ID: 635338
Sample Name:
SecuriteInfo.com.Trojan.Inject.11626.30754
Cookbook: default.jbs
Time: 19:29:20
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

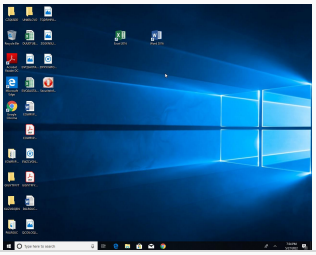
Windows Analysis Report

SecuriteInfo.com.Trojan.Inject.11626.30754

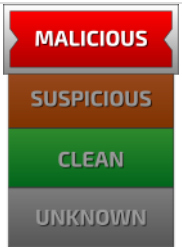
Overview

General Information

Sample Name:	SecuriteInfo.com.Trojan.Inject.11626.30754 (renamed file extension from 30754 to exe)
Analysis ID:	635338
MD5:	dd43bd8cdc55dd..
SHA1:	b7b49d8b277b6c..
SHA256:	7dc00d4ca525d3..
Tags:	exe GuLoader
Infos:	



Detection



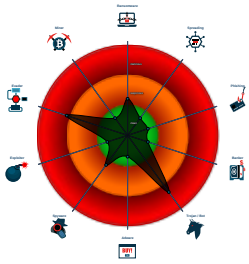
GuLoader

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
- Sample file is different than original …
- PE file contains strange resources
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Trojan.Inject.11626.exe (PID: 6384 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe" MD5: DD43BD8CDC55DD9C8A168F7D5E67DB30)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://185.222.57.79/SALES/muhasebe@par%20v4_zZlYyWbWEF39.bin1"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.790910785.0000000003291000.00000040.00001000.00020000.00000000.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

