ID: 626424
Sample Name:
SecuriteInfo.com.Trojan.NSISX.Spy.Gen.2.8452.17207
Cookbook: default.jbs
Time: 00:37:34
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

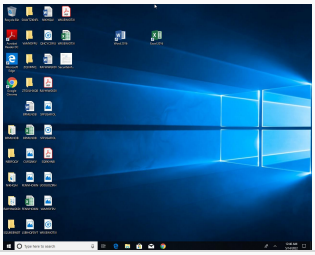
Windows Analysis Report

SecuriteInfo.com.Trojan.NSISX.Spy.Gen.2.8452.17207

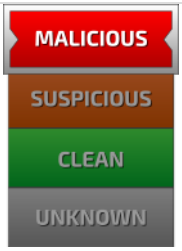
Overview

General Information

Sample Name:	SecuriteInfo.com.Trojan.NSISX.Spy.Gen.2.8452.17207 (renamed file extension from 17207 to exe)
Analysis ID:	626424
MD5:	14848f52302c15..
SHA1:	04d62d915bd1a8.
SHA256:	4ac982ea35522a..
Tags:	exe
Infos:	



Detection



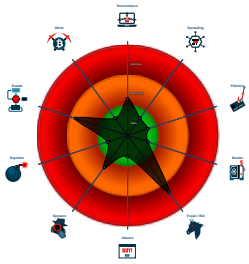
FormBook

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Multi AV Scanner detection for drop…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Yara signature match
- Antivirus or Machine Learning detec…
- Extensive use of GetProcAddress (…
- PE file contains strange resources
- Drops PE files

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Trojan.NSISX.Spy.Gen.2.8452.exe (PID: 5944 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Trojan.NSISX.Spy.Gen.2.8452.exe" MD5: 14848F52302C15E27B26FEE5FADA11C1)
  - miylwnpd.exe (PID: 3908 cmdline: C:\Users\user\AppData\Local\Temp\miylwnpd.exe C:\Users\user\AppData\Local\Temp\zehirtbl MD5: FF4C2F4D6E1FA34E8B958993C0DE134D)
    - miylwnpd.exe (PID: 1900 cmdline: C:\Users\user\AppData\Local\Temp\miylwnpd.exe C:\Users\user\AppData\Local\Temp\zehirtbl MD5: FF4C2F4D6E1FA34E8B958993C0DE134D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.beamaster.info/p0ip/"
  ],
  "decoy": [
    "webberkerr.com",
    "lelezhuanshu.xyz",
    "weedformellc.com",
    "ikzoekeenbedrijfsruimte.com",
    "swahlove.com",
    "dubaidesertsafari.travel",
    "atozmedicalimages.com",
    "uniytriox.com",
    "clickyourcat.com",
    "shandun-safety.com",
    "pakmart.center",
    "roxxiesixx.com",
    "twistedtaqueriachicago.com",
    "studynursingaustralia.online",
    "wellnesstestinggroup.com",
    "justusebias.com",
    "yqvzs.com",
    "co1l7o8vy.com",
    "lightning.legal",
    "cardamagescanner.com",
    "megawatchinc.com",
    "sadebademli.com",
    "bcoky.com",
    "unleashingyou-lifecoaching.com",
    "epsubtitles.online",
    "susanpetersonrealty.com",
    "gdderui.com",
    "claris-studio.cloud",
    "cryptomnis.com",
    "1ens.domains",
    "localbusinessassets.com",
    "et9n7e4vf.com",
    "quoteypants.com",
    "bokepremaja18.biz",
    "xiangqinmao.com",
    "lilot-pland45.site",
    "exilings.com",
    "nft-id.net",
    "sport-outdoorpacks.com",
    "plnykosik.online",
    "cidesadelcentro.com",
    "stunning-black.xyz",
    "zoeyunker.com",
    "videogamesgroup.com",
    "autodnstest.com",
    "bookworms.store",
    "69817269.com",
    "one-session22-lp.com",
    "modelofindia.com",
    "kennnyshands.com",
    "otopenishop.net",
    "freegameswithoutdownload.online",
    "alaskanwave.net",
    "tjkt8.com",
    "abv.wiki",
    "protoncarsale.com",
    "zhipurc.com",
    "psicologamoderna.com",
    "hidinginplainsight.digital",
    "cuamini-trankien.xyz",
    "yustunning.com",
    "apeironpay.xyz",
    "allowdrops.xyz",
    "allyouneedstore.xyz"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.233653327.0000000002CB0000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.233653327.0000000002CB0000.00000004.00001000.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8f92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16335:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15de1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16437:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165af:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1505c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa722:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca8a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.233653327.0000000002CB0000.00000004.00001000.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18809:$sqlite3step: 68 34 1C 7B E1 • 0x1891c:$sqlite3step: 68 34 1C 7B E1 • 0x18838:$sqlite3text: 68 38 2A 90 C5 • 0x1895d:$sqlite3text: 68 38 2A 90 C5 • 0x1884b:$sqlite3blob: 68 53 D8 7F 8C • 0x18973:$sqlite3blob: 68 53 D8 7F 8C

