ID: 634596
Sample Name:
SecuriteInfo.com.generic.ml.22865.12721
Cookbook: default.jbs
Time: 14:04:15
Date: 26/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

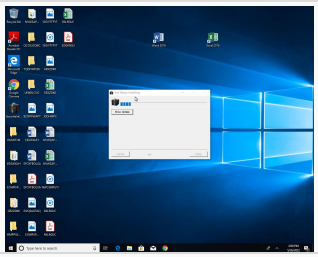
Windows Analysis Report

SecuriteInfo.com.generic.ml.22865.12721

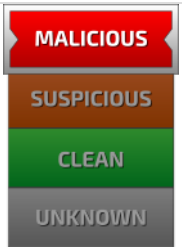
Overview

General Information

Sample Name:	SecuriteInfo.com.generic.ml.22865.12721 (renamed file extension from 12721 to exe)
Analysis ID:	634596
MD5:	deb3e51a2d7d56.
SHA1:	a780f7bbf2255a7.
SHA256:	4b4bb7b5e2fbe3..
Tags:	exe
Infos:	



Detection



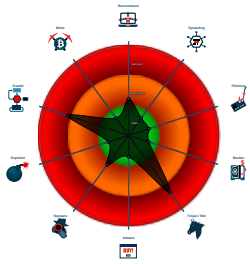
GuLoader

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- PE file does not import any functions
- Sample file is different than original …
- PE file contains strange resources
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.generic.ml.22865.exe (PID: 6612 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe" MD5: DEB3E51A2D7D566C86B22046C1058F1A)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://www.fides-kenya.com/yem/wam.bin"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.886303775.0000000003200000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

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

Networking

C2 URLs / IPs found in malware configuration

Data Obfuscation

Yara detected GuLoader

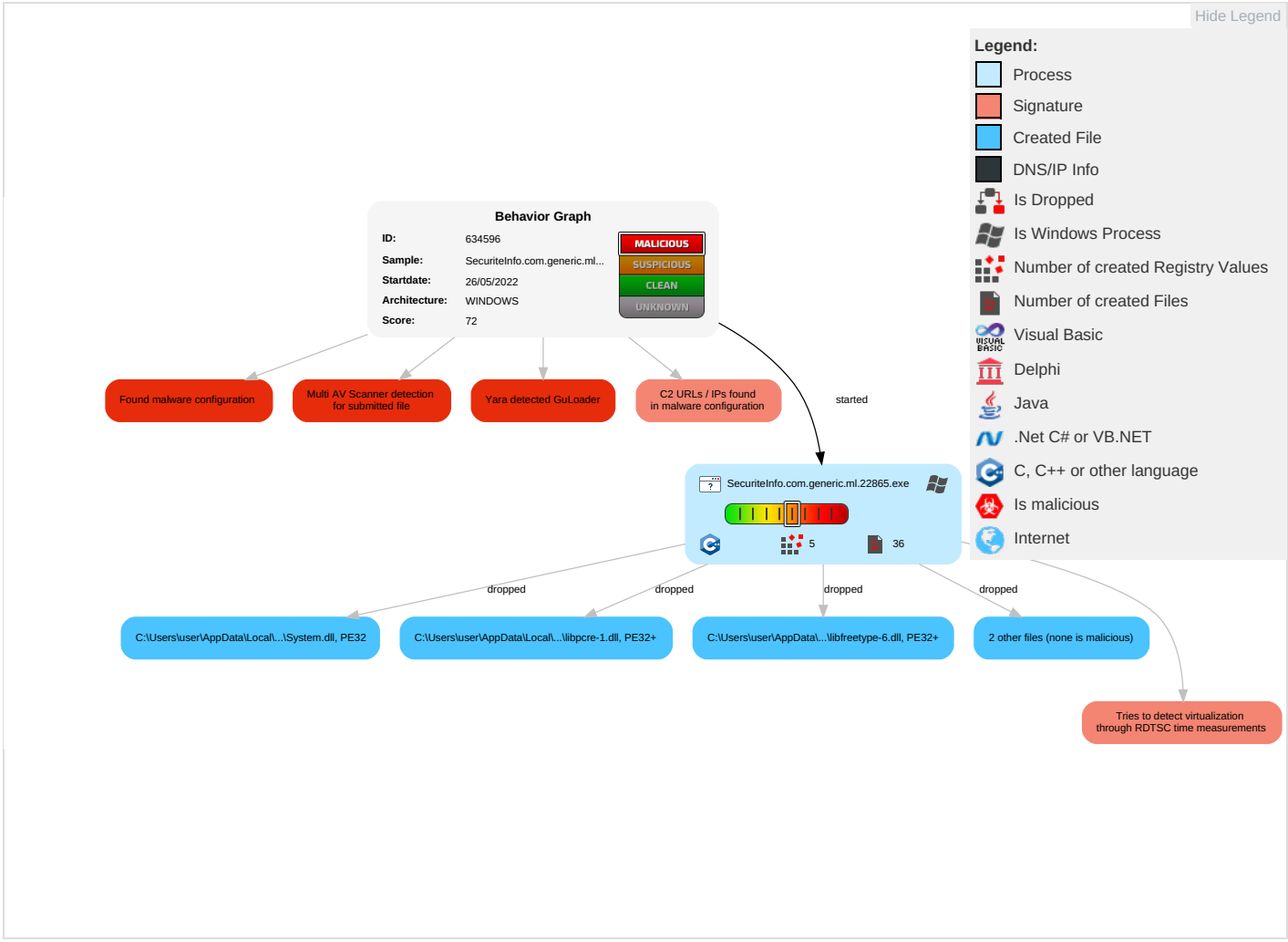
Malware Analysis System Evasion

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 Windows Service	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 Windows Service	1 Obfuscated Files or Information	LSASS Memory	1 Query Registry	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)	Obfuscated Files or Information	Security Account Manager	3 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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 3 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