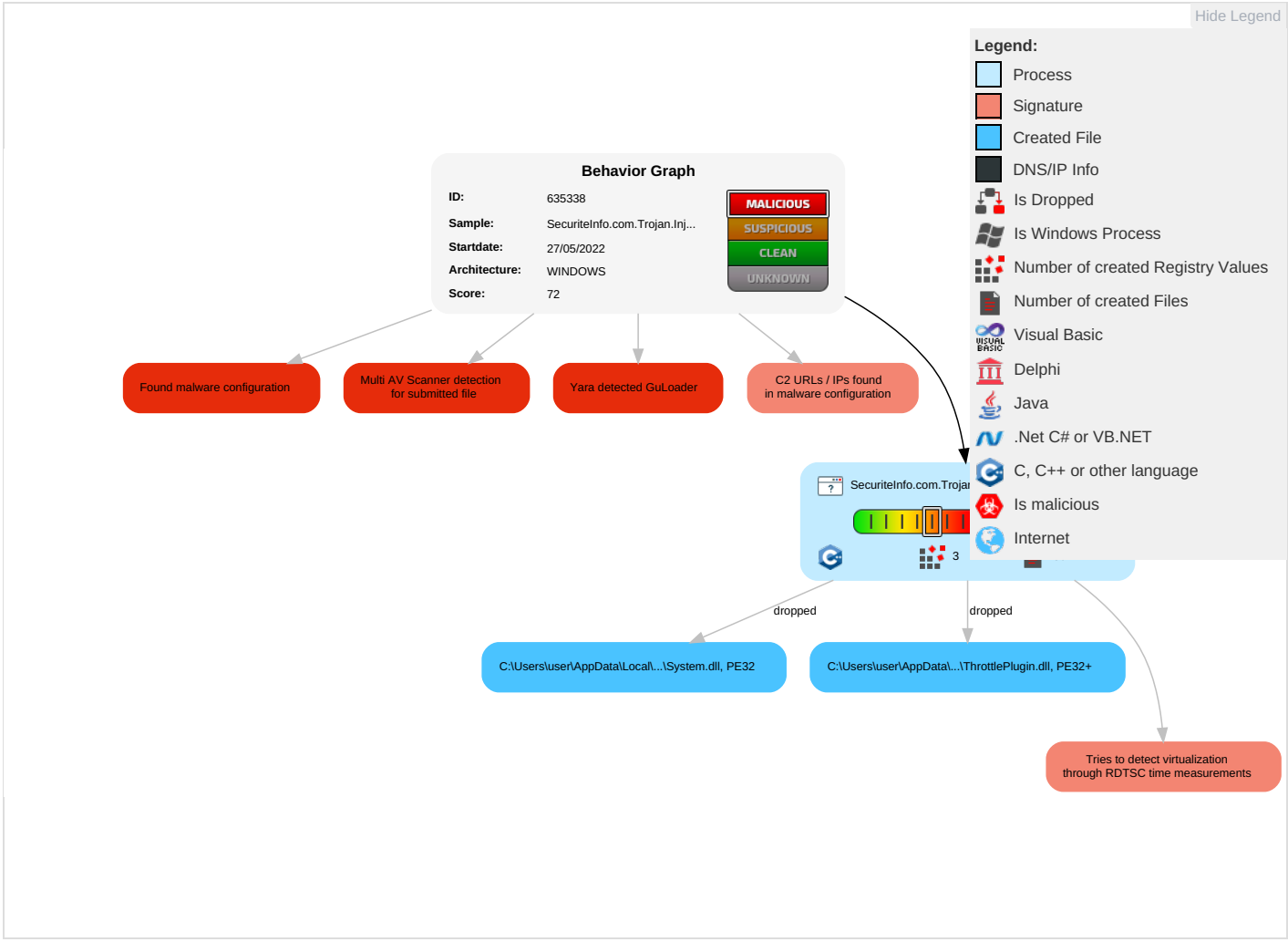
Malware Analysis System Evasion

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	Path Interception	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	Boot or Logon Initialization Scripts	1 Obfuscated Files or Information	LSASS Memory	3 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 4 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.Trojan.Inject.11626.exe	12%	Virustotal		Browse
SecuriteInfo.com.Trojan.Inject.11626.exe	5%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\ThrottlePlugin.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\ThrottlePlugin.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\ThrottlePlugin.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsaA34A.tmp\System.dll	2%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsaA34A.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsaA34A.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.222.57.79/SALES/muhasebe@par%20v4_zZlYyWbWEF39.bin1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.222.57.79/SALES/muhasebe@par%20v4_zZlYyWbWEF39.bin1	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://creativecommons.org/ns#DerivativeWorks	SecuriteInfo.com.Trojan.Inject.11626.exe, 00000000.00000002.789161040.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.11626.exe, 00000000.00000002.790363953.0000000002881000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.0.dr	false		high
http://creativecommons.org/ns#ShareAlike	SecuriteInfo.com.Trojan.Inject.11626.exe, 00000000.00000002.789161040.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.11626.exe, 00000000.00000002.790363953.0000000002881000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.0.dr	false		high
http://creativecommons.org/licenses/by-sa/4.0/	user-not-tracked-symbolic.svg.0.dr	false		high
http://creativecommons.org/ns#Distribution	SecuriteInfo.com.Trojan.Inject.11626.exe, 00000000.00000002.789161040.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.11626.exe, 00000000.00000002.790363953.0000000002881000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.0.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.Trojan.Inject.11626.exe	false		high
http://creativecommons.org/ns#Notice	SecuriteInfo.com.Trojan.Inject.11626.exe, 00000000.00000002.789161040.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.11626.exe, 00000000.00000002.790363953.0000000002881000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.0.dr	false		high
http://creativecommons.org/ns#Reproduction	SecuriteInfo.com.Trojan.Inject.11626.exe, 00000000.00000002.789161040.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.11626.exe, 00000000.00000002.790363953.0000000002881000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.0.dr	false		high
http://creativecommons.org/ns#Attribution	SecuriteInfo.com.Trojan.Inject.11626.exe, 00000000.00000002.789161040.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.11626.exe, 00000000.00000002.790363953.0000000002881000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.0.dr	false		high
http://creativecommons.org/ns#	SecuriteInfo.com.Trojan.Inject.11626.exe, 00000000.00000002.789161040.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.Trojan.Inject.11626.exe, 00000000.00000002.790363953.0000000002881000.00000004.00000800.00020000.00000000.sdmp, user-not-tracked-symbolic.svg.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:	635338
Start date and time: 27/05/202219:29:20	2022-05-27 19:29:20 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.Inject.11626.30754 (renamed file extension from 30754 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:	18
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@1/11@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.8% (good quality ratio 61.6%) • Quality average: 88.9% • Quality standard deviation: 21.3%
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, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, store-images.s-microsoft.com, login.live.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 NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

