



ID: 755965
Sample Name: SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe
Cookbook: default.jbs
Time: 11:36:08
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 3
Joe Sandbox Signatures 4
AV Detection 4
Malware Analysis System Evasion 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 7
Domains and IPs 7
Contacted Domains 7
URLs from Memory and Binaries 7
World Map of Contacted IPs 7
General Information 7
Warnings 7
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 8
Domains 8
ASNs 8
JA3 Fingerprints 8
Dropped Files 8
Created / dropped Files 8
C:\Users\user\AppData\Local\Temp\nsaACB6.tmp\System.dll 8
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Obeyeo.Bib 8
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armoniac\Urokkeligheden.Ord114 9
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armoniac\libgiognutls.dll 9
Static File Info 10
General 10
File Icon 10
Static PE Info 10
General 10
Authenticode Signature 10
Entrypoint Preview 11
Rich Headers 12
Data Directories 12
Sections 12
Resources 12
Imports 13
Possible Origin 13
Network Behavior 13
Statistics 13
System Behavior 13
Analysis Process: SecuriteInfo.com.Win32.Evo-gen.11060.2891.exePID: 5028, Parent PID: 3452 13
General 13
File Activities 14
File Created 14
File Deleted 16
File Written 16
File Read 17
Registry Activities 17
Key Created 17
Key Value Created 18
Disassembly 18

Copyright Joe Security LLC 2022

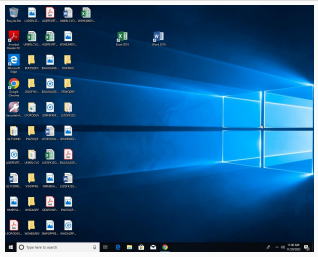
Windows Analysis Report

SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe

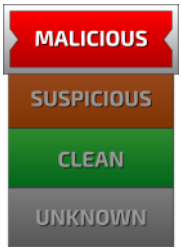
Overview

General Information

Sample Name:	SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe
Analysis ID:	755965
MD5:	7081c4822cf1c7…
SHA1:	4ee3b6c423b1c9..
SHA256:	b5330f82f3c5c3f…
Tags:	exe
Infos:	



Detection

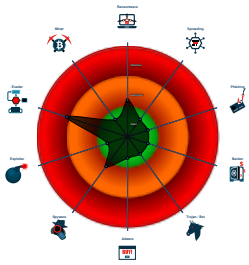


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Tries to detect virtualization through…
- Uses 32bit PE files
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Detected potential crypto function
- Stores files to the Windows start me…
- PE / OLE file has an invalid certifica…
- PE file contains more sections than…
- Contains functionality to dynamicall…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe (PID: 5028 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe MD5: 7081C4822CF1C7572DD82822B8F27C49)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Copyright Joe Security LLC 2022

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Malware Analysis System Evasion