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.miylwnpd.exe.2cb0000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.miylwnpd.exe.2cb0000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7e08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8192:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15535:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14fe1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15637:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x157af:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x8baa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1425c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9922:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab87:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bc8a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.miylwnpd.exe.2cb0000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a09:$sqlite3step: 68 34 1C 7B E1 • 0x17b1c:$sqlite3step: 68 34 1C 7B E1 • 0x17a38:$sqlite3text: 68 38 2A 90 C5 • 0x17b5d:$sqlite3text: 68 38 2A 90 C5 • 0x17a4b:$sqlite3blob: 68 53 D8 7F 8C • 0x17b73:$sqlite3blob: 68 53 D8 7F 8C
1.2.miylwnpd.exe.2cb0000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.miylwnpd.exe.2cb0000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8f92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16335:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15de1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16437:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165af:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1505c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa722:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca8a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Multi AV Scanner detection for dropped file

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

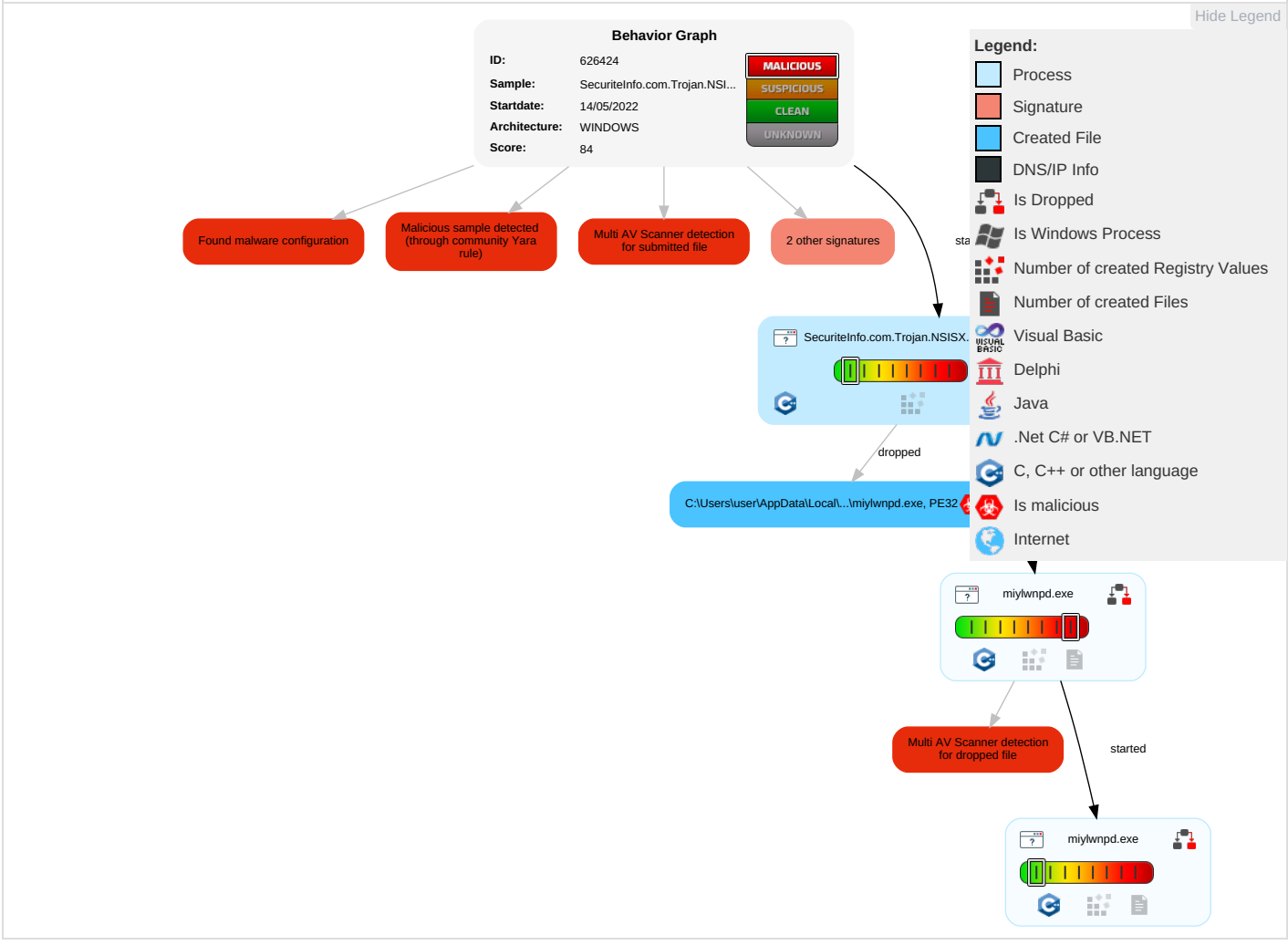
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	Path Interception	1 Access Token Manipulation	1 Access Token Manipulation	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 1 Process Injection	1 1 Process Injection	LSASS Memory	1 3 Security Software Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Software Packing	NTDS	1 4 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