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\CYKELPARKERINGENS.ini

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	43
Entropy (8bit):	4.693479289485192
Encrypted:	false
SSDEEP:	3:JODb6MHIymy32ov:Jebozyn
MD5:	8B36E2227A5BD0472C64194B43581D90
SHA1:	E391FCABCE78C902A95B2B3A90F46380AA0E6031
SHA-256:	7A5D1B27408729909236B8B98CD3D19002750B7297981F32A6E6DD743B16BFB4
SHA-512:	FE426325981C65C37C16AE8021B2D8EDB50009743DC54C3EA2F496CA020BB980BCC43D70F5A2498A2AB8315183F5D2437DB72CCE69698978D927FA0E25DB137
Malicious:	false
Reputation:	low
Preview:	[Vddelber60]..Paxilla=EKSKOMMUNIKATIONERS..

C:\Users\user\AppData\Local\Temp\GL-1.0.typelib

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1245
Entropy (8bit):	5.462849750105637
Encrypted:	false
SSDEEP:	24:hM0mIAvy4Wvsqs1Ra7JZRGNeHX+AYcvP2wk1RjdEF3qpMk5:lmIAq1UqsziJZ+eHX+AdP2TvpMk5
MD5:	5343C1A8B203C162A3BF3870D9F50FD4
SHA1:	04B5B886C20D88B57EEA6D8FF882624A4AC1E51D
SHA-256:	DC1D54DAB6EC8C00F70137927504E4F222C8395F10760B6BEECFCFA94E08249F
SHA-512:	E0F50ACB6061744E825A4051765CEBF23E8C489B55B190739409D8A79BB08DAC8F919247A4E5F65A015EA9C57D326BBEF7EA045163915129E01F316C4958D949
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml">.. <head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>..<title>404 - File or directory not found.</title>..<style type="text/css">.. ..b ody{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}..fieldset{padding:0 15px 10px 15px;} ..h1{font-size:2.4em;mar gin:0;color:#FFF;}..h2{font-size:1.7em;margin:0;color:#CC0000;} ..h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} ..#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;..background-color:#555555;}..#content{margin:0 0 0 2%;position:relative;}...content-container{ background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}..-->..</style>..</head>..<body>.. Server Error .. .. <div class="co

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	40
Entropy (8bit):	4.412814895472355
Encrypted:	false
SSDEEP:	3:bAL2Wlv3AhWuvU2:bu2gYEd2
MD5:	176F3A8631F14F0421935D07502B8CD9
SHA1:	70C91B54BDE9BA107AB322ECACF16C60E0D8E57B
SHA-256:	F507F6BB14F286DD6835A18FC9ECDB86F73DBA96E9E281D626718447F1C496BB
SHA-512:	CC963E6BD3577D12FAC185D3D61CCC72098C52E5F2E907E5724BA7BC9FF022A2E74D0DF18D82AD7EC645FEE9328458B7493B1BDD7F1216A677A42F851656836
Malicious:	false
Reputation:	low
Preview:	[Godgrendes]..Resipiscence=Mightily197..

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	380640
Entropy (8bit):	6.00755593352656
Encrypted:	false
SSDEEP:	6144:tqpZKqQPNb5tPcACMBdK99Uf2o7nypI83l4tHY1706ePrz2lxf:tqEvcA49Ro7R64Pi
MD5:	07B4E869E84B557512EE38A5C283FEF3
SHA1:	85AFD748ACB7DB97C763ABFEA292E8543B084517
SHA-256:	C718B6BF9A427A117FFC1AB1C0E02551AFB2675406BAC625534E02179DB12C9D
SHA-512:	C1E7E9781B538D6FD1265DF135606483DCC80B190FFB6DE6C9A7C4DD83B2B4453C746FE7C4E4AE577BE5DD40D4BB98BE8D0325119148D81D8D3CD094E9260E7
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....$.....EK..+...+...+.....+...*...+.....+.../...+...(...+.$.*...+...,...+...-...+...*...+...*...+.$.....+.$.+...+.$.....+.....+.$.)...+.Rich..+.....PE..d...W6;a....." .....2.....$y..... .....P....`.....pK..T....K..0.....p.....!.....T.....(.....h.....text...<..... ..`.rdata.. .....@..@.data....%.....~.....@....pdata...!....."....@..@.rsrc...p.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\Waxiness.Sym