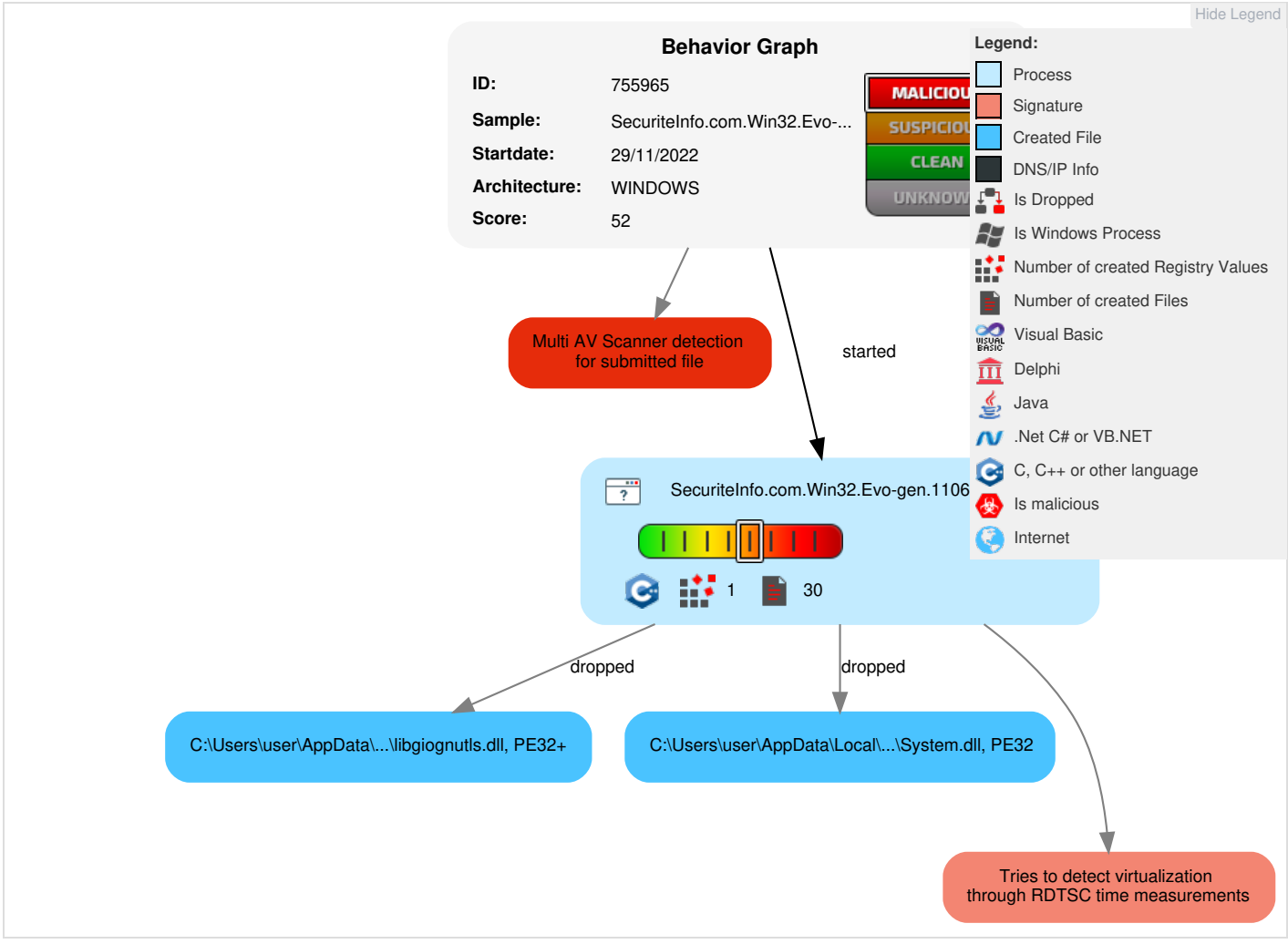


Tries to detect virtualization through RDTSC time measurements

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	1 Native API	1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	1 Access Token Manipulation	OS Credential Dumping	1 Security Software 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	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Obfuscated Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 3 System Information 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