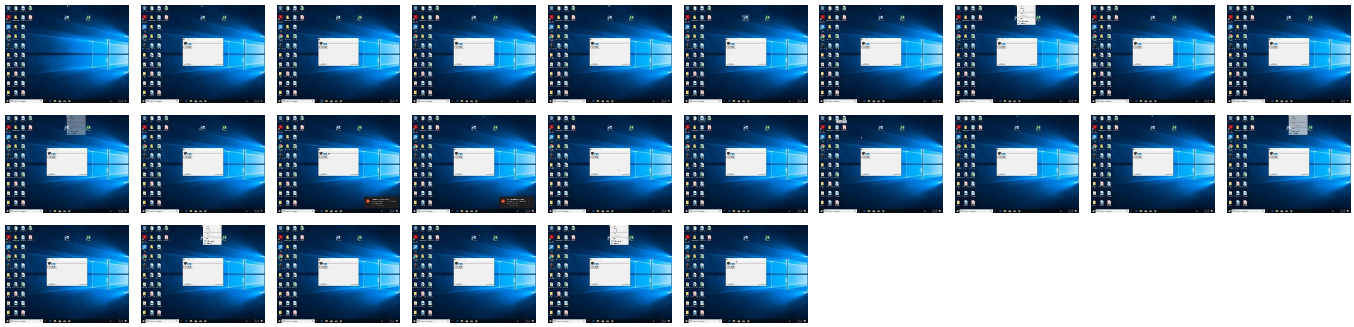
Behavior Graph



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.generic.ml.22865.exe	9%	Virustotal		Browse
SecuriteInfo.com.generic.ml.22865.exe	6%	Metadefender		Browse
SecuriteInfo.com.generic.ml.22865.exe	19%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\MpCommu.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\MpCommu.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MpCommu.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\lang-1034.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\lang-1034.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\lang-1034.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\libfreetype-6.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\libfreetype-6.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\libpcre-1.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\libpcre-1.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\libpcre-1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsh9F2D.tmp\System.dll	2%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsh9F2D.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsh9F2D.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.avast.com0/	0%	URL Reputation	safe	
http://www.fides-kenya.com/yem/wam.bin	0%	Virustotal		Browse
http://www.fides-kenya.com/yem/wam.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.fides-kenya.com/yem/wam.bin	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.avast.com0/	SecuriteInfo.com.generic.ml.22865.exe, 00000000.00000002.885721867.000000000285C000.00000004.00000800.00020000.00000000.sdmp, lang-1034.dll.0.dr	false	• URL Reputation: safe	unknown
http://creativecommons.org/licenses/by-sa/4.0/	network-server.png.0.dr	false		high
http://scripts.sil.org/OFLSource	SecuriteInfo.com.generic.ml.22865.exe, 00000000.00000002.885721867.000000000285C000.00000004.00000800.00020000.00000000.sdmp, SourceCodePro-Black.otf.0.dr	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	SecuriteInfo.com.generic.ml.22865.exe, 00000000.00000002.885721867.000000000285C000.00000004.00000800.00020000.00000000.sdmp, MpCommu.dll.0.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.generic.ml.22865.exe	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	SecuriteInfo.com.generic.ml.22865.exe, 00000000.00000002.885721867.000000000285C000.00000004.00000800.00020000.00000000.sdmp, MpCommu.dll.0.dr	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordDigest	SecuriteInfo.com.generic.ml.22865.exe, 00000000.00000002.885721867.000000000285C000.00000004.00000800.00020000.00000000.sdmp, MpCommu.dll.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	634596
Start date and time: 26/05/202214:04:15	2022-05-26 14:04:15 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.generic.ml.22865.12721 (renamed file extension from 12721 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:	19
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:	mal72.troj.evad.winEXE@1/15@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.8% (good quality ratio 61.6%) • Quality average: 88.8% • Quality standard deviation: 21.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:05:30	API Interceptor	1x Sleep call for process: SecuriteInfo.com.generic.ml.22865.exe modified

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\ArtDeco_green_6.bmp

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, frames 3
Category:	dropped
Size (bytes):	5273
Entropy (8bit):	7.8459330085163606
Encrypted:	false
SSDEEP:	96:BSTzREvsu6i0msHhj/HJBGZgCCoRPpr0wIqPnKV1+zNdgyJN6zx+f:oXRduqmuH7WTCoZpr0wIKnqtBy
MD5:	87BD29AF594463CC21D67CDC21F5B782
SHA1:	ED6D1F8936D968BE1DDAE4E38C3C38697B9BC038
SHA-256:	4D24FDEE4E7EC7B701C7148481B4EDD0D7941FD3656F4AED722D35F4FC2B9E1D
SHA-512:	80BF149D0246932A1139FC9B7ADD97B73B66BA8DE1C2905381520C535CC712AECBEDDC33B81A0770E73D3C4F6036974CD66B0C26F9CD4F16EF8FADE97E395 73
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d.....:Exif..MM.*.....Q.....Q.....aQ.....a.....C.....C.....n.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....(...(...(...(...(...(...(...(..Q.Y.Y~..$.m.x.Y..>?Muw..+....}x.w.$....$.o.v.....v.....&6....s.....>...~..?.<..m...i.f..?g\{.`..:....& .|...)..9'8.....Z.3...."U*s?y..e/.1.\..... ..0_..'.<..@...3K/.-.]4k$../..\....O....:..q.d.?.>...}.....$o.s...T.l1P.F.0..X.\.c_.v.....G .U.H..:.....N@u

C:\Users\user\AppData\Local\Temp\MpCommu.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	349736
Entropy (8bit):	6.164191441093237
Encrypted:	false
SSDEEP:	6144:kj1LBBf6sKCJIELSHbz0RzFu8xbpr+6vl:GBBwyLAMJFuw
MD5:	DFA10F926778550AB0BB0804629686D2
SHA1:	33CEA03A49A941ADF49BE28F797D8E76E1D83828
SHA-256:	22136256BF7D3D9F96B21C32A5409CF014705C7673787A6ACC8C0CDCACC2F9F5
SHA-512:	7E9C97E2C667EF7C1E35C5C6B777A2A458BB8D42B5355B13E164C4F4F857788EB127651CD1947C87BBECCE9ACDE210DCF9AC186C85769669F0CAE055AD217 45
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R{..<(..<(..<(.=)..<(.8)..<(.?)..<(...(..<(..=(..<(.9)..<(.<)..<(.2)..<(..(..<(.>)..<(Rich..<(.....PE..d...r..6....." .....l.....P.....f.....`.....1.....`A.....`.....0...h....@..(.....2.....(<...P.....P...T... .....x...(...p..... .....text....j.....l..... ..`.rdata..$N.....P...p.....@..@.data...l".....@....pdata...2.....4.....@. .@.rsrc...(....@.....@..@.reloc.....P.....@..B.....

