	
SecuriteInfo.com.Trojan.Packed2.43183.29557.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.0.AddInProcess32.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
11.2.AddInProcess32.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.c/gP	0%	Avira URL Cloud	safe	
http://ns.d	0%	Avira URL Cloud	safe	
http://www.granthamrobotics.com/sadn/?5jDxn=9rYPWNexEp&9r8=cvOZMLUYKOYUB2MIVs3brF1aeCykDgyLTnisf2vSTBUNQvDIkJgvRwpKMlOnwLgVr/YP	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://ns.adobe.cobjP	0%	Avira URL Cloud	safe	
www.roamallday.com/sadn/	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://ns.ado/1P	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.mclpay.com/sadn/?9r8=DXfJxxxI+/4CaoDoAzC1V5G6SJQKNuW4mru3KXZlF9SJY6Uq4c9wctugrHKIzz2k7BKt&5jDxn=9rYPWNexEp	0%	Avira URL Cloud	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	13.59.53.244	true	false		high
granthamrobotics.com	34.102.136.180	true	false		unknown
www.stealthshop.net	74.220.199.6	true	false		unknown
www.mclpay.com	unknown	unknown	true		unknown
www.granthamrobotics.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.granthamrobotics.com/sadn/?5jDxn=9rYPWNexEp&9r8=cvOZMLUYKOYUB2MIVs3brF1aeCykDgyLTnisf2vSTBUNQvDIkJgvRwpKMlOnwLgVr/YP	false	• Avira URL Cloud: safe	unknown
www.roamallday.com/sadn/	true	• Avira URL Cloud: safe	low
http://www.mclpay.com/sadn/?9r8=DXfJxxxI+/4CaoDoAzC1V5G6SJQKNuW4mru3KXZlF9SJY6Uq4c9wctugrHKIzz2k7BKt&5jDxn=9rYPWNexEp	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.59.53.244	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
34.102.136.180	granthamrobotics.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432683
Start date:	10.06.2021
Start time:	16:57:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.Packed2.43183.29557.7257 (renamed file extension from 7257 to exe)

Copyright Joe Security LLC 2021

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:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/2@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 13.9% (good quality ratio 12.8%) • Quality average: 74.2% • Quality standard deviation: 30%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:58:06	API Interceptor	218x Sleep call for process: SecuriteInfo.com.Trojan.Packed2.43183.29557.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
13.59.53.244	PROFORMA FATURA PDF.exe	Get hash	malicious	Browse	• www.lcpcap.com/owws/?6lM=tC19x4LEJPVs8ONi+s37iu7cXys1nv6MWGTi+k5+Xwww0X6jnHUjFOF1LJ5LiQA8pgEL&4hnLI4=tVkpfp903TM
	STATEMENT.exe	Get hash	malicious	Browse	• www.linjudama.com/s5cm/?7nwhw=QDP0f9nkNg998lwZsNWJ9sidgDpm9neJ2Jn8Yw6wtNyTzbKtz13+oJch9rhNvjF++nAV&ML=EZBXFN7pQ8l