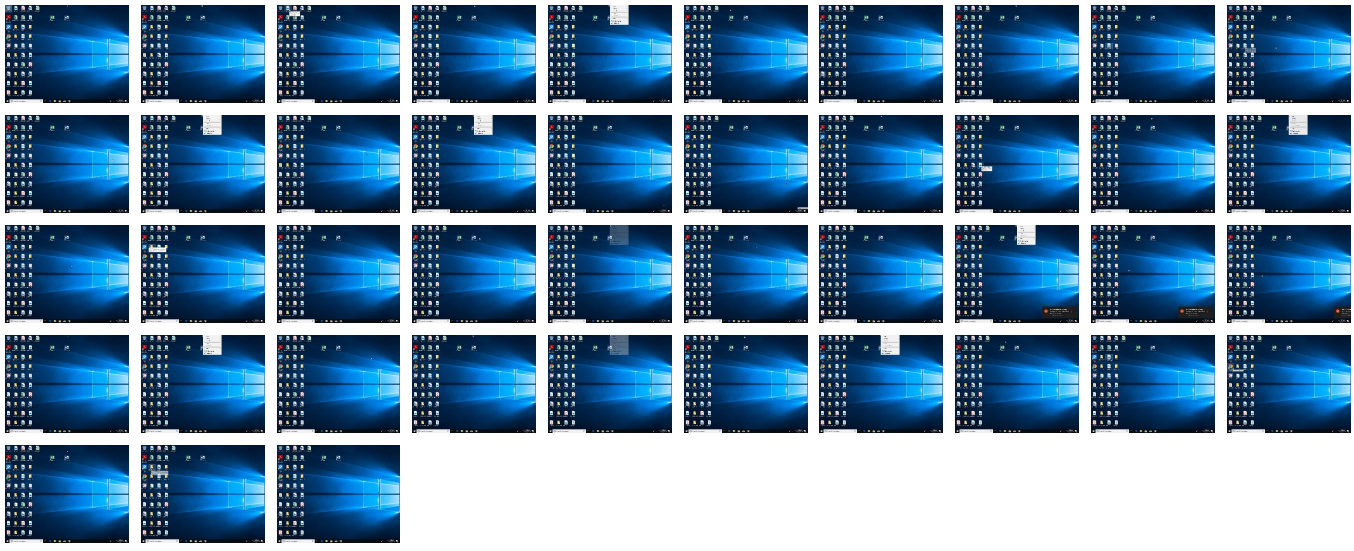
Behavior Graph



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.Win32.Evo-gen.11060.2891.exe	20%	ReversingLabs	Win32.Trojan.Nemesis	
SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe	29%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsaACB6.tmp\System.dll	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsaACB6.tmp\System.dll	1%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armoniac\libgiognutls.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armoniac\libgiognutls.dll	0%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

Copyright Joe Security LLC 2022

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755965
Start date and time:	2022-11-29 11:36:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	15
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:	mal52.evad.winEXE@1/4@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.8% (good quality ratio 84.5%) • Quality average: 87.8% • Quality standard deviation: 21.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ocsp.digicert.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.

Copyright Joe Security LLC 2022

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\nsaACB6.tmp\System.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	11776
Entropy (8bit):	5.656065698421856
Encrypted:	false
SSDEEP:	192:eY24sihno00Wfl97nH6T2enXwWobpWBTU4VtHT7dmN35Ol+Sl:E8Qll975eXqlWBrz7YLOl+
MD5:	17ED1C86BD67E78ADE4712BE48A7D2BD
SHA1:	1CC9FE86D6D6030B4DAE45ECDDCE5907991C01A0
SHA-256:	BD046E6497B304E4EA4AB102CAB2B1F94CE09BDE0EEBBA4C59942A732679E4EB
SHA-512:	0CBED521E7D6D1F85977B3F7D3CA7AC34E1B5495B69FD8C7BFA1A846BAF53B0ECD06FE1AD02A3599082FFACAF8C71A3BB4E32DEC05F8E24859D736B828092CD5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2% • Antivirus: Virustotal, Detection: 1%, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...u.u.u...s.u.a....r.!..q....t....t.Richu.....PE..L.....MX.. .....!..... .....'.....0.....`.....2.....0..P.....P.....0..X.....text..... ..... ..... ..`.rdata..S....0.....$.....@..@.data...x....@.....(.....@....reloc..b....P.....*.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Obeyeo.Bib