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe
File Type:	data
Category:	dropped
Size (bytes):	133983
Entropy (8bit):	4.053356129693858
Encrypted:	false
SSDEEP:	1536:0aDhpwRpeoT7/pL9vWX8iQC21Jl4YULhmlxv:0aTWeoT7/YUyVhmxv
MD5:	B364DBDF5A8A0C58CD4B721BE9432C48
SHA1:	B4159BD48769E110F77AC738B411ABFB73BE5A16
SHA-256:	1EE1B8AE17CE30ACC1DCC52DD1B0B569BB336E8D2E67E5DAC944B2D3DE4F0762
SHA-512:	CFE74620FF111A58B53BF6A495649F556E655C87BA3A4574346975D9A17D52F7140EB0DA76DBFA0D8CD33EE9525674B8BEBCF8E08CD833D66BBFA9229804978B
Malicious:	false
Preview:	.....

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced

Category:	dropped
Size (bytes):	685
Entropy (8bit):	7.621282940093077
Encrypted:	false
SSDEEP:	12:6v/7U+KyobNKxqUPO9/qRw6l2ZK2zirFLDbFJXy+MAg+eElsD8itXaBdHjGGrOKF:N+KyobksUVRqK2+LX/zlsYR3HjGCbx
MD5:	8C4F73C63672801A4629BA32BFAF9E31
SHA1:	C59877FEA56A2D45E36389366B0CCBC0AC2B720B
SHA-256:	DFAFC0CCDCD4A2B74B8F74ECBE0BE82FC9FF3D055A8C9585DD78379DB7F01063
SHA-512:	E4479DFE6F342212DA86B0B4BE1095162F07F7AE98AC1921CC9ED7BB650E7024CF80D1A82EA99D3744C9127FA046E82C81D4D82D17152D868DD7D1D78ACE205
Malicious:	false
Preview:	.PNG.....IHDR.....a...tIDATx.....ki.G.....pm.....c.m.v.....uNr...O.....".....\.B.....q.J.....|.^^^.....g....6..^..NV(..../.wAli.n.,,.....A~k....5....YwdS.....O/.s.9.k..|v.d.....<F.F.....z.9 CDn.IzeS.^.w.).V.0.?.._.-.....p?.....A.KV..}r...M.....<..p.....h.hEGg+.Z.$.jx7}LN....,....+...`..-N.6.8....T.T.r.zH.?...@.X...L.....fgg..{.....EQq....n.G..{65<.cD)d>.c..V}r.>z.S.D"...[.p.M.4>|.3|..7..j8:.@..5.s.P...N..P..Vi8..<3.g.5...hO..-d..Z.,.....A.Yc..3.5|.Nk.....I.7.*..a..x....2R.....sn..0..2...o....Q.)<A..M.....%`....P...Q.w. ..G.ggr.F..O5.`.5.(g...7.....3l.-d..,..1F..[t.l9.g..FX.....IEND.B`.

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	166
Entropy (8bit):	5.876785121167948
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllZMFnt4UoEw2GUqcklEj9h0XGqV/maXyj2flljp:6v/lhPysLEnt4UoEwsqckGpq6jy/jp
MD5:	A008C1D205C5B08639C0A8D8673C6C72
SHA1:	5190570B97A6F75F1D10D3D1EC6E46AEC8705B0B
SHA-256:	54A3EBAD22462339574D87D835CA626E039E9B38A625806BAA051F80A327C428
SHA-512:	AC5F3ED7773C04223650B757F6168FA4F6C57BA4F0C073BD5AB933B96F0FC3AEE918543C4AEA703A9F472045C6FC5CEA012935850F2971A8107772B96F341AB5
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....]IDAT8.c`..8.....>... F...4..u...IJ.....43B.....!..X.D.&rl.5...<...IPO.....R..3...W.....o2...M`....IEND.B`.