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO 0003789311.exe	Get hash	malicious	Browse	• www.irx1.com/hdno/?gL3T50=HFQPP850&lr=8VXYlJ+qC9Zm/oWjwI4An6+SwQ6WUPemFoSpbmpwN9y10//JZ5Swhoao6e+gJuvLUJpT
	tgb4.exe	Get hash	malicious	Browse	• www.downloadzilla.com/wdva/?h0DhCjC=lrtSiwQ0UV0iJ6qUawKzcS7ioNEK6Lev//Bpbi3MeUICWQT1VbW7IcDrVARDUN0Nz4+z&NXEL9=AbCxIhG8PxkDPDd0
	item.exe	Get hash	malicious	Browse	• www.wayinfinite.com/m3rc/?Ntipth=llyx&s864=FekLAVUqIGMz2T4hePSh2wVAHI49txL7qiZrReFERor7hYZGq5xwg9yju7MLNYYUY1/6
	mal1.exe	Get hash	malicious	Browse	• www.haifu168.com/kum/?GVM=/29xL9VS3/1U5/xPfegU/SuNpJoOLIhFGQE0mZ39nj/4nJDMDsD3ZSJRA6e20dMlRTAQ&oX=Txo8nZfpzf4tf
	PO_0065-2021.exe	Get hash	malicious	Browse	• www.wayinfinite.com/m3rc/?JhJ=FekLAVUqIGMz2T4hePSh2wVAHI49txL7qiZrReFERor7hYZGq5xwg9yju4gxOZ0vbCercw0EmQ==&qR=J4i8zf50NBY44rGp
	MkV1zeHKw7.exe	Get hash	malicious	Browse	• www.keguanchina.com/xkcp/
	n2fpCzXURP.exe	Get hash	malicious	Browse	• www.painhut.com/p2io/?bl=403u/w6B7XptcAEzuvN4cykoFcXgffqxcXNiYWMFmnIxKaVZCbECctw1BX3zhA2M1C5a&Qxo=L6hP-X9hEvs0
	Purchase Inquiry&Product Specification.exe	Get hash	malicious	Browse	• www.zut8.com/cu6s/?u6utf=vbhk+Gd5SI7yY0pWs+GOsHeqw10/7SXUKzBTc6E2X7f/RncSflutcU0Ht12xIKOqIhKG&9rN46F=xVMHGdB8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	pictures.exe	Get hash	malicious	Browse	• www.futurenetx.com/8be3/?9rj0aZJ=EfmCLjhd39MMAKmRQG/HdYdrkTVM2IhR6h/3hOqgtPexGMVICk1civ/2eSKsRkUfPy9S&b6=uVBXJryHZFi0GnH
	f268bad6_by_Libranalysis.exe	Get hash	malicious	Browse	• www.volesvip.com/ugtw/?T6AH=bX/3LJmnBl2vQdkn0rMpdCAP7W11AfQ6M2gpr3oowtVX7S9qBtzDmLsBN4rg+TmDiFhP&wP9=mh2P2V3
	Specifikacije ponude proizvoda Mesutex 2021 doc.exe	Get hash	malicious	Browse	• www.ryanscode.com/ftgq/?1bS=WXotCFzhm&pP-=23JWsXMNU3B901upE30epEJ3klQjQSAbj7e94TDSIuOB/RvSwvTb1tco95KeTC9gByt0NHr7dw==
	FY9Z5TR6rr.exe	Get hash	malicious	Browse	• www.topsych.com/bucw/?l0GD1=xBZDi6rpmLdp-&4hlPBD=pHmd48aeJBSPZZ4oXPqMUa9iB+zw7o9633Qm6JoN2J/ksYljdm2ak3+3AB9oAE45NnYEmo/gHQ==
	New order list.exe	Get hash	malicious	Browse	• www.rewsales.com/3nop/?Ft5pL0-=XTaJjzM4uCDOYtA+7yjD+eZH5K6XMAmSlRwTD4qGykZpCu9jO9GFDFvkz/CxvnMAuMtTc+GeGg==&Dffl=ZfopiXtpbJ6
	tgix.exe	Get hash	malicious	Browse	• www.junkglobal.com/oerg/?AtxLpld=O3Nafde195flLn5s8vzxaW/utgaD58xH6xfGUR8Mza6C00S5vKcvEZVNFsrWPkksds0V&orW=W6L4IdAHz
	945AEE9E799851EB1A2215FE1A60E55E41EB6D69EF4CB.exe	Get hash	malicious	Browse	• kenal.co/elber/fre.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	Letter 09JUN 2021.xlsx	Get hash	malicious	Browse	• 52.14.32.15
	PO#78765439.ZIP.exe	Get hash	malicious	Browse	• 52.14.32.15
	New Order Vung Ang TPP Viet Nam.exe	Get hash	malicious	Browse	• 3.143.65.214
	PROFORMA FATURA PDF.exe	Get hash	malicious	Browse	• 13.59.53.244
	6dTTv9IdCw.exe	Get hash	malicious	Browse	• 3.143.65.214

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Telex_Payment.exe	Get hash	malicious	Browse	• 52.14.32.15
	STATEMENT.exe	Get hash	malicious	Browse	• 13.59.53.244
	QyKNw7NioL.exe	Get hash	malicious	Browse	• 3.143.65.214
	SKMBT41085NC9.exe	Get hash	malicious	Browse	• 52.14.32.15
	CC for account.exe	Get hash	malicious	Browse	• 13.59.53.244
	CARGO ARRIVAL NOTICE-MEDICOM AWB.exe	Get hash	malicious	Browse	• 52.14.32.15
	statement.exe	Get hash	malicious	Browse	• 52.14.32.15
	CONTRACT SWIFT.exe	Get hash	malicious	Browse	• 52.14.32.15
	RE; KOC RFQ for Flangers - RFQ 22965431.exe	Get hash	malicious	Browse	• 52.14.32.15
	PO 0003789311.exe	Get hash	malicious	Browse	• 13.59.53.244
	tgb4.exe	Get hash	malicious	Browse	• 13.59.53.244
	transferencia bancaria.exe	Get hash	malicious	Browse	• 52.15.160.167
	SHIPPING DOCUMENT_7048555233PDF.exe	Get hash	malicious	Browse	• 3.143.65.214
	item.exe	Get hash	malicious	Browse	• 13.59.53.244
	mal1.exe	Get hash	malicious	Browse	• 13.59.53.244