C:\Users\user\AppData\Local\Temp\OLIGOCARPOUS.SNO

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	data
Category:	dropped
Size (bytes):	144776
Entropy (8bit):	7.53285913295622
Encrypted:	false
SSDEEP:	1536:uPIMC3CoPO4bEtoxzYk55G6J9reDiy8rdsidRg5PdNdxCNBXl6ZjvhvzIMAzys3E:WIv7OSX269rUmsWXl6ZjvnAzys3OqwL
MD5:	1CA9D8B65434B23BBB1F878FB7E15B45
SHA1:	B08D04A9B064652238DAC280153990D8556AAD9E
SHA-256:	A0631B0E00F3221BC06C36AF0B18D8528603CED8491173AFA9F955C91C9F90E2
SHA-512:	2D94B7E8A9352FE149CD305529A45FFC5099B7E6C2FA55B83A615F216C7C6207373768734C67CE9750A60E18E8A8718EDE1D2CEF194ED3E1746B704B8D15C24
Malicious:	false
Reputation:	low
Preview:	m.7..y.....3....y..>,..'h,....Sc.....L._z.kM..z.....).....@y9...7H.}..`.Li.1.^.@b.G.....M.q.F&.0.h[&.....0..^=.....Is$.....C*A&..ox.*r.foM...W{fUkR.^...(..W...k....%.o..r.... q.Zw..!.....:.TT.vm<..+.y(..],.I.5X'R>.|.#..f.}..|z0.g.....~..N..W+...Y...h.....g...._[1.....0.n..I(n.s...>oC..%4+....Jh....f.k..1P..=.a."..W.....-...."q;.....%...h....7.`.....9..+...@!. ..G.~2>r.J.\.l.u.x...o...#d....)M.S5X.&...Q.d|93.... |D"...vg..6D.%[.~.....u.o.R.o|*.o.@3.T....,..~./..|.,.....j.....LZ....n.....QM..._...r]a...JPJ.9j..6.uK.....v2*.....z.ZC.qzz.`.....J...4.0 c!....Q.I.W...z|.K~T..Z.{.cnG.....E=...A..2.t.A..0...c.....\}?..JKQ...h..".37.;...jg.U.~d.....<...W.e.x.@@.1..^O.....p.Gj.H.R..B.E...]..n..Z..ot.. ...i..._...AyU.L...../.....:y... M.h....M.G...K.w.....~Z.H~.e..`.;.9.!.1*.....O..0..]..... 6@.V.g.....F.@A.'K.w?.vGHB...Fgk'[....a1..T.C.....*.wM.4...;+..g3(r...T..&?)...5..../.8._.x1X<y4.!

C:\Users\user\AppData\Local\Temp\SourceCodePro-Black.otf

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	OpenType font data
Category:	dropped
Size (bytes):	134872
Entropy (8bit):	6.990627903031805
Encrypted:	false
SSDEEP:	3072:sz0DOC7z/NU32nX3CC38LWDvzsGgDHKEqnk8X+5s9n5cWY2+o:57z/NU32nkWDvRzBl+5s9mWYvo
MD5:	49776B1F23800D9C82D529FCC027D16D
SHA1:	7BA6D923A0D163CE16DA4DD1105945C47406CADC
SHA-256:	78ADEC30836955EDFB3968D23F79662A64E62B5DE236C64FC9964C7632D83963
SHA-512:	252DEDE5F71BB6736DCFC76D0CBF52B0FA01D92813CF4A74714C9D271C10286336405C15A06778E3617B7485030FC1D9FB314A6BB302446F299162C22C0068BF
Malicious:	false
Reputation:	low
Preview:	OTTO.....`BASEe.].....FCFF .....FL....DSIG.....GDEF.....,....GPOS.{.\.....GSUB..].....JOS/2.....P...`cmap.spB.....3fhead..h<.....6hhea.3.s...$...$hmtx...~.. .....Bmaxp. P....H....name...7.....post...3..F,... .....4.]._.<.....*.:...$.....X.*.*.....P.. .....X.....X...K...X...^.2.,..... .....8.....ADBO... .....`..... .....J.~.....$.....<.....H.....T.....`.....l.....&.~.....&.....*.....6.....D.*.....:.n.....2.....$..... .....D.*.....*.....H.....*.....d.X.....&.....4.....4.....2..... .<.....4.\..... ..... ".....4.....$.F..... .j.....,.....0.....

C:\Users\user\AppData\Local\Temp\analysekapitlet.ini

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	38
Entropy (8bit):	4.438588368649811
Encrypted:	false
SSDEEP:	3:9J7KCE/VJOKkJe:9XE/Vwc
MD5:	2904F70F565669B3C2799CD77F98909F
SHA1:	567E83FD531B1530D2476B43AE79114D543B195A
SHA-256:	327226A389956762200BA7198625E1DEB03D036CB218E8F1AFD7C9B727AA32EE
SHA-512:	F0BD8A19527942FE0170E001F36D0A4234A5D049D897A2B7A225C061A9B2B5C0E37E2BFE0B2BB945464B90E6BDD7922E4E8A62EF0686D7A09E2F544FBA2A54A 3
Malicious:	false
Reputation:	low
Preview:	[Disfellowship219]..totempl=Forgrown..