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe

File Type:	data
Category:	dropped
Size (bytes):	178824
Entropy (8bit):	6.515135274289935
Encrypted:	false
SSDEEP:	1536:Aqnh3ZWvlivpBh2LolEVEF+F2MVQ454gp3cHE6xBiP29vpAX5D57DwVaDXW:RkYzh2Lol/FdUJNfPgk5DVDUd
MD5:	52F571D999E9DD5B6ABFFE0CC9BF8DF3
SHA1:	67743CD31368EA4C7C350C5071A6B1D8A5AF400B
SHA-256:	7CC58916DBEADFF389E9375FD1F8973DB606156E953F309C55C40384E54765E3
SHA-512:	0BA04B8CDA196099229824B65348B71483D50377D10660AF8CD70A10919A310D88DDBA80D1F595524F71764BB2A765C87B9E5E2276391B11A272A52E3BBA7C11
Malicious:	false
Reputation:	low
Preview:	...6.{..N..p2...H.=L.]......I..b.0..2).v..X..~..q..nm.9..$h....YZ..}..V.u..E.a(M.........q......@9.n.`7......z.N...<...&..h..\.....&.h@p.....%.~5._b..b........B(....:.4.....t.S0..J..0.h.&. .H.t.gV.&..y.,J.3...m..\.......~n..L.AnI.....C.a.7w^!9.D.]J.....p...C8..Hn.....14.\|.. ...k........_9.....@%......S..d.>.*I.9.@.....I.....,.4G.l.}..e....<.....]...wj.Z.^...j.Fv.#..9n.c{.`..4U...,Q... v.g.t)..o...g......E.}..9...1....Wbl..JT%8..m[x.a.u.7.i).....1+..$l@...x$.~......6q.BE.x..7...n.n..gOZ.V.7..6.a!.c....`.vGm)..."L#~..E.....tV.....DjX.....Z.>..Z.).c.............D7}d.v.. . .%...v.fH.....Cw..x.^......b\ct....Y.*.g.b...1*cR..%6F'.......Q-.......GH....L!?1...<.^Rf.G.H[O.<.Ke.....R..._e..1..s........y.~..x!...Tl.... .a .;..KG.]%:."%.O..X.S..b..t.o{.......#..9...b. .J.e..w...<~b........5.................XC....Z....E.zE.g.k.X.^.=.W)...>.'K.h<.C\././.7.d......~./.a~.Yc.......4...{....d..m."...v.....v".....iY....9..ka.....M...m.})).....Y..f..-..4..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armoniac\Urokkeli gheden.Ord114

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe
File Type:	data
Category:	dropped
Size (bytes):	119298
Entropy (8bit):	**7.998253263209972**
Encrypted:	**true**
SSDEEP:	1536:6JcdhM4/003cKP7zr9UE0q19q9MUxJ0O1mwVrLSft3KeDQMjE4le/l1NUYeECfZm:LdhM4/Fpb/1Ca2LEt9DQMA4lGVUh14B
MD5:	251C92F85825E5BBBE4D7624FC7F4AE4
SHA1:	BF396458B8D37DCC5880B29A7482A4896828C35F
SHA-256:	20694D441EEAB696B6D6AE5B7785BB0CAD19E1708EF49C28737CAD1805B49CDC
SHA-512:	5730DF53CE6DE9791F81287EA340ECDECEF1B99B80DC7501F9739083AF5D66543795E82C19388522580A43B8553FEAA2D5C0B419502BC7325E34F1862BBD44D
Malicious:	false
Reputation:	low
Preview:	...Ct.m.j\i...G..@k.....D.....W.S.CE.P'.O....9l....4Y%\.R...%..'.D.o.%9h.....vP.h0...E_..1.}.....{...).h....F.r..lm....D..{..dF4.@F..=.....G..&..... v47.L..V..%.$x..rK..ue=. w.)..+b...$.m.Gj..@x.3...14J...#"....G| v8@Y2.R..v.."j...~.,..<..}...&H9F..v..=....>;.....HF..c...~..'c.f.p0"...>Q|./."...n..t.....$^.Z.c....h(.df.B..`,..#.?s.8..k'.B.t.....<3..s..h- ).Q..\R.O.C=.c.<S..b(..Q#.....r...j..z...U.vU.>..C...@...G-..7=.....".mu52.[...`Bf}0q.V.IF.\|(.pMo...^L.I.@.#[bH...1..I.I.Mi..iB..(N"$e.....r..9....1z.2..P.G*H..p....sE..O.cR.I.Z.H /.u_.Z+"Rk.M.g..q....Z..{0...*g....;....t..QF2.oA.v{....h.....TIN...r.. O.u..P...(........G.....+kk%9W.b.I.Q.....Gy9^~./..Q8..lo]$.5.....4. };.....80....ze.^I....WL.b....!..0.N.{Q...'..... I..dnP....7.p..aB.w.Z.v]R.../r.C6(q.C...%...n....2@..0$.X.;CW.1...5...s#.]..x[h..T./.>.(...dJ...q?._I....K...1'....9.).n1#..5:&.S3^........Z.Z.0.c._.'.....r;bw.P.....K.^.....(....'..4.?....N....#.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armoniac\libgiogn utls.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	131991
Entropy (8bit):	5.8780987492725405
Encrypted:	false
SSDEEP:	1536:v6J1cdTEl2OzvUtevCuoCW9fPr+vo9F5J7YWv3vbRnBycYWOGWSeaGymtYWOGWSS:VdW2OLgNCwXKSH8WPvVBjA+KE8S5
MD5:	10D998CF80B4437C2979B25EBCBE16D1
SHA1:	79C99DD2ABB99253E41C5E40DAB29522F93345BB
SHA-256:	A0A87BC30F4B39D7B642841A10208CE5286C6CA712B28B9D921E1EA6F547AEE6
SHA-512:	44863645B48815C3C248111F86440E3A0C515AF61B5A17D15B5A6C7304277F76056BCEB6C579E7824E11ADCA4DB3E385FA8019D602C40FA527E725C09B6AA523
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....&"...%.....P.....@.....g}.. ..`... .....IE.....0..... i..(.....text...X.....`..`.data..... .....@. ...rdata...A...0...B.....@..@.pdata.....R.....@..@.xdata..X.....`.....@..@.bss....p.....edata.....n.....@..@.idata.. IE.....F...p.....@....CRT....X.....@....tls..... .....@....reloc.....0.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.505402259729816
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.Win32.Evo-gen.11060.2891.exe
File size:	477800
MD5:	7081c4822cf1c7572dd82822b8f27c49
SHA1:	4ee3b6c423b1c9ebf5befbc73d1eef0c576cf026
SHA256:	b5330f82f3c5c3f223ae9decd3ebdcd74d1a13d95b1c42bd7b2de4e6c6cb0083
SHA512:	6e3377e6a47518f2267cd38646e2cec576d41fd8a67c8c2590f43bf353c0b1f322fc229e70bc98e9c7dfaa1a11cf872a0c8e2c15a31ee90ef1c4e65eac98ee3a
SSDEEP:	12288:Lz772qgvq2nLm4W2RPLKb+nFzIQ3Ja8TA:gXnS4W2RPLKm/of
TLSH:	4DA4D096F74155D6CC24177259BB9D3702B3BD7E14B10B5F61AE32322F332828A07A2E
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...P...P...P..*_...P...P..OP..*_...P...s...P...V...P..Rich.P.....PE..L...8.MX.....b...*.....J4.....@