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	Letter 1019.xlsx	Get hash	malicious	Browse	• 18.140.1.169
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 143.204.98.37
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	• 75.2.26.18
	U03c2doc.exe	Get hash	malicious	Browse	• 108.128.23 8.226
	Letter 09JUN 2021.xlsx	Get hash	malicious	Browse	• 18.140.1.169
	Docc.html	Get hash	malicious	Browse	• 13.224.99.74
	ManyToOneMailMerge Ver 18.2.dotm	Get hash	malicious	Browse	• 52.209.246.140
	Sleek_Free.exe	Get hash	malicious	Browse	• 143.204.209.58
	ManyToOneMailMerge Ver 18.2.dotm	Get hash	malicious	Browse	• 52.216.141.230
	#Ud83d#Udcde_#U25b6#Ufe0f.htm	Get hash	malicious	Browse	• 15.236.176.210
	WV Northern Community College.docx	Get hash	malicious	Browse	• 52.43.249.183
	wzdu53.exe	Get hash	malicious	Browse	• 13.249.13.113
	com.duolingo_1162_apps.evozi.com.apk	Get hash	malicious	Browse	• 52.222.174.5
	rnPij0Z886.dll	Get hash	malicious	Browse	• 13.224.91.73
	Plex-v8.7.1.20931_build_812981296-armeabi-v7a(Apkg od.net).apk	Get hash	malicious	Browse	• 99.81.164.127
	Nota Fiscal Eletronica 00111834.msi	Get hash	malicious	Browse	• 54.171.246.133
	#U00a0Import Custom Duty invoice & its clearance d ocuments.exe	Get hash	malicious	Browse	• 75.2.26.18
	919780-920390.exe	Get hash	malicious	Browse	• 99.83.162.16
	lLJGwAgWDh.exe	Get hash	malicious	Browse	• 13.56.50.119
	KYC Compliance 10031.xlsx	Get hash	malicious	Browse	• 13.53.52.84

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\AddI nProcess32.exe	SecuriteInfo.com.Trojan.GenericKD.37066764.6014.exe	Get hash	malicious	Browse	
	lueTCJ7lV4.exe	Get hash	malicious	Browse	
	ZwqvqceZYv.exe	Get hash	malicious	Browse	
	My First Game.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.MSIL_Kryptik.ANN.genEldorado. 6306.exe	Get hash	malicious	Browse	
	62c59ba0_by_Libranalysis.exe	Get hash	malicious	Browse	
	Payment-slip011002883864.exe	Get hash	malicious	Browse	
	Payment Copy#513.exe	Get hash	malicious	Browse	
	Payment-slip000898070.exe	Get hash	malicious	Browse	
	47755769_by_Libranalysis.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.46273706.27055.exe	Get hash	malicious	Browse	
	RFQ# PC1746006.exe	Get hash	malicious	Browse	
	po.exe	Get hash	malicious	Browse	
	0kTpSR8QiF.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ-EB200-PLOO1_Bidding.pdf.exe	Get hash	malicious	Browse	
	po.exe	Get hash	malicious	Browse	
	BID INSTRUCTIONSCOMMERCIAL.exe	Get hash	malicious	Browse	
	RFQ-IOCL-PP-IN-301.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Agent.FGSF.21849.exe	Get hash	malicious	Browse	
	TT-SWIFT.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.Packed2.43183.29557.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Packed2.43183.29557.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1402
Entropy (8bit):	5.338819835253785
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4K5AE4Kzr7K84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoesX3:MIHK5HKXE1qHbHK5AHKzvKviYHKhQnoe
MD5:	F2152F0304453BCFB93E6D4F93C3F0DC
SHA1:	DD69A4D7F9F9C8D97F1DF535BA3949E9325B5A2F
SHA-256:	5A4D59CD30A1AF620B87602BC23A3F1EFEF792884053DAE6A89D1AC9AAD4A411
SHA-512:	02402D9EAA2DF813F83A265C31D00048F84AD18AE23935B428062A9E09B173B13E93A3CACC6547277DA6F937BBC413B839620BA600144739DA37086E03DD8B4F
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Co