C:\Users\user\AppData\Local\Temp\applications-system.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped

Size (bytes):	852
Entropy (8bit):	7.714388915009416
Encrypted:	false
SSDEEP:	24:PUalwngqdk8kgfLRaKT4+vZsnKzajzkPTD+3xc:MWckSLRj4+vZsKzajzkPTWc
MD5:	C007F7CF6900C902101AF7DEEAB1A81D
SHA1:	7A10B42A75F63FB53D5FAB96A9521D91FB639C35
SHA-256:	3237623948F6A90DE7731BC8E50C212DCD356220F84A74615A52820446B22CC9
SHA-512:	0CE9BD720137D084ED622B517F968ADF659C30BD89F04D52B11FC1B16E9BCEC27FDCAF64F24522B4F1818FD9F09AB79ADD18819D0A385D52A390ADD8D3E90A27
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....IDATx.u..pCg8.m...8...p...X..m.q.....2..g..k1W.....\.c8.6..2}nt.:."......e...E.).....f`~ifjniJ....l.....Rf.X./,.g....s..K.. . .t:@...P$....4.oh\|.....L\|.t9.....e..Y..\.[..#}...>U.`7.....}j\|r.....`.....e.D2>.'..J....l.@..m.j5.`.B-.F.tvv..?..X.."d..Y.J..pOff.M.l..Y9...*.\,.....EGW.....y\GW.lht.....pw....4'.....YX..~Ee.T..*}..j["".....A.l6+.o....$.[....u.....*.lBumE...b.W.T3S.X..qvQ..T.#.....J.....j.....W.....PP .AGO.i]CM.?...^i.h.[.....,_.{.+.....`{ay.,WH./.@K[.Qk{s.:XWfee]....v{W+"...Uj%TV.....x....,..%.E!...k....Ag.....w...7.....a....((.G2.....%..G...B.n....K.b....."..y@..<95v.9.p./R3...0..yerr.5.MIK.c..._.....;eHrJ.^Rj.2)9.....ugrj.D*...d.rj"+-#%h...O.D..?...Itt.-..[.....Q..c....cb...!..z.....)..]...&..H....IEND.B`.

C:\Users\user\AppData\Local\Temp\lang-1034.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	173064
Entropy (8bit):	3.693018919711273
Encrypted:	false
SSDEEP:	1536:pS8DwEnRUjJhZpn9uf9Zmzv7kLV2B68v+JqL/wX8P66QhaF5tVw:s88LDZpncqzv7orc+JqL/wXhlaF5tO
MD5:	4F18D3455ED4916E37CAE7DC97E4F281
SHA1:	B8C07DD3C97231EBD51A4AA9DB64E32378AAE1E2
SHA-256:	9254A461B08B2CEEC9B70B733DB20D83CED38928BB36CB4AFBBC2CE70EC4A709
SHA-512:	589875F2066D05AD61B1508D2AE69EE5F8648FC0505BD1B6DCD341382CFD87DFE3E12885096B5B506C0D86D8342355AED2320961921CBB5E6E2FBC6A7033181
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R...R..R.@...R.@.P...R.Rich..R.....PE..L....\)b.....!.....".....@.....~.....rdata..p.....@..@.rsrc....~.. .....@..@.....\)b.....T.....rdata.....T....rdata$zzzdbg.... ... ...rsrc$01.....@...^...rsrc$02.....

C:\Users\user\AppData\Local\Temp\libfreetype-6.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	740140
Entropy (8bit):	6.445034069568258
Encrypted:	false
SSDEEP:	12288:m5h4fluyHZyxAW+RHDfi7qmkLpRxNRcldaxSqKfEWmjJthNw:m5Gy+mHL6qXLPv0dax3vZjJthNw
MD5:	0F0A450E617F355FCA577DED02E52EDE
SHA1:	AEB92363E754D5EE6DB1E634C04EB1EFE6E3276B
SHA-256:	161E0693AD4FE7E9EB411411AD72697FCB7BB18BF0BCAE2D884A52875B0CD2F8
SHA-512:	26A05A5B794C56FC2C4B794CE38598F78124B89AE8C815BB0F487EAD639B7039FFFC5067D2A1E22455FDE69BE8E70D97663E9C9B1D7A2CD3753F92303717BDA2
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....8..}.....&"...%.x...4.....P.....b.....Cy....`... .....@.....`.....E.....x..(.....@d.....text....v.....x.....`..`.data.....\|.....@....rdata.....~.....@..@.pdata...E.....F...j.....@..@.xdata..XG.....H.....@..@.bss.....0.....edata.....@.....@..@.idata.....`.....@....CRT....X.....$.....@....tls.....&.....@....rsrc.....(.....@....reloc.....,.....@..B.....

C:\Users\user\AppData\Local\Temp\libpcre-1.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	281695
Entropy (8bit):	6.168605016920544
Encrypted:	false
SSDEEP:	3072:uD/iPx3WGmBoVKxtW0qib30Mj/vYYoGtjGeIGA9R23m6+PiaAtB3NFUQ8:uTUGprc6HfIG86+adX3NFUQ8
MD5:	A4E14B1F3042BFBF0B018561F8611D93
SHA1:	5C4C26F66ADCC1B40D7FF3113701FD9DCA9F74E6
SHA-256:	624E1E55F227897EB6E5852D28F0448F25ADE61A98894789FD45A3F8AE32D0EA
SHA-512:	DA4D86DF061948A37D513132686E91E13960FA28EB427BB841E0DACBF91564B3713DE6CA5EE49D17C0E1B449C0252EF9F4E8C02205BF2169CA7D761DC387280 2
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....F../.....&"...$.....B.....P.....e.... .`... .....5.....P..... ?..(.....X.....text.....`.P`.data.....@.P ..rdata.. z.....|.....@.`@.pdata.....P.....&.....@.0@.xdata.....`.....,.....@.0@.bss.....p.....`..edata..5.....2.....@.0@.idata... .....:.....@.0..CRT....X.....@.....@.@..tls.....B.....@.@..reloc.....D.....@.0B.....

C:\Users\user\AppData\Local\Temp\lilas.lnk

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun D ec 31 23:06:32 1600, length=0, window=hide
Category:	dropped
Size (bytes):	956
Entropy (8bit):	3.058049005002623
Encrypted:	false
SSDEEP:	12:8wl0GsX2lw/tz+7RafgKD4Tb6cNlb6cDQ18/+CNJkKAb4t2Y+xIBjK:8dTaRMgKsTb6kb6fSPHAJ7aB
MD5:	FE7B156B846B0136F2569EA0FD23CDDD
SHA1:	358C6D45DB9A4F969414DFDD14876AB10243027D
SHA-256:	A2A111EA2717C3E0FA8742D00DD7314BF1B0636AC7043173568364869E33B5BE
SHA-512:	7848BDD99C823CE6B242BBA001577957A5F2D4FB50B4B50E182165D36EB64B4FAE470C6910F264F8D8AE91088E28FCAE314DE09E8B8C14837E7E1C294140A86 2
Malicious:	false
Preview:	L.....F.....9....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....Z.1.....user..B..... .....e.n.g.i.n.e.e.r.....V.1.....AppData.@.....A.p.p.D.a.t.a.....P.1.....Local.<.....L.o.c.a.l.....N.1..... .....Temp..:.....T.e.m.p.....l.2.....TOLVAARIGE.exe..N.....T.O.L.V.A.A.R.I.G.E...e.x.e.....\.T.O.L.V.A.A.R.I.G.E...e.x.e .$.C.:.\.U.s.e.r.s.\.e.n.g.i.n.e.e.r.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.....(.....l^".`G...3..qs.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9 .3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