File Icon



Icon Hash:	b8eee6a4c0c8c6c2

Static PE Info

General

Entrypoint:	0x40344a
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x584DCA38 [Sun Dec 11 21:50:48 2016 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:	4ea4df5d94204fc550be1874e1b77ea7

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Warrambool, OU="Gennembryde Catbrier ", E=Lrerforsamlingen@Resoneres187.ti, O=Warrambool, L=Betpouy, S=Occitanie, C=FR
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 5/16/2022 6:16:58 AM 5/15/2025 6:16:58 AM
Subject Chain	• CN=Warrambool, OU="Gennembryde Catbrier ", E=Lrerforsamlingen@Resoneres187.ti, O=Warrambool, L=Betpouy, S=Occitanie, C=FR
Version:	3
Thumbprint MD5:	50955086B951A7063EA053252647D196
Thumbprint SHA-1:	B2C1191B987021E62094F55BD9D8BCF9138BF3A6
Thumbprint SHA-256:	26FCB244ABFE2816CFB307605DB0353DBE6BE089ACEC8D49A63FDE728C428741
Serial:	D479F570518060D0

Entrypoint Preview
Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A230h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080B4h]
call dword ptr [004080B0h]
cmp ax, 00000006h
je 00007FA8D4CE9183h
push ebx
call 00007FA8D4CEC2DCh
cmp eax, ebx
je 00007FA8D4CE9179h
push 00000C00h
call eax
mov esi, 004082B8h
push esi
call 00007FA8D4CEC256h
push esi
call dword ptr [0040815Ch]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007FA8D4CE915Ch
push ebp
push 00000009h
call 00007FA8D4CEC2AEh
push 00000007h
call 00007FA8D4CEC2A7h
mov dword ptr [0042A244h], eax
call dword ptr [0040803Ch]
push ebx
call dword ptr [004082A4h]
mov dword ptr [0042A2F8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 004216E8h
call dword ptr [00408188h]
push 0040A384h
push 00429240h
call 00007FA8D4CEBE90h
call dword ptr [004080ACh]
mov ebp, 00435000h
push eax
push ebp
call 00007FA8D4CEBE7Eh
push ebx
call dword ptr [00408174h]
add word ptr [eax], 0000h