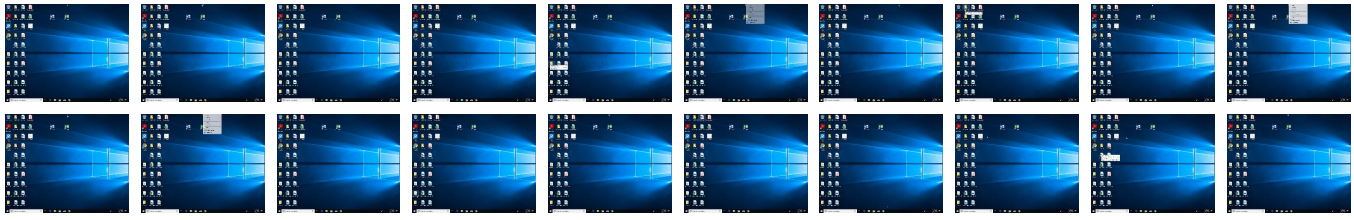
Behavior Graph



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.NSISX.Spy.Gen.2.8452.exe	41%	Virustotal		Browse
SecuriteInfo.com.Trojan.NSISX.Spy.Gen.2.8452.exe	34%	ReversingLabs	Win32.Trojan.Nsisx	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\miylwnpd.exe	20%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\miylwnpd.exe	24%	ReversingLabs	Win32.Trojan.Midie	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.miylwnpd.exe.2cb0000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.beamaster.info/p0ip/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.beamaster.info/p0ip/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.Trojan.NSISX.Spy.Gen.2.8452.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626424
Start date and time: 14/05/202200:37:34	2022-05-14 00:37:34 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.NSISX.Spy.Gen.2.8452.17207 (renamed file extension from 17207 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:	22
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:	mal84.troj.winEXE@5/4@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.8% (good quality ratio 94.3%) • Quality average: 83.4% • Quality standard deviation: 27.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.NSISX.Spy.Gen.2.8452.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	80384
Entropy (8bit):	6.294028811173466
Encrypted:	false
SSDEEP:	1536:XsTaC+v1CUfr0oxAomP3cX/4pi2sWjcdjXI:ua5wUD1/ui5j4
MD5:	FF4C2F4D6E1FA34E8B958993C0DE134D
SHA1:	8E8DE477AD67E1B107396B8B9BE749363EF10640
SHA-256:	38DD484E87FBD4520A99EAD1FDC0010F45A3D5F8A22B1BBD01E3FCBD56104AB3
SHA-512:	D64482AB140944CF138E47914EFD3EE2362E0FE98D519A89EAE6D31E03E9C51BFCBB4D44BA634526F393613F0AD8C14971BA240DBF2560BC57FF1C3705967F36
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 20%, Browse • Antivirus: ReversingLabs, Detection: 24%
Reputation:	low

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w...w...w...%`..w...%^..w...%a.w.....w...w..w..p....w..p.~..w..p... .w..Rich.w.....PE..L.....~b.....7.....@.....@.....$.....p.....T.....@..... .....text...U..... ..`.rdata...N.....P.....@..@.data... 1...0.....@....rsrc.....p.....*.....@..@.reloc.....,..... ..@..B..... .....