C:\Users\user\AppData\Local\Temp\AddInProcess32.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Packed2.43183.29557.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	42080
Entropy (8bit):	6.2125074198825105
Encrypted:	false
SSDEEP:	384:gc3JOvwWj8Gpw0A67dOpRIMKJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+QsPZw:g4JU8g17dl6Iq88MoBd7mFViqM5sL2
MD5:	F2A47587431C466535F3C3D3427724BE
SHA1:	90DF719241CE04828F0DD4D31D683F84790515FF
SHA-256:	23F4A2CCDCE499C524CF43793FDA8E773D809514B5471C02FA5E68F0CDA7A10B
SHA-512:	E9D0819478DDDA47763C7F5F617CD258D0FACBBBFFE0C7A965EDE9D0D884A6D7BB445820A3FD498B243BBD8BECBA146687B61421745E32B86272232C6F9E90D8
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: SecuriteInfo.com.Trojan.GenericKD.37066764.6014.exe, Detection: malicious, Browse • Filename: lueTCJ7lV4.exe, Detection: malicious, Browse • Filename: ZwqvqceZYv.exe, Detection: malicious, Browse • Filename: My First Game.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.W32.MSIL_Kryptik.ANN.genEldorado.6306.exe, Detection: malicious, Browse • Filename: 62c59ba0_by_Libranalysis.exe, Detection: malicious, Browse • Filename: Payment-slip011002883864.exe, Detection: malicious, Browse • Filename: Payment Copy#513.exe, Detection: malicious, Browse • Filename: Payment-slip000898070.exe, Detection: malicious, Browse • Filename: 47755769_by_Libranalysis.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.GenericKD.46273706.27055.exe, Detection: malicious, Browse • Filename: RFQ# PC1746006.exe, Detection: malicious, Browse • Filename: po.exe, Detection: malicious, Browse • Filename: 0kTpSR8QiF.exe, Detection: malicious, Browse • Filename: RFQ-EB200-PLOO1_Bidding.pdf.exe, Detection: malicious, Browse • Filename: po.exe, Detection: malicious, Browse • Filename: BID INSTRUCTIONSCOMMERCIAL.exe, Detection: malicious, Browse • Filename: RFQ-IOCL-PP-IN-301.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Agent.FGSF.21849.exe, Detection: malicious, Browse • Filename: TT-SWIFT.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..X.....w... .....@.. ..... .`.....Hw..O..... .....f..`>.....v..... ....H.....text....W... ...X..... ..`.rsrc... .....Z.....@..@.relo c.....d.....@..B.....\|w.....H.....#...Q.....u.....0..K.....-..*..i....*...r...p.o....,...r...p.o....-..*....o.....o.....$...*.....o....(....(.....:...(....o.....r...p.o.....4.....o..... .....o.....s .....o!...s".....s#.....r]..prg..po$.....r...p.o$....r...pr...po$.....s.....(%....tB...r...p(&...&..r...p.('...s(.....o)...&..o*....(+...o,.....&...(- ....*.....3..@.....R...s.....s....(....*:.(/.....}P...*J.{P....o0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.735718668413099
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.Packed2.43183.29557.exe
File size:	557568
MD5:	4e9095ceadd56bc68a99947ab929f691
SHA1:	bce676ea49fb6709dc0e9a23df2e918e05b4074b
SHA256:	1fe427cfa805bbabdc371ae3f6ccea4088ca76e8b9fce9828a74885d72339020
SHA512:	f0019d55c93ee2ca616ad53635592352ae313684291c5aa2bfba7130d13b964220d393a9867bc1e985b2b8f904cf8b8a210aeb571c140642f0eb0ee98cc67898
SSDEEP:	6144:mP2KJg5YoBA4cG+qw1y/lcCcfcgjXLSua0QxCiNLd7UXm7Ej2l++7dWS9WVKBlch:m1MA4cScHfc4euixCiZiXurSkV6y
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....B.....x..... .....@.. ..... .`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4897de
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, HIGH_ENTROPY_VA
Time Stamp:	0x1FAF421A [Wed Nov 5 12:56:58 1986 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x877e4	0x87800	False	0.627983740775	data	6.74662046366	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8a000	0x596	0x600	False	0.410807291667	data	4.04237592323	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8c000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/10/21-16:59:51.470333	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49766	80	192.168.2.4	34.102.136.180
06/10/21-16:59:51.470333	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49766	80	192.168.2.4	34.102.136.180
06/10/21-16:59:51.470333	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49766	80	192.168.2.4	34.102.136.180
06/10/21-16:59:51.608156	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49766	34.102.136.180	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 16:59:51.350280046 CEST	192.168.2.4	8.8.8.8	0x5b59	Standard query (0)	www.granthamrobotics.com	A (IP address)	IN (0x0001)
Jun 10, 2021 16:59:56.618190050 CEST	192.168.2.4	8.8.8.8	0x567	Standard query (0)	www.mclpay.com	A (IP address)	IN (0x0001)
Jun 10, 2021 17:00:02.063884974 CEST	192.168.2.4	8.8.8.8	0xd155	Standard query (0)	www.stealthshop.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 16:59:51.418663025 CEST	8.8.8.8	192.168.2.4	0x5b59	No error (0)	www.granthamrobotics.com	granthamrobotics.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 16:59:51.418663025 CEST	8.8.8.8	192.168.2.4	0x5b59	No error (0)	granthamrobotics.com		34.102.136.180	A (IP address)	IN (0x0001)
Jun 10, 2021 16:59:56.776873112 CEST	8.8.8.8	192.168.2.4	0x567	No error (0)	www.mclpay.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 16:59:56.776873112 CEST	8.8.8.8	192.168.2.4	0x567	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		13.59.53.244	A (IP address)	IN (0x0001)
Jun 10, 2021 16:59:56.776873112 CEST	8.8.8.8	192.168.2.4	0x567	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		52.14.32.15	A (IP address)	IN (0x0001)
Jun 10, 2021 16:59:56.776873112 CEST	8.8.8.8	192.168.2.4	0x567	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.143.65.214	A (IP address)	IN (0x0001)
Jun 10, 2021 17:00:02.214797020 CEST	8.8.8.8	192.168.2.4	0xd155	No error (0)	www.stealthshop.net		74.220.199.6	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.granthamrobotics.com
- www.mclpay.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49766	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 16:59:51.470333099 CEST	5054	OUT	GET /sadn/?5jDxn=9rYPWNexEp&9r8=cvOZMLUYKOYUB2MIVs3brF1aeCykDgyLTnisf2vSTBUNQvDIkJgvRwpKMlOnwLgVr/YP HTTP/1.1 Host: www.granthamrobotics.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 10, 2021 16:59:51.608155966 CEST	5055	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 10 Jun 2021 14:59:51 GMT Content-Type: text/html Content-Length: 275 ETag: "60ba413e-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49767	13.59.53.244	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 16:59:56.918880939 CEST	5056	OUT	GET /sadn/?9r8=DXfJxxxI+/4CaoDoAzC1V5G6SJQKNuW4mru3KXZlF9SJY6Uq4c9wctugrHKIzz2k7BKt&5jDxn=9rYPWNexEp HTTP/1.1 Host: www.mclpay.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 16:59:57.059190989 CEST	5056	IN	HTTP/1.1 404 Not Found Date: Thu, 10 Jun 2021 14:59:57 GMT Content-Type: text/html Content-Length: 153 Connection: close Server: nginx/1.16.1 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 36 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx/1.16.1 </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Trojan.Packed2.43183.29557.exe PID: 6916
Parent PID: 5892