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	0x6e000	0x28868	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x73510	0x1558	.rsrc
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	0x2b4	.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	0x61f1	0x6200	False	0.6656967474489796	data	6.477074763411717	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x13a4	0x1400	False	0.4529296875	data	5.163001655755973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20338	0x600	False	0.501953125	data	3.9745558434885093	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x43000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x6e000	0x28868	0x28a00	False	0.4693269230769231	data	6.072692072533226	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x6e3b8	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States
RT_ICON	0x6e720	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536	English	United States
RT_ICON	0x7ef48	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 36864	English	United States
RT_ICON	0x883f0	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 20736	English	United States
RT_ICON	0x8d878	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384	English	United States
RT_ICON	0x91aa0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	English	United States
RT_ICON	0x94048	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	English	United States
RT_ICON	0x950f0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	English	United States
RT_ICON	0x95a78	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	English	United States
RT_DIALOG	0x95ee0	0x144	data	English	United States
RT_DIALOG	0x96028	0x13c	data	English	United States
RT_DIALOG	0x96168	0x100	data	English	United States
RT_DIALOG	0x96268	0x11c	data	English	United States

Copyright Joe Security LLC 2022

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x96388	0xc4	data	English	United States
RT_DIALOG	0x96450	0x60	data	English	United States
RT_GROUP_ICON	0x964b0	0x76	data	English	United States
RT_MANIFEST	0x96528	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetCurrentDirectoryW, GetFileAttributesW, GetFullPathNameW, Sleep, GetTickCount, CreateFileW, GetFileSize, MoveFileW, SetFileAttributesW, GetModuleFileNameW, CopyFileW, ExitProcess, SetEnvironmentVariableW, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, GetVersion, SetErrorMode, WaitForSingleObject, GetCurrentProcess, CompareFileTime, GlobalUnlock, GlobalLock, CreateThread, GetLastError, CreateDirectoryW, CreateProcessW, RemoveDirectoryW, lstrcmpiA, GetTempFileNameW, WriteFile, lstrcpyA, lstrcpyW, MoveFileExW, lstrcatW, GetSystemDirectoryW, GetProcAddress, GetModuleHandleA, GlobalFree, GlobalAlloc, GetShortPathNameW, SearchPathW, lstrcmpiW, SetFileTime, CloseHandle, ExpandEnvironmentStringsW, lstrcmpW, GetDiskFreeSpaceW, lstrlenW, lstrcpynW, GetExitCodeProcess, FindFirstFileW, FindNextFileW, DeleteFileW, SetFilePointer, ReadFile, FindClose, MulDiv, MultiByteToWideChar, lstrlenA, WideCharToMultiByte, GetPrivateProfileStringW, WritePrivateProfileStringW, FreeLibrary, LoadLibraryExW, GetModuleHandleW
USER32.dll	GetSystemMenu, SetClassLongW, IsWindowEnabled, EnableMenuItem, SetWindowPos, GetSysColor, GetWindowLongW, SetCursor, LoadCursorW, CheckDlgButton, GetMessagePos, LoadBitmapW, CallWindowProcW, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, wsprintfW, ScreenToClient, GetWindowRect, GetSystemMetrics, SetDlgItemTextW, GetDlgItemTextW, MessageBoxIndirectW, CharPrevW, CharNextA, wsprintfA, DispatchMessageW, PeekMessageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, GetClientRect, FillRect, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, LoadImageW, SetTimer, SetWindowTextW, PostQuitMessage, ShowWindow, GetDlgItem, IsWindow, SetWindowLongW, FindWindowExW, TrackPopupMenu, AppendMenuW, CreatePopupMenu, DrawTextW, EndPaint, CreateDialogParamW, SendMessageTimeoutW, SetForegroundWindow
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectW, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, SHGetPathFromIDListW, SHBrowseForFolderW, SHGetFileInfoW, ShellExecuteW, SHFileOperationW
ADVAPI32.dll	RegDeleteKeyW, SetFileSecurityW, OpenProcessToken, LookupPrivilegeValueW, AdjustTokenPrivileges, RegOpenKeyExW, RegEnumValueW, RegDeleteValueW, RegCloseKey, RegCreateKeyExW, RegSetValueExW, RegQueryValueExW, RegEnumKeyW
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