C:\Users\user\AppData\Local\Temp\nsaF211.tmp

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.NSISX.Spy.Gen.2.8452.exe
File Type:	data
Category:	dropped
Size (bytes):	274424
Entropy (8bit):	7.537223383847658
Encrypted:	false
SSDEEP:	3072:5vonGilTM+lGDSQ7923iyT+7EqtxRuNfpzqk2POHpfA6zIya5wUD1/ui5j4:5von9M+0eQ79IoTtcC6fA6zmwQu
MD5:	0A075A0200A53ACFD831038EC6C896F1
SHA1:	07E7D01FA876F8A37EE6FE1FAA34BA6C97A8E402
SHA-256:	DF91BE25213DA8243E34DCCBE3017FD53F9F493DD516D9D55263501375BA4122
SHA-512:	F43698C1374F37CD9F2F64866E611A8F0E98CE0107094AD1AB2AE1158E9993DE5586B4F8A8869414805C80DC88E40B9791172D9CC8CAC36DC1E34DB03E5F844
Malicious:	false
Reputation:	low
Preview:	.3.....,.....h...T%.....2.....3..... .....G.....j.....^..... ....

C:\Users\user\AppData\Local\Temp\qaodb6jx48te

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.NSISX.Spy.Gen.2.8452.exe
File Type:	data
Category:	dropped
Size (bytes):	175615
Entropy (8bit):	**7.990059953409327**
Encrypted:	**true**
SSDEEP:	3072:2vonGilTM+lGDSQ7923iyT+7EqtxRuNfpzqk2POHpfA6zY:2von9M+0eQ79IoTtcC6fA6zY
MD5:	6EB3509F6E43EEA8950ADBC156A96248
SHA1:	019A49C79CFB4503F005BA4347FD5EBF8C99718E
SHA-256:	F203F8DB5CFD1E17D03DD57BA2766F15F2A189E80080089C673BED271C87CDB7
SHA-512:	95F99448679A60B2707DE05E3D348CFB4F6E4112E2780ED53CC6E540C7493A0169316EBEAF992274D4474B8F36FEA5357CD2794AD8AA77CC6FEC2C48CC892C 9
Malicious:	false
Reputation:	low
Preview:	...PH....[!...X.....#....._=.Be...>.....i.`..n.....%.m.8..$./L.+..S..9.1.64.%....W5...,?....Cj/..f.1}8.....)i..5B\.....i...Ym....V.32Ay.+8y.-.....].U.v..:...m.0.....E}.7j....q9... ...Y..G.}....Z..N.....{!.....O.O.0.....a%\|x....^H....x.".1".'q...<.....=.Xe...>.....i.`..n.....,....c...74..=rlp.....{.9..GZ.^.....HX.7Ab.%.V.)i..5B<..E...].....6..$.....0...@...>..a,./\_....n. M:f=.:.....0..S....E..7j...oq.....h.OG.}....Z...../.....{!W.....O.....a,|x....G..Z.x."..".5'q.....\_=.Be...>.....i.`..n.....,....c...74..=rlp.....{.9..GZ.^.....HX.7Ab.%.V.)i..5B<..E...].....6..$ .....0...@...>..a,./_....n.U.v..:...P.0."S....E}.7j...oq.....G.}....Z...../.....{!W.....O.....a,|x....G..Z.x."..".5'q....._=.Be...>.....i.`..n.....,....c...74..=rlp.....{.9..GZ.^.....HX.7 Ab.%.V.)i..5B<..E...].....6..$.....0...@...>..a,./_....n.U.v..:...P.0."S....E}.7j...oq.....G.}....Z...../..