C:\Users\user\AppData\Local\Temp\nsaA34A.tmp\System.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.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\rt64win7.inf

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe
File Type:	Windows setup INFormation, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	1292652
Entropy (8bit):	3.864768543104337
Encrypted:	false
SSDEEP:	3072:veHaqq95T1TpRKkYxyZuSkIRipOp1MbSqh43FFc23lRxSsopQfql1Ody29kn1jYF:XaekadZaJiaeQMV
MD5:	2D947C4C9147622CFC588FC5C17DDDEC

SHA1:	B367B48D1282E39E37B8992615FF9947DEE8CFED
SHA-256:	EBB8155AC71DD53258CE3772F189B4771272BA55E15A6DABDE2BEA6896DC2CC3
SHA-512:	3213B423153A1350AA3A0213079EDF21D77022C7839EB3A905F7EE8A02028E6A572499223889A55C2EF4646C0D3B2CB6DC64E1DCCEF26053EF80D34313EAD88
Malicious:	false
Preview:	..;. .*.*. .C.O.P.Y.R.I.G.H.T. .(.C.). .2.0.0.7.-.2.0.1.3. .R.e.a.l.t.e.k. .C.O.R.P.O.R.A.T.I.O.N.....;.....;. .R.e.a.l.t.e.k. .P.C.I.e. .F.E. .F.a.m.i.l.y. .C.o.n.t.r.o.l.l.e.r.....;. .R.e.a.l.t.e.k. .P.C.I. .G.B.E. .F.a.m.i.l.y. .C.o.n.t.r.o.l.l.e.r.....;. .R.e.a.l.t.e.k. .P.C.I.e. .G.B.E. .F.a.m.i.l.y. .C.o.n.t.r.o.l.l.e.r.....;.....[.v.e.r.s.i.o.n.].....S.i.g.n.a.t.u.r.e. . . .=. .".$.W.i.n.d.o.w.s. .N.T.$."".....C.l.a.s.s. . . . . .=. .N.e.t.....C.l.a.s.s.G.U.I.D. . . .=. .{.4.d.3.6.e.9.7.2.-.e.3.2.5.-.1.1.c.e.-.b.f.c.1.-.0.8.0.0.2.b.e.1.0.3.1.8.}.....P.r.o.v.i.d.e.r. . . . .=. .%.R.e.a.l.t.e.k.%.....D.r.i.v.e.r.V.e.r. . . .=. .0.4./.1.0./.2.0.1.3.,.7...0.7.2...0.4.1.0...2.0.1.3.....C.a.t.a.l.o.g.F.i.l.e...N.T. .=. .r.t.6.4.w.i.n.7...c.a.t.....[.M.a.n.u.f.a.c.t.u.r.e.r.].....%.R.e.a.l.t.e.k.%.=.R.e.a.l.t.e.k.,. .N.T.a.m.d.6.4.....[.C.o.n.t.r.o.l.F.l.a.g.s.].....E.x.c.l.u.d.e.F.r.o.m.S.e.l.e.c.t. . . . . .=. .*.....[.R.e.a.l.t.e.k...N.T.a.m.d.6.4.].....;. .8.

C:\Users\user\AppData\Local\Temp\user-not-tracked-symbolic.svg

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	4730
Entropy (8bit):	4.970880293743837
Encrypted:	false
SSDEEP:	96:VkoIankPYfLoIJomlXTlUxSHtuubQLqJlm0mxmOmTGmVm/mYmY:VkfcMI64RflubQW/BEjPoKlp
MD5:	8F7C767AFA41E6D03BDE59296DFF8175
SHA1:	EEFA541D3A06CAFEB62A535B86D1A95D6AAE1CD6
SHA-256:	292770B23ED69AF4EDE9255BB66ADF3D3A0FF62D827D2BA05ED2C44A57228ED6
SHA-512:	FFE75CCD2EFFA74E24955BF36DBD86BB1B30F880D233D8F5C5431E99169224E89E7C59FDD052C6F9544E05CF11FD425F01ADD6E87B512C318132D963CB338B4
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="no"?>.<svg. xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:cc="http://creativecommons.org/ns#". xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#". xmlns:svg="http://www.w3.org/2000/svg". xmlns="http://www.w3.org/2000/svg". width="16". version="1.1". style="enable-background:new". id="svg7384". height="16.000645">. <metadata. id="metadata90">. <rdf:RDF>. <cc:Work. rdf:about="">. <dc:format>image/svg+xml</dc:format>. <dc:type. rdf:resource="http://purl.org/dc/dcmitype/StillImage" />. <dc:title>Gnome Symbolic Icons</dc:title>. <cc:license. rdf:resource="http://creativecommons.org/licenses/by-sa/4.0/" />. </cc:Work>. <cc:License. rdf:about="http://creativecommons.org/licenses/by-sa/4.0/">. <cc:permits. rdf:resource="http://creativecommons.org/ns#Reproduction" />. <cc:permits. rdf:resource="htt