C:\Users\user\AppData\Local\Temp\microphone-hardware-disabled-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	223
Entropy (8bit):	6.55427581037989
Encrypted:	false
SSDEEP:	6:6v/lhPys5+G7Zv9TOdnE/q5KBdsu4TmS/Vp:6v/7ZZBOl9K5e
MD5:	AA3A4757FF50F980EC23D5A65F6FBC0D
SHA1:	ABA35FCE13E7EEC52BDCD1756AB6AC7F3CBE0B17
SHA-256:	3E4429457A1C313920FAFE775494BBA5049BBFA41A4F29789CCC19432FD89348
SHA-512:	C26C744CE5149634D6698A7181F1F08668FEA902004BDDF0EA011097D139A58173ECE62B22DA376608406AA1A1FC65B496EF1373E1C6B532C430240F3AE7CF8F
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...=..1....*.....QY...s.q...`+...Z.TK..+....$.^!..[,.>.g.q.1.a.Q.2L/..R,..*w...Z.3?5.Qu.SE.o(..c..!..h...1....K.B;..3.y.Z..yh7M.N... D.....z'.....)....IEND.B`.

C:\Users\user\AppData\Local\Temp\multimedia-player-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	218
Entropy (8bit):	6.548843212391007
Encrypted:	false
SSDEEP:	6:6v/lhPysNBnmGKjdTJ8K49bFOk7K8ml2up:6v/7tBm5pJ8K8bFYl2c
MD5:	FDD6EA8CAE0923DB4A381DB85A2D1DB8
SHA1:	7906C57D827F884958F72BBD1C67A52D48566F13
SHA-256:	E53F28526B8E67491CD5CB7D1CBC0402F0D6FCB5C8C8E9428BFDD1D46AE1D7F2
SHA-512:	FDC59FA991F2EB0770A6D54B892BE9F635F35A4D5FB258D5D8259C1BD30574B24892E9DC1936CCD012366578EEDB5B0FDD989B2544842B25D45B77653BE157D9
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8.....0...P.h.h..a..{0cr....$'...O.!...;...v....@q..#gu.....C._.p.=... .....{G.....X$.....F..7i.....@....3.....$..p..E..LwO'n...F1.[.tn....IEND.B`.

C:\Users\user\AppData\Local\Temp\network-server.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	718
Entropy (8bit):	7.267310509580342
Encrypted:	false
SSDEEP:	12:6v/7maZB4RO4HE+swFIUyrlxSTWLCMpffTn0589Gug9Beu1qG6Fh1ClN:tak15ypxST1MpffTAjv9R1dujmN
MD5:	151CC83E1B8F2239625A521AD3889884
SHA1:	F6951B61B7BE182EE6493DD7CB02DDF5EBE2BCB3
SHA-256:	B698DFD02677369423FDA9D0A2C499A1B7788A4AA3D500D20E1DFBDC47E64599
SHA-512:	A23168D29CFF32344EEA6C2D2895FD8055C5318074C0EE34DCEEC391630350E98A9D8813736ADB49EE87D8B2F02FE219E08811F569887F846D400D92A66DD08
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....o.d....tEXtSoftware.www.inkscape.org..<.....tEXtTitle.Adwaita Icon Template...?....tEXtAuthor.GNOME Design Team`.v~...R tEXtCopyright.CC Attribution-ShareAlike http://creativecommons.org/licenses/by-sa/4.0/.Tb.....IDAT8...Ok.Q...w&.S.V.....`..&P?..].N..R.....Eq..Ih.....d..CG.vH'..<.m.M" 8xW.w...R(I.V?Vnz.'..)e].6.....i...Y)...TTZ..e....&..{..r...h.a...PJ...p..D..A.C|.GX..~E[.v.I....>{.G..#..\.%...u.(.\`...z=...ss.qw\>mm....@_~...[...L.c.1..*..4..O.q.,^b"5.@..>..+...".F. .."9...j....L.G.....J.../.[....TJ..b..X|.....Q*.74M.k..J....pt{A..~.....a.2..z..n.w.M...P..~6s.....l~.m.`...w....?~.2.....WQ...d..e...Yc.-..{._b....K....IEND.B`.

C:\Users\user\AppData\Local\Temp\nsh9F2D.tmp\System.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 2%, Browse • Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B..... ....

C:\Users\user\AppData\Local\Temp\task-past-due.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	562
Entropy (8bit):	7.483849388462199