C:\Users\user\AppData\Local\Temp\zehirtbl

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.NSISX.Spy.Gen.2.8452.exe
File Type:	data
Category:	dropped
Size (bytes):	5171
Entropy (8bit):	6.118274194888097
Encrypted:	false
SSDEEP:	96:BXrtcxDxcjguWPxAcgUAyF1DQHWF3yW5SSn/MLmyJo3XFWDNbxUuyFxFV04mxkzq:2WguW5TAquH8cSn/MLmyJo3XFWZAFnRw
MD5:	ACB8234D1D848397EC3B1EB59A25AC91
SHA1:	7D17F048DDC6D19A40898B6079D36E0E1BDAB195
SHA-256:	942BD175D04B7C5567EB7F3EABC39866736B8922C68539D16DA9A32A839B5820
SHA-512:	601CA88B29149B9DDADECF29BBBBAAE1B626B84AE8C7BD580EB7BDF64FB3CDC9CD20563EFAEA229640194CE27684024EA62C8DE148E81CC045C40E9AFCB7 7459
Malicious:	false
Reputation:	low

Preview:	..%.....].".M."..m".M."…u.J.qE.....Y.r.!r....u..v.....U..Qr.!r....u..k.....=..9r.!r....u..<.....e..ar.!r....u.....M..!....7.%..M...!...m..i.....d.....q..L.?...Z\....q..O..q....Y.i].....)(fF. qr.U.r.=.r.e..r.M..r.m.r...[....!Z...Y-....]r.U...%"(..]..q.....J.).....) f..Y...]...dO!.....".M."..u..%..6.!.-..%.....L..L...u..q..%....%....u..qdO!...wK.....O....rR.....O%.. ..... .O%.....E".M."..J.u.....U..q..u.....qK....q..q..u..u.i..(...M...%..%..d... U.. Q...%.LI... U.. Q...%..M...(U...rR.f.....?prr..Y."..r.%..rrr..Y..Y.....]...J.]....]dO.....".M."..J.uE.....M..q..u... ..qK....q..q..u..u.i.....M".....%..%..d... M.. I..!..%.LI... M.. I....%.<I.. M.. I....d.%..?....M...I...%.LI... M.. I.(.%..M...(M...wK.o.....qrr..Y.....%.....r..r..r..r.!r.%.4srr..Y..Y.....].. .J.]....]dO.....J.u.....i..q..u.....qK....q..q..u..u.i.....M...%..%..d... i.. ...!..%.LI... i.. ....%..M...(i.. ..H.....Aqrr..Y.#r.!r.%..pr

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.333983439825163
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Trojan.NSISX.Spy.Gen.2.8452.exe
File size:	428316
MD5:	14848f52302c15e27b26fee5fada11c1
SHA1:	04d62d915bd1a81c4b5ed35df6edb953107398c8
SHA256:	4ac982ea35522a13de30ff7ddbbec9becf2c7528a48f0aff377e3d6758a7ae7b
SHA512:	aee08da4569bc969db4c086cb89950e311aaab9bf94677d9ba532b256ed5a29cc5942d48ca7c58ec8bee095d8e84b1f91935d61a9c601e1f9950c93a4ddd99c3
SSDEEP:	6144:eOtlldxqG7hiusCwlvcyHQOEYf5iTQuuAxjNnmJvLtVeV+hLk7:eORQiuqEyHH1GtNnmFBi+lg
TLSH:	B694E092D5C041A5EC794B34B53B1D3A16A7FFB9BCF9EA8E864D71312B732C2401B942
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@.....PE..L.....Oa.....h....:....

File Icon

Icon Hash:	81090f232b232380

Static PE Info

General

Entrypoint:	0x403646
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:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9AA9 [Sat Sep 25 21:54:49 2021 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:	61259b55b8912888e90f516ca08dc514

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi

Instruction
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F16FCE2A37Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F16FCE2A34Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [007A8B58h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b9000	0x28ee8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
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	0x67c4	0x6800	False	0.675180288462	data	6.49518266675	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.14106681717	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x39ebb8	0x600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a9000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3b9000	0x28ee8	0x29000	False	0.555979658918	data	5.77947429109	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b9280	0x10828	data	English	United States
RT_ICON	0x3c9aa8	0x1013c	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x3d9be8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4294901499, next used block 4294901499	English	United States
RT_ICON	0x3dde10	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4294901501, next used block 4294901757	English	United States
RT_ICON	0x3e03b8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294967294, next used block 4294967294	English	United States
RT_ICON	0x3e1460	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x3e18c8	0x100	data	English	United States
RT_DIALOG	0x3e19c8	0x11c	data	English	United States
RT_DIALOG	0x3e1ae8	0x60	data	English	United States
RT_GROUP_ICON	0x3e1b48	0x5a	data	English	United States
RT_MANIFEST	0x3e1ba8	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked

DLL	Import
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

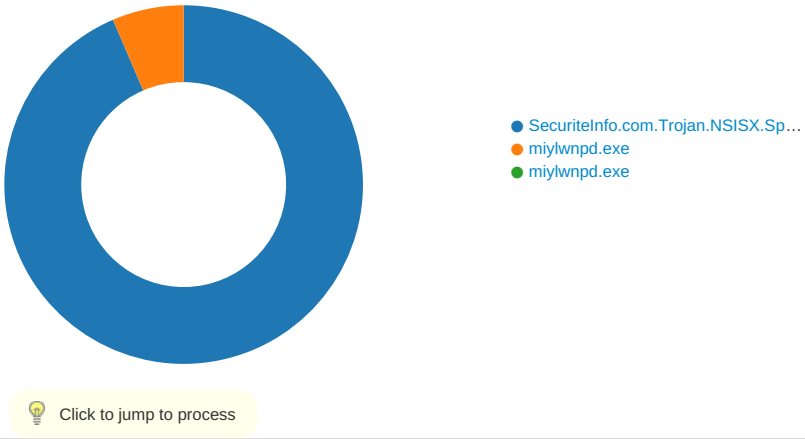
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.NSISX.Spy.Gen.2.8452.exe PID: **5944**, Parent PID: **5072**

General

Target ID:	0
Start time:	00:38:34
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.NSISX.Spy.Gen.2.8452.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Trojan.NSISX.Spy.Gen.2.8452.exe"
Imagebase:	0x400000
File size:	428316 bytes
MD5 hash:	14848F52302C15E27B26FEE5FADA11C1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsaF210.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061CC	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsaF211.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061CC	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsfF27F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061CC	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
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	405C28	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsfF27F.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405BE8	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
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	405C28	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\qaodb6jx48te	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40618A	CreateFileW
C:\Users\user\AppData\Local\Temp\zehirtbl	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40618A	CreateFileW
C:\Users\user\AppData\Local\Temp\miylwnpd.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40618A	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsaF210.tmp	success or wait	1	40398E	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsfF27F.tmp	success or wait	1	405DA9	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsaF211.tmp	0	32768	fd 33 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 03 00 00 00 fd 19 00 00 68 00 00 00 54 25 00 00 00 00 00 00 fd 32 00 00 01 00 00 00 fd 33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	3,hT%23	success or wait	9	40622A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qaodb6jx48te	0	16384	7f fd fd 50 48 0e fd fd fd 5b 21 0f 2e fd 58 08 fd fd fd fd fd fd 07 fd fd 09 fd 23 fd 52 fd fd 7f 5f 3d 2e 42 65 06 fd 0d 3e 0a 73 fd 7f 04 69 fd 60 fd 1a 6e fd 0f 4c fd fd 5a fd 25 fd 6d fd 38 fd fd 24 fd 2f 4c fd 2b 01 fd 53 fd 17 39 fd 31 fd 36 34 00 25 10 fd fd 19 57 35 fd fd 2c fd 3f fd fd fd 09 43 6a 2f fd fd 66 fd 31 7d 38 7f fd fd fd fd 29 69 fd fd 35 42 5c fd fd fd fd fd fd fd 69 17 fd fd 59 6d fd fd fd fd 56 fd 33 32 41 79 fd 2b 38 79 fd 2d fd fd 7f fd fd fd 18 10 fd fd fd fd fd 5d fd 55 18 76 fd fd 3a fd 07 fd 6d 03 30 fd 00 fd e3 fd 0f fd 45 7d fd 37 6a fd fd 0d fd 71 39 fd fd fd 16 fd 17 59 fd fd 47 fd 7d fd fd 0b fd 5a 06 fd 4e fd fd 1a 12 fd 0d fd fd 0c 7b 21 fd fd fd fd 1a fd fd 17 4f fd 4f fd 30 04 fd 88	PH[!.X#_=.Be>i`n%m8$/ L+S9164%W5,? Cj/f1}8)i5B\iYmV32Ay+8y -]Uv :m0E}7jq9YG}ZN{!OO0	success or wait	11	40622A	WriteFile
C:\Users\user\AppData\Local\Temp\zehirtbl	0	5171	fd 09 25 0d 0d 26 fd fd fd 7e fd fd fd 08 5d 0d 22 fd 4d fd 22 fd fd 6d 22 fd 4d fd 22 fd 4e 08 75 0d 4a fd 71 45 0d 0d 0d fd 08 59 0d 72 fd 21 72 fd fd fd fd 75 fd fd 76 0d 0d 0d fd fd 55 fd fd 51 72 fd 21 72 fd fd fd fd 75 fd fd 6b 0d 0d 0d fd fd 3d fd fd 39 72 fd 21 72 fd fd fd fd 75 fd fd 3c 0d 0d 0d fd fd 65 fd fd 61 72 fd 21 72 fd fd fd fd 75 fd fd fd 0d 0d 0d fd fd 4d fd fd 49 fd fd fd 09 fd 37 07 25 fd 06 4d 0e 0e fd 21 fd fd fd 6d fd fd 69 fd fd fd fd fd 09 1e 64 fd 64 fd fd fd 66 fd 71 fd 09 4c 1e 3f 07 fd fd 5a 5c fd fd 0e fd 71 fd 09 4f fd fd 71 fd fd fd 08 59 fd 69 5d 07 1e fd 0d 0d 0d 0d fd 09 29 28 66 46 08 71 72 fd 55 fd 72 fd 3d fd 72 fd 65 fd fd 72 fd 4d fd fd 72 fd 6d fd 72 fd fd e8 5b fd fd fd fd 21 5a	%]"M"m"M"uJqEYr!ruvU Qr!ruk=9r! ru<ear!ruMI7%M!midqL? Z\qOqYi]) (fFqrUr=rerMrmr[!Z	success or wait	1	40622A	WriteFile
C:\Users\user\AppData\Local\Temp\miylwnpd.exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 16 fd fd 77 fd fd fd 77 fd fd fd 77 fd fd fd 25 60 fd fd 77 fd fd fd 25 5e fd fd 77 fd fd fd 25 61 fd 77 fd fd 1f fd fd fd 77 fd fd fd 77 fd fd 77 fd fd 70 0e fd fd fd 77 fd fd 70 0e 7e fd fd 77 fd fd 70 0e fd fd fd 77 fd fd 52 69 63 68 fd 77 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd fd 7e 62 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$www%`w%^w%a www wpwp~wpwRichwPEL~b	success or wait	5	40622A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Trojan.NSISX.Spy.Gen.2.8452.exe	unknown	512	success or wait	396	4061FB	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Trojan.NSISX.Spy.Gen.2.8452.exe	unknown	16384	success or wait	14	4061FB	ReadFile
C:\Users\user\AppData\Local\Temp\nsaF211.tmp	unknown	4	success or wait	1	4061FB	ReadFile
C:\Users\user\AppData\Local\Temp\nsaF211.tmp	unknown	13238	success or wait	1	403465	ReadFile
C:\Users\user\AppData\Local\Temp\nsaF211.tmp	unknown	4	success or wait	3	4061FB	ReadFile