C:\Users\user\AppData\Local\Temp\video-joined-displays-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	208
Entropy (8bit):	6.572781220141588
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllUxPFp/7l04sR5/7dY+MK6Ie+ed0oxIwsoazRC4I:6v/lhPysIzlZsfdY+MKda8RC4KymCeVp
MD5:	E2FC23D36F5488D1F2888D524F933582
SHA1:	335CA8F69FF42E4418F0C95A9626F7B027F62139
SHA-256:	07AEFFEAC02CD1501C54E5D66ED1816B83AF04E51B1676AF3C4A538FDC9E9E4A
SHA-512:	EA3B15A24F8B3FF83DE6ABB7392A0672A55F1F87DDC485B2AD517E76B48358C852484CF2D23FD7989992676AF73640D6CC2002FD2F0FD2EAA29C39C7DFE503A
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8..1.. .E..@v....P.....8.O.....w4@.8`..I.I....0...&y..../9..r....5..@....P.+..l..*..8..~...@....p...y.#0)....o...fq....>....S.^&.n....IEND.B`.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.793691216814324
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Trojan.Inject.11626.exe
File size:	658225
MD5:	dd43bd8cdc55dd9c8a168f7d5e67db30
SHA1:	b7b49d8b277b6cb3d3006e912ad78558872119fb

SHA256:	7dc00d4ca525d39db7c57bcbcf2a17720f3e1d2eaecfc714f5e28f0e2a09633b
SHA512:	445e59a9fd2b4a0361772e6865866aee8511e583c0771b16c8e48d32940eecafa2baa05645fd5b5e4b0f75d78f57e6548304b04be241cc25dead38c4a77583ae
SSDEEP:	12288:0YgT387AbTc/v4b0h2gdYBXnQLGT/Fp0hZAvcG0ePzNSd01RHqtZCCNfn6THbMcR:0Ygo7AbTc/v4b0h2gqBXnQLGT/Fp0hZO
TLSH:	66E418B2A130868AD5E91EF25E5AB93091B22C7CDCE2110DA9F6370DD6F231145DEB4F
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:	ac9eb23233b28eaa

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 00007FA270AF948Ah

Instruction
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 00007FA270AF945Ah
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	0x52000	0x63d38	.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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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	0x27000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x52000	0x63d38	0x63e00	False	0.295598990926	data	5.64645184571	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x523d0	0x368	data	English	United States
RT_ICON	0x52738	0x4180c	data	English	United States
RT_ICON	0x93f48	0x10828	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xa4770	0x94a8	data	English	United States
RT_ICON	0xadc18	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0xb1e40	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 95	English	United States
RT_ICON	0xb43e8	0x988	data	English	United States
RT_ICON	0xb4d70	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0xb51d8	0xb8	data	English	United States
RT_DIALOG	0xb5290	0x144	data	English	United States
RT_DIALOG	0xb53d8	0x13c	data	English	United States
RT_DIALOG	0xb5518	0x100	data	English	United States
RT_DIALOG	0xb5618	0x11c	data	English	United States
RT_DIALOG	0xb5738	0x60	data	English	United States
RT_GROUP_ICON	0xb5798	0x68	data	English	United States
RT_VERSION	0xb5800	0x1f4	data	English	United States
RT_MANIFEST	0xb59f8	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
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
ProductName	Wadiesant
FileDescription	Unpackagedfotomo
FileVersion	19.29.0
Comments	CHONDROITI
CompanyName	Conteketra
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.Trojan.Inject.11626.exe PID: 6384, Parent PID: 2488