Encrypted:	false
SSDEEP:	12:6v/7F9WLE/mpAJyXrrPWBQXhKTclrG/9/8W8OInefodAbctQ2TpmOtaxXc:q9uKIPuQXhKIhrOaefkA4tQ2EQ
MD5:	7A1C7CD0874509E35CA8738D6426EC61
SHA1:	02964393DAD3BB1EAA38C7315E80CA32B1C16B95
SHA-256:	8E1E44F59B17C6BFF086F0B2DD4DD1325DF9CD276629BC7ABDBA6719DD76289F
SHA-512:	74527D173C08228EE551E7BC54460B3E2B8ABA6A2C964C736EB92F3B6AEB576026C96B9DA1C78A72E854D44258E1DD3ABFCD2F01C81D0784559CEC0A2848E1E5
Malicious:	false
Preview:	.PNG.....IHDR.....a....IDATx.....Q.Fk[A....66k.m....m.m.....$93...A.~C".<..?t.....%....=.A!./.?l..x.....:<yv...uhmka.....j.?[...+..dE..U/Y....X.j..P.h..o%n....X..G.?....X5..-.e...k.l..L..T..gO"==.U.e.HKK.3'.D"a....`....P.l..B.....|..;wo..W.^....ove..p....I.....(--EEE.O.9.....4Jm.!.ttt ,4.:..uuu.AYY.TJ9.r.....S....~..8.....B..B..#))I..!.....".A..9.+....4Ju..Z.....w..x..mu.*...VW...0_|`...Q...H.=.<..?.m....A.`....8:...2.....#P..F..1...=@..P..l.....a}./.....x...w.!....."_.w.....IEND.B`.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.905193911181419
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.generic.ml.22865.exe
File size:	912777
MD5:	deb3e51a2d7d566c86b22046c1058f1a
SHA1:	a780f7bbf2255a7dcd963c80fad20ee164ca6b93
SHA256:	4b4bb7b5e2fbe3814fca75d1ab132a97c67255ebfe6dc4f3312d64483a181286
SHA512:	c68bfec94fe42bea3b7c5f088963ff57d07866e8f773b290ca4b04422e5d34938b9c56e17ada69cd5bf0087fcf1f70551132ca0de21949c579615c296b1f3410
SSDEEP:	24576:sYii5KdghcAySSqmCJD8TWNaR87OxF7IziqjGFb:FiMKSjiqZJgTS9AFemb
TLSH:	551512640F9AC417E371C0FAA9B7C6486B76C9083E798481CFF61F75A678BAC5817183
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....

File Icon

Icon Hash:	70f8adbcb8bca828

Static PE Info

General

Entrypoint:	0x403640
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:	0x614F9B1F [Sat Sep 25 21:56:47 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
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 00007F962CBC95AAh
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 00007F962CBC957Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], 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	0x63000	0x14ec0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
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	0x6676	0x6800	False	0.656813401442	data	6.41745998719	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	0x20378	0x600	False	0.509765625	data	4.11058212765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x38000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x63000	0x14ec0	0x15000	False	0.326160249256	data	5.55589914674	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x63298	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x73ac0	0x25a8	data	English	United States
RT_ICON	0x76068	0x10a8	data	English	United States
RT_ICON	0x77110	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x77578	0x100	data	English	United States
RT_DIALOG	0x77678	0x11c	data	English	United States
RT_DIALOG	0x77798	0xc4	data	English	United States
RT_DIALOG	0x77860	0x60	data	English	United States
RT_GROUP_ICON	0x778c0	0x3e	data	English	United States
RT_VERSION	0x77900	0x27c	data	English	United States
RT_MANIFEST	0x77b80	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

Version Infos

Description	Data
LegalCopyright	Bademestersnona
FileVersion	14.20.6
CompanyName	fenolersfagins
LegalTrademarks	Indlststro
Comments	CARAGUATAUNACHI
ProductName	SKNSFORRETNI
FileDescription	ethere
Translation	0x0409 0x04b0

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.generic.ml.22865.exe PID: 6612, Parent PID: 1800

General

Target ID:	0
Start time:	14:05:23
Start date:	26/05/2022

Path:	C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe"
Imagebase:	0x400000
File size:	912777 bytes
MD5 hash:	DEB3E51A2D7D566C86B22046C1058F1A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.886303775.0000000003200000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsm9E60.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsm9E61.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsh9F2D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	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	2	405C22	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	2	405C22	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	2	405C22	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	2	405C22	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	2	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsh9F2D.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	405BE2	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsh9F2D.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW

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	405C22	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	405C22	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	405C22	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	405C22	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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\OLIGOCARPOUS.SNO	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\ArtDeco_green_6.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\MpCommu.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\SourceCodePro-Black.otf	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\applications-system.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\lang-1034.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\libfreetype-6.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\libpcre-1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\microphone-hardware-disabled-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\multimedia-player-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\network-server.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\task-past-due.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\UNDERMINERENDES	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\UNDERMINERENDES\Censoren105	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405C22	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsh9F2D.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	3	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\nsh9F2D.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	1	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsm9E60.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsh9F2D.tmp	success or wait	1	405DA3	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	406224	WriteFile
C:\Users\user\AppData\Local\Temp\nsh9F2D.tmp\System.dll	0	12288	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 00 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	406224	WriteFile
unknown	49969	16157	75 6e 6b 6e 6f 77 6e	unknown	success or wait	83	406224	WriteFile
C:\Users\user\AppData\Local\Temp\OLIGOCARPOUS.SNO	0	16384	6d fd 37 0c fd 79 fd 01 0b fd fd fd 33 fd fd 17 05 79 07 fd 3e 2c fd fd 27 68 2c fd fd 0d fd 53 63 0b fd fd 11 fd fd fd 1a 4c fd 5f 7a 02 6b 4d 0c fd 7a fd 44 17 00 fd fd 29 fd 09 10 fd 2e fd fd 40 79 39 0e fd fd 37 48 fd 7d fd fd 60 fd 4c 69 fd 31 15 5e 02 40 62 fd 47 12 fd fd 01 7f fd 19 86 fd fd 4d 07 71 fd 46 26 fd 30 64 68 5b 26 fd fd fd fd fd fd 30 fd fd 5e 3d fd fd fd 00 fd fd 49 73 24 1d fd fd fd 18 fd 0a 43 2a 41 26 fd 0d 6f 78 fd 2a 72 c7 66 6f 4d fd 07 fd 57 7b 66 55 6b 52 fd 5e fd fd fd 28 fd fd 57 fd fd fd 6b fd 02 fd 17 25 fd 6f fd 1d 72 0b fd 0a fd 71 fd 5a 77 fd fd 21 fd 0f 0b fd fd fd 05 fd fd fd 3a fd 54 54 fd 76 6d 3c fd fd 2b fd 79 28 fd 16 5d 2c fd 49 13 35 58 27 52 3e fd 7c fd 23 fd 03 66 2c 7d fd 56	m7y3y>,'h,ScL_zkMz).@y97H}`Li1^@bGMqF&0h[&0^=Is$C*A&ox*rfoMW{fUkR^(Wk%orqZw!:TTvm<+y(],I5X'R>|#f,}	success or wait	9	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ArtDeco_green_6.bmp	0	5273	fd fd fd fd 00 10 4a 46 49 46 00 01 01 01 00 64 00 64 00 00 fd fd 00 3a 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 03 51 10 00 01 00 00 00 01 01 00 00 00 51 11 00 04 00 00 00 01 00 00 0f 61 51 12 00 04 00 00 00 01 00 00 0f 61 00 00 00 00 fd fd 00 43 00 02 01 01 01 01 01 02 01 01 01 02 02 02 02 02 04 03 02 02 02 02 05 04 04 03 04 06 05 06 06 06 05 06 06 06 07 09 08 06 07 09 07 06 06 08 0b 08 09 0a 0a 0a 0a 0a 06 08 0b 0c 0b 0a 0c 09 0a 0a 0a fd fd 00 43 01 02 02 02 02 02 02 05 03 03 05 0a 07 06 07 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a fd fd 00 11 08 00 6e 00 6e 03 01 22 00 02 11 01 03 11 01 fd fd 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00	JFIFdd:ExifMM*QQaQaCCnn"	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\MpCommu.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 00 00 01 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 00 fd fd 52 7b fd fd 3c 28 fd fd 3c 28 fd fd 3c 28 d3 3d 29 fd fd 3c 28 d3 38 29 fd fd 3c 28 d3 3f 29 fd fd 3c 28 fd fd fd 28 fd fd 3c 28 fd fd 3d 28 fd fd 3c 28 d3 39 29 fd fd 3c 28 d3 3c 29 fd fd 3c 28 d3 32 29 fd fd 3c 28 d3 fd 28 fd fd 3c 28 d3 3e 29 fd fd 3c 28 52 69 63 68 fd fd 3c 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$R{<(<(<(=)<(8)<(?)<((<(=(<(9)<(<)<(2)<((<(>)<(Rich<(	success or wait	22	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\SourceCodePro-Black.otf	0	16384	4f 54 54 4f 00 0e 00 fd 00 03 00 60 42 41 53 45 65 1e 5d fd 00 02 0e fd 00 00 00 46 43 46 46 20 52 fd fd 00 00 46 4c 00 01 fd fd 44 53 49 47 00 00 00 01 00 02 0e fd 00 00 00 08 47 44 45 46 fd 0d fd fd 00 01 fd 2c 00 00 02 fd 47 50 4f 53 fd 7b fd 5c 00 01 fd 04 00 00 14 fd 47 53 55 42 01 fd 5d 05 00 01 38 00 00 1d 4a 4f 53 2f 32 fd fd fd fd 00 00 01 50 00 00 00 60 63 6d 61 70 07 73 70 42 00 00 12 fd 00 00 33 66 68 65 61 64 19 fd 68 3c 00 00 00 fd 00 00 00 36 68 68 65 61 06 33 00 73 00 00 01 24 00 00 00 24 68 6d 74 78 fd fd fd 7e 00 01 fd fd 00 00 0c 42 6d 61 78 70 06 20 50 00 00 00 01 48 00 00 00 06 6e 61 6d 65 fd fd 0f 37 00 00 01 fd 00 00 11 12 70 6f 73 74 fd fd 00 33 00 00 46 2c 00 00 00 20 00 01 00 00 00 02 09 fd 34 fd 5d fd 5f 0f 3c fd 00 03 03	OTTO`BASEe]FCFF FLDSIGGDEF,GPO S{\GSUB]JOS/2P`cmaps pB3fheadh< 6hhea3s$$hmtx~BmaxpPHname7post3F, 4]_<	success or wait	9	406224	WriteFile
C:\Users\user\AppData\Local\Temp\applications-system.png	0	852	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 03 1b 49 44 41 54 78 01 75 12 03 70 43 67 38 fd 6d fd fd fd 38 1e fd fd 70 fd fd fd 58 fd b6 6d 1b 71 fd 36 fd a4 fd fd 32 fd fd 67 fd fd 6b 31 57 fd fd 0c fd fd fd 5c fd 63 38 fd 36 fd fd 32 7d 6e 74 fd 3a fd 22 fd fd fd fd fd fd 65 fd fd fd 45 fd 29 1c 0e fd fd fd 66 60 7e 69 66 6a 6e 69 4a fd a8 2e 18 6c fd fd fd fd fd 52 66 fd 58 fd 2f 2c b0 67 17 fd fd fd 73 fd fd 4b fd fd 20 fd 20 fd 74 3a 40 fd fd fd 50 24 00 fd fd 06 34 92 6f 68 7c fd 7f 19 18 fd 18 fd 08 fd fd fd 00 12 00 fd 4c 7c fd 74 39 fd fd fd 05 fd 0a 15 fd 65 fd fd 59 03 fd 5c 0a 5b db c3 23 7d fd fd fd 3e 55 fd 60 37 17 00 2e fd 18 fd 1d fd	PNGIHDRaIDATxupCg8 m8pXmq2gk1W\ c862}nt:"eE)f`~ifjniJ.lRfX/ ,gsK t:@P$4oh|L|t9eY\ [#}>U`7.	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lang-1034.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 00 fd fd 3c fd fd fd 52 fd fd fd 52 fd fd fd 52 fd 40 fd fd fd 52 fd 40 fd 50 fd fd fd 52 fd 52 69 63 68 fd fd 52 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 0c 5c 29 62 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 00 00 00 00 00 00 fd 02 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$<RRR@R@PRRichRPEL\)b!	success or wait	11	406224	WriteFile