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

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe PID: **5028**, Parent PID: **3452**

General

Target ID:	0
Start time:	11:36:57
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe
Imagebase:	0x400000
File size:	477800 bytes
MD5 hash:	7081C4822CF1C7572DD82822B8F27C49
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	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsfAB4D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E55	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsfAB4E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E55	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	3	4058C9	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	3	4058C9	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	3	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	4058C9	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Obeyeo.Bib	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armoniac	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4058C9	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armoniac\libgiognutls.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armonia c\Urokkeligheden.Ord114	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E13	CreateFileW
C:\Users\user\AppData\Local\Temp\nsaACB6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E55	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	4058C9	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	4058C9	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	4058C9	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	4058C9	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	4058C9	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsaACB6.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	405889	CreateDirectoryW

<table>
<tr><th>File Path</th><th>Access</th><th>Attributes</th><th>Options</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsaACB6.tmp\System.dll</td><td>read attributes | synchronize | generic write</td><td>device</td><td>synchronous io non alert | non directory file</td><td>success or wait</td><td>1</td><td>405E13</td><td>CreateFileW</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsaACB6.tmp\System.dll</td><td>read attributes | synchronize | generic write</td><td>device</td><td>synchronous io non alert | non directory file</td><td>object name collision</td><td>3</td><td>405E13</td><td>CreateFileW</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsaACB6.tmp\System.dll</td><td>read attributes | synchronize | generic write</td><td>device</td><td>synchronous io non alert | non directory file</td><td>object name collision</td><td>19411</td><td>405E13</td><td>CreateFileW</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsaACB6.tmp\System.dll</td><td>read attributes | synchronize | generic write</td><td>device</td><td>synchronous io non alert | non directory file</td><td>object name collision</td><td>6</td><td>405E13</td><td>CreateFileW</td></tr>
</table>