General

Target ID:	0
Start time:	19:30:31
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe"
Imagebase:	0x400000
File size:	658225 bytes
MD5 hash:	DD43BD8CDC55DD9C8A168F7D5E67DB30
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: 00000000.00000002.790910785.0000000003291000.00000040.00001000.00020000.00000000.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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nseA0F6.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\nsuA155.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	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\nsaA34A.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	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\nsaA34A.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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsaA34A.tmp\System.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\Waxiness.Sym	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\GL-1.0.typelib	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\ThrottlePlugin.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\applications-other.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\folder-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\rt64win7.inf	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\user-not-tracked-symbolic.svg	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\video-joined-displays-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\nsaA34A.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	4	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nseA0F6.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsaA34A.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	4	406224	WriteFile
C:\Users\user\AppData\Local\Temp\nsaA34A.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	110837	25458	75 6e 6b 6e 6f 77 6e	unknown	success or wait	59	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Waxiness.Sym	0	16384	03 03		success or wait	9	406224	WriteFile
C:\Users\user\AppData\Local\Temp\GL-1.0.typelib	0	1245	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - Fil	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ThrottlePlugin.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 28 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 45 4b fd fd 2b 18 fd fd 2b 18 fd fd 2b 18 fd fd 18 fd fd 2b 18 fd fd 2a 19 fd fd 2b 18 fd fd 2e 19 fd fd 2b 18 fd fd 2f 19 fd fd 2b 18 fd fd 28 19 fd fd 2b 18 24 fd 2a 19 fd fd 2b 18 fd fd 2c 19 fd fd 2b 18 fd fd 2d 19 fd fd 2b 18 fd fd 2a 19 fd fd 2b 18 fd fd 2a 18 03 fd 2b 18 24 fd 2e 19 fd fd 2b 18 24 fd 2b 19 fd fd 2b 18 24 fd fd 18 fd fd 2b 18 fd fd fd 18 fd fd 2b	MZ@(!L!This program cannot be run in DOS mode.$EK++++*+.+/+(+$*+,+-+*+*+$.+$++$++	success or wait	24	406224	WriteFile
C:\Users\user\AppData\Local\Temp\applications-other.png	0	685	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 02 74 49 44 41 54 78 01 fd fd 03 fd 6b 69 1c 47 fd fd fd fd fd 70 6d 1b fd fd 2e fd f6 fd 3a fd 63 f6 6d fd 76 fd fd fd 8b 17 75 4e 72 fd fd fd 4f 0e fd 15 fd fd fd 22 1f 18 2e fd 5c fd 42 2e fd fd fd a0 10 fd 71 fd 4a fd 17 fd 97 fd 03 7c fd 5e 5e 5e fd fd 13 0a fd fd 67 0e 1b fd fd 36 fd fd 5e fd fd 4e 56 28 fd fd fd 07 2f 1f 77 41 49 69 fd 6e 1f 2c 2c 23 fd fd 0c fd 41 7e 6b a1 ac fd fd 35 fd 59 fd 4d 59 77 64 53 fd 06 17 fd fd fd fd fd fd 4f 2f fd 73 1c 39 1e 6b 1e 17 7c 76 dd 64 fd fd fd fd fd fd 3c 46 fd 46 10 10 fd 1d 1a 1a 7a 1d 39 20 43 44 6e fd 49 7a 65 53 fd 5e 03 77 fd 29 fd 56 fd 30 fd 3f fd	PNGIHDRatIDATxkiGpm. cmvuNrO".\ B.qJ|^^^g6^NV(/wAIin,,A ~k5YwdSO/s9k|vd<FFz9 CDnIzeS^w)V0?	