C:\Users\user\AppData\Local\Temp\libfreetype-6.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 00 50 45 00 00 64 fd 0c 00 00 00 00 00 00 38 0b 00 7d 00 00 00 fd 00 26 22 0b 02 02 25 00 78 08 00 00 34 0b 00 00 0c 00 00 50 13 00 00 00 10 00 00 00 00 fd 62 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 fd 0b 00 00 04 00 00 43 79 0b 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.$PEd8}&"%x4PbCy`	success or wait	46	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\libpcre-1.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 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 00 50 45 00 00 64 fd 0b 00 00 00 00 00 00 46 04 00 2f 00 00 00 fd 00 26 22 0b 02 02 24 00 fd 02 00 00 42 04 00 00 02 00 00 50 13 00 00 00 10 00 00 00 00 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 fd 04 00 00 04 00 00 65 fd 04 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.$PEdF/&"$BPe`	success or wait	18	406224	WriteFile
C:\Users\user\AppData\Local\Temp\microphone-hardware-disabled-symbolic.symbolic.png	0	223	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd fd fd 3d 0a 02 31 10 fd fd fd 2a fd fd fd fd fd 51 59 fd 1e fd 73 fd 71 fd fd fd 60 2b fd fd fd 5a fd 54 4b fd 0b 2b fd fd 14 fd 24 13 5e 21 fd 00 5b 2c fd 3e fd 67 fd 71 fd 31 fd 61 fd 51 fd 32 4c 2f fd fd 52 2c 13 fd 2a 77 fd 14 fd 5a a0 33 3f 35 fd 51 75 fd 53 45 fd 6f 28 fd fd 63 fd fd 21 fd fd 68 fd 13 fd 31 fd 1d fd fd 4b fd 42 3b fd fd 33 fd 79 fd 5a 13 fd 79 68 37 4d fd 4e 12 fd fd 44 fd df fd 1e fd 1b 7a 27 10 fd 02 08 fd 29 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dIDAT8 =1*QYsq`+ZTK+$^! [,>gq1aQ2L/R,*wZ3? 5QuSEo( c!h1KB;3yZyh7MNDz')IE NDB`	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\multimedia-player-symbolic.symbolic.png	0	218	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd 53 fd 0d fd 30 0c fd fd 50 fd 68 fd 68 fd 1c 61 05 02 7b 30 63 72 09 07 fd 0a 24 27 fd fd 12 4f fd 21 fd fd fd 02 3b fd 09 14 fd 76 fd 00 fd fd 40 71 14 fd 23 67 75 08 fd fd 1c 1c 09 43 fd 5f fd 70 fd 3d fd 1d 14 20 02 fd fd 0d c5 fd 7b 47 11 fd fd 05 fd fd 14 58 24 fd fd fd fd fd 09 fd 46 08 0a 37 69 fd fd 12 01 fd 40 fd fd fd fd 33 fd fd fd 0f fd 24 fd 22 70 fd fd 45 fd fd 4c 77 4f 27 6e fd 01 fd 46 31 fd 5b fd 74 6e 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dIDAT80 Phha{0cr$' O!;v@q#guC_p= {GX$F7i@3$pELwO' nF1[tnIENDB`	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\network-server.png	0	718	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 09 70 48 59 73 00 00 0e fd 00 00 0e fd 01 fd 6f fd 64 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 77 77 77 2e 69 6e 6b 73 63 61 70 65 2e 6f 72 67 fd fd 3c 1a 00 00 00 1b 74 45 58 74 54 69 74 6c 65 00 41 64 77 61 69 74 61 20 49 63 6f 6e 20 54 65 6d 70 6c 61 74 65 fd fd fd 3f 00 00 00 18 74 45 58 74 41 75 74 68 6f 72 00 47 4e 4f 4d 45 20 44 65 73 69 67 6e 20 54 65 61 6d 60 fd 76 7e 00 00 00 52 74 45 58 74 43 6f 70 79 72 69 67 68 74 00 43 43 20 41 74 74 72 69 62 75 74 69 6f 6e 2d 53 68 61 72 65 41 6c 69 6b 65 20 68 74 74 70 3a 2f 2f 63 72 65 61 74 69 76 65 63 6f 6d 6d 6f 6e 73 2e 6f 72 67 2f 6c 69 63 65 6e 73 65 73 2f 62 79 2d 73 61 2f 34 2e 30	PNGIHDRapHYsodtEXtSoftwarewww.inkscape.org<tEXtTitleAdwaita Icon Template?tEXtAuthorGNOME Design Team`v~RtEXtCopyrightCC Attribution-ShareAlikehttp://creativecommons.org/licenses/by-sa/4.0	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\task-past-due.png	0	562	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 01 fd 49 44 41 54 78 01 fd fd 03 fd 1c 51 14 46 6b 5b 41 1d fd 0e fd 36 36 6b f6 6d fd fd fd f6 6d f6 6d 7f fd fd fd fd 24 39 33 0f fd fd 41 00 7e 43 22 13 3c 14 08 3f 74 7f 14 fd 03 fd 25 12 fd fd fd 3d fd 41 21 ad 2f 03 3f 6c fd 0d 78 fd 01 fd fd fd fd fd fd 3a 3c 79 76 1f fd 0d 75 68 6d 6b 61 fd fd fd fd fd fd fd 6a fd 3f 5b 05 fd fd 2b fd fd 64 45 fd d3 55 2f 59 fd fd 7a 9a 58 0d 6a 13 fd 50 fd 68 fd 04 6f 25 6e ba fd fd fd 58 fd fd 47 fd 3f fd fd fd fd 58 35 1c fd 2d fd 65 01 fd 17 6b 10 6c 0e fd 4c 0c fd 54 fd fd 67 4f 22 3d 3d 05 55 fd 65 fd 48 4b 4b a9 33 27 3d 44 22 61 fd fd fd fd 60 01 fd fd fd 50 fd	PNGIHDRaIDATxQFk[A66kmmm$93A~C"<?t%=A!/?lx:<yvuhmkaj?[+dEU/YXjPho%nXG?X5-eklLTgO"==UeHKK3'D"a`P	success or wait	1	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe	unknown	512	success or wait	262	4061F5	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe	unknown	16384	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsm9E61.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsm9E61.tmp	unknown	31800	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nsm9E61.tmp	unknown	4	success or wait	13	4061F5	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.generic.ml.22865.exe	unknown	16384	success or wait	48	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsm9E61.tmp	unknown	4	success or wait	1	4061F5	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\spndingsfejlen	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Klarings	success or wait	1	406532	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Klarings\DIALEKTEN	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Knscellens122	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Knscellens122\tabulr	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Struldbruggism	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Struldbruggism\Redbook227	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Klinken	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Klinken\Supervision	success or wait	1	406532	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\spndingsfejlen	INTWISTING	dword	0	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Klarings\DIALEKTEN	Ratifikationsdokumenternes159	binary	FF D4 51 82	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\Knscellens122\tabulr	Expand String Value	expand unicode	%WINDIR%\Hjlpeprogrammet186.log	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\Struldbruggism\Redbook227	Expand String Value	expand unicode	%WINDIR%\Saxonies.log	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Klinken\Supervision	faststtende	unicode	Lagede	success or wait	1	40251B	RegSetValueExW

Disassembly

No disassembly