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsfAB4D.tmp	success or wait	1	4036D7	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsaACB6.tmp	success or wait	1	405A32	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	32768	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	405EB3	WriteFile
unknown	43561	32768	75 6e 6b 6e 6f 77 6e	unknown	success or wait	21	405EB3	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Obeyeo.Bib	0	16384	fd fd fd 36 fd 7b fd 3b 4e 9a fd 70 32 fd fd fd 48 fd 3d 4c fd 5d fd 5e fd 0f 08 fd 6c fd fd 62 fd 30 fd fd 32 29 0e 76 fd fd 58 1b fd 7e fd 16 71 fd fd 6e 6d fd 39 07 2e 24 68 fd 01 7f fd 59 5a 04 fd 7d fd fd 56 ea 75 fd fd 45 fd 61 28 4d fd fd fd fd c7 fd e5 fd fd 1f 71 14 fd fd fd 02 fd 40 39 32 6e fd 60 37 fd fd fd 15 fd fd 7a 0e 4e fd fd 7f 3c fd 19 fd 26 17 07 68 fd fd 5c fd 15 fd fd 7f 26 fd 68 40 70 fd fd fd 1c 0e 25 fd 7e 35 fd 5f 62 10 fd 62 fd fd fd fd 10 05 fd bf 42 28 7f fd fd fd 3a fd 34 fd fd 0e fd fd fd 74 fd 53 30 fd 0e 4a fd 1b 30 13 68 fd 26 fd b5 48 1c 74 fd 67 56 fd 26 fd fd 79 fd 2c 4a 2e 33 fd fd fd 6d 0c fd 5c fd fd 0b fd fd 00 1c 7e 6e fd 0a 4c fd 41 6e 49 fd fd 1a fd fd 43 fd 61 fd 37 77 5e	6{Np2H=L]lb02)vX~qnm9.$hYZ}VuEa(Mq@9n`7zN<&h\&h@p%~5_bbB(:4tS0J0h&HtgV&y,J.3m\~nLAnICa7w^	success or wait	11	405EB3	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armoniac\libgiognutls.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 50 45 00 00 64 fd 0b 00 00 00 00 00 00 fd 01 00 fd 01 00 00 fd 00 26 22 0b 02 02 25 00 0a 01 00 00 fd 01 00 00 04 00 00 50 13 00 00 00 10 00 00 00 00 fd fd 02 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 40 02 00 00 04 00 00 67 7d 02 00 03 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd&"%P@g}`	success or wait	9	405EB3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armoniac\Urokkeligheden.Ord114	0	16384	fd fd fd 43 74 fd 6d 17 6a 5c 69 fd fd 12 47 fd fd 40 6b fd fd fd 1e fd fd 44 11 fd df fd fd 57 fd 53 fd 43 45 fd 50 27 fd 4f fd fd 02 fd 39 6c fd 46 fd fd 34 59 25 5c fd 52 fd fd 14 25 17 fd 27 fd 44 fd 6f fd 25 39 68 fd fd fd fd 12 fd fd fd 76 50 08 68 30 2e fd fd 45 5f fd fd 31 00 7d fd fd 3d fd e2 fd fd fd fd fd fd fd 85 fd 0b 7b fd 06 fd 29 fd 68 fd fd fd fd 46 fd 72 fd fd 6c 6d 0d fd 01 1f 44 0a 14 7b fd fd 64 46 34 fd 40 46 fd fd 3d 07 19 fd 11 fd 47 fd fd 26 fd fd 10 15 fd fd fd 20 76 34 37 fd 4c 53 18 56 00 fd 25 fd 24 78 07 fd 72 4b fd 11 75 65 3d 1d 77 fd 29 fd fd 2b 62 fd fd 1d 24 fd 6d fd 47 6a fd fd 40 78 fd 33 fd 08 15 31 34 4a 17 03 fd 23 22 fd 13 11 fd 47 7c 20 76 38 40 59 32 fd 52 fd fd 76 fd fd 22	Ctmj\iG@kDWSCEP'O9l4Y%\R%'Do%9hvPh0.E_1}{)hFrlmD{dF4@F=G& v47LV%$xrKue=w)+b$mGj@x314J#"G| v8@Y2Rv"	success or wait	8	405EB3	WriteFile
C:\Users\user\AppData\Local\Temp\nsaACB6.tmp\System.dll	0	11776	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 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 31 fd fd fd 75 fd 75 fd 75 fd fd bd 73 fd 75 fd 61 b3 76 fd fd 72 fd 21 4c fd 71 fd 16 16 fd 74 b3 4a b8 fd 74 fd 52 69 63 68 75 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 50 45 00 00 4c 01 04 00 1a fd 4d 58 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 20 00	MZ@!L!This program cannot be run in DOS mode.$1uuusuar!qttRichuPELMX!	success or wait	1	405EB3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe	unknown	512	success or wait	370	405E84	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe	unknown	16384	success or wait	1	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsfAB4E.tmp	unknown	4	success or wait	1	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsfAB4E.tmp	unknown	26442	success or wait	1	403269	ReadFile
C:\Users\user\AppData\Local\Temp\nsfAB4E.tmp	unknown	4	success or wait	3	405E84	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe	unknown	16384	success or wait	16	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsfAB4E.tmp	unknown	16384	success or wait	28	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsfAB4E.tmp	unknown	4	success or wait	1	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsfAB4E.tmp	unknown	4	success or wait	2	405E84	ReadFile
C:\Users\user\AppData\Local\Temp\nsfAB4E.tmp	unknown	4	success or wait	19411	405E84	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armoniac\Urokkeligheden.Ord114	unknown	2	success or wait	318	4026D2	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Obeyeo.Bib	unknown	1052672	success or wait	1	10002965	ReadFile

Registry Activities

Key Created

Copyright Joe Security LLC 2022

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Spaan	success or wait	1	40242E	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Spaan\Pushfully	success or wait	1	40242E	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Spaan\Pushfully	Trials101	binary	FF C0 52 EF	success or wait	1	40248E	RegSetValueExW

Disassembly

No disassembly