General

Start time:	16:57:55
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Packed2.43183.29557.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Packed2.43183.29557.exe'
Imagebase:	0x3a0000
File size:	557568 bytes
MD5 hash:	4E9095CEADD56BC68A99947AB929F691
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.737256043.00000000037CC000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.737256043.00000000037CC000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.737256043.00000000037CC000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.737458183.0000000003817000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.737458183.0000000003817000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.737458183.0000000003817000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.738166081.00000000038E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.738166081.00000000038E0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.738166081.00000000038E0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: AddInProcess32.exe PID: 6200 Parent PID: 6916

General

Start time:	16:58:37
Start date:	10/06/2021
Path:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
Imagebase:	0xcd0000
File size:	42080 bytes
MD5 hash:	F2A47587431C466535F3C3D3427724BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.803111095.0000000001290000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.803111095.0000000001290000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.803111095.0000000001290000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.801838633.0000000001180000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.801838633.0000000001180000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.801838633.0000000001180000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.801642119.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.801642119.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.801642119.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.725117231.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.725117231.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.725117231.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 6200

General

Start time:	16:58:42
Start date:	10/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: systray.exe PID: 2108 Parent PID: 3424

General

Start time:	16:59:10
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\systray.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\systray.exe
Imagebase:	0x1c0000
File size:	9728 bytes
MD5 hash:	1373D481BE4C8A6E5F5030D2FB0A0C68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.900861159.0000000002CC0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.900861159.0000000002CC0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.900861159.0000000002CC0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.900522638.0000000000330000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.900522638.0000000000330000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.900522638.0000000000330000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 4812 Parent PID: 2108

General

Start time:	16:59:15
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Local\Temp\AddInProcess32.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Deleted

Analysis Process: conhost.exe PID: 5964 Parent PID: 4812

General

Start time:	16:59:15
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021