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\folder-symbolic.symbolic.png	0	166	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 5d 49 44 41 54 38 fd 63 60 fd 02 38 fd fd fd fd 1f 0b 3e fd fd fd 20 46 fd 01 fd 34 fd fd 75 06 06 06 49 4a 0c fd fd fd fd 34 33 42 05 fd 01 fd fd 2e fd 21 d4 fd 58 fd 44 03 26 72 6c 1d 35 fd 06 06 3c fd fd fd 49 50 4f 18 18 18 18 20 0c 52 fd fd 33 06 06 06 57 fd fd 0e 05 00 fd 6f 32 fd fd fd 4d 60 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|d]IDAT8 c`8> F4uIJ 43B.!XD&rl5<IPOR3Wo2 M`IENDB`	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rt64win7.inf	0	16384	fd fd 3b 00 20 00 2a 00 2a 00 20 00 43 00 4f 00 50 00 59 00 52 00 49 00 47 00 48 00 54 00 20 00 28 00 43 00 29 00 20 00 32 00 30 00 30 00 37 00 2d 00 32 00 30 00 31 00 33 00 20 00 52 00 65 00 61 00 6c 00 74 00 65 00 6b 00 20 00 43 00 4f 00 52 00 50 00 4f 00 52 00 41 00 54 00 49 00 4f 00 4e 00 0d 00 0a 00 3b 00 0d 00 0a 00 3b 00 20 00 52 00 65 00 61 00 6c 00 74 00 65 00 6b 00 20 00 50 00 43 00 49 00 65 00 20 00 46 00 45 00 20 00 46 00 61 00 6d 00 69 00 6c 00 79 00 20 00 43 00 6f 00 6e 00 74 00 72 00 6f 00 6c 00 6c 00 65 00 72 00 0d 00 0a 00 3b 00 20 00 52 00 65 00 61 00 6c 00 74 00 65 00 6b 00 20 00 50 00 43 00 49 00 20 00 47 00 42 00 45 00 20 00 46 00 61 00 6d 00 69 00 6c 00 79 00 20 00 43 00 6f 00 6e 00 74 00 72 00 6f 00 6c 00 6c 00 65 00 72 00 0d 00 0a	; ** COPYRIGHT (C) 2007-2013 Realtek CORPORATION;; Realtek PCIe FE Family Controller; Realtek PCI GBE Family Controller	success or wait	79	406224	WriteFile
C:\Users\user\AppData\Local\Temp\user-not-tracked-symbolic.svg	0	4730	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 6e 6f 22 3f 3e 0a 3c 73 76 67 0a 20 20 20 78 6d 6c 6e 73 3a 64 63 3d 22 68 74 74 70 3a 2f 2f 70 75 72 6c 2e 6f 72 67 2f 64 63 2f 65 6c 65 6d 65 6e 74 73 2f 31 2e 31 2f 22 0a 20 20 20 78 6d 6c 6e 73 3a 63 63 3d 22 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 6e 73 23 22 0a 20 20 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 0a 20 20 20 78 6d 6c 6e 73 3a 73 76 67 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 0a 20 20	<?xml version="1.0" encoding="UTF-8" standalone="no"?><svg xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:cc="http://creativecommons.org/ns#" xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#" xmlns:svg="http://www.w3.org/2000/svg"	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\video-joined-displays-symbolic.symbolic.png	0	208	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 51 31 0e fd 20 0c 45 fd fd 40 76 fd fd 01 1c 50 17 fd fd fd fd 18 1d fd fd 10 0b 38 fd 4f fd fd fd fd 7f fd fd 77 34 40 0f 38 60 fd fd 49 fd 49 09 0c fd fd 30 fd fd fd 26 79 15 08 1b fd 2f 39 2e fd 72 fd fd fd fd 35 fd fd 40 fd 0d 14 fd 50 fd 2b 15 fd 6c fd fd 2a fd 09 38 fd fd 7e fd fd fd 40 fd 13 fd fd 70 fd fd fd 79 fd 23 30 29 fd 05 fd fd 6f fd fd 05 66 71 fd fd fd fd 3e fd 01 fd fd 53 fd 5e 26 fd 6e 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dIDAT81E@vP8Ow4@8`II0&y/9.r5@P+l*8~@py#0)ofq>S^&nIENDB`	success or wait	1	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe	unknown	512	success or wait	875	4061F5	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe	unknown	16384	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsuA155.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsuA155.tmp	unknown	15448	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nsuA155.tmp	unknown	4	success or wait	9	4061F5	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Inject.11626.exe	unknown	16384	success or wait	13	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsuA155.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\Waxiness.Sym	unknown	1048576	success or wait	1	734E2C59	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\medtag	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\medtag\Erethitic	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Bastille56	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Bastille56\Skrivebordsskuffe50	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\reclothing	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\reclothing\Taxifly	success or wait	1	406532	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\medtag\Erethitic	enregistration	unicode	Jordbrugets124	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Bastille56\Skrivebordsskuffe50	Expand String Value	expand unicode	%WINDIR%\PITHECIA.log	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\reclothing\Taxifly	NDRAAB	binary	1F CD 6E	success or wait	1	40251B	RegSetValueExW

Disassembly

No disassembly