Analysis Process: miylwnpd.exe PID: **3908**, Parent PID: **5944**

General

Target ID:	1
Start time:	00:38:36
Start date:	14/05/2022
Path:	C:\Users\user\AppData\Local\Temp\miylwnpd.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\miylwnpd.exe C:\Users\user\AppData\Local\Temp\zehirtbl
Imagebase:	0x2e0000
File size:	80384 bytes
MD5 hash:	FF4C2F4D6E1FA34E8B958993C0DE134D
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: 00000001.00000002.233653327.0000000002CB0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.233653327.0000000002CB0000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.233653327.0000000002CB0000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 20%, Virustotal, Browse • Detection: 24%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zehirtbl	unknown	4096	success or wait	1	2E2C9C	ReadFile
C:\Users\user\AppData\Local\Temp\zehirtbl	unknown	4096	success or wait	1	2E2C9C	ReadFile

Analysis Process: miylwnpd.exe PID: **1900**, Parent PID: **3908**

General

Target ID:	2
Start time:	00:38:37
Start date:	14/05/2022
Path:	C:\Users\user\AppData\Local\Temp\miylwnpd.exe
Wow64 process (32bit):	
Commandline:	C:\Users\user\AppData\Local\Temp\miylwnpd.exe C:\Users\user\AppData\Local\Temp\zehirtbl
Imagebase:	
File size:	80384 bytes
MD5 hash:	FF4C2F4D6E1FA34E8B958993C0DE134D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly