ID: 634994
Sample Name:
SecuriteInfo.com.W32.AIDetect.malware2.5627.14109
Cookbook: default.jbs
Time: 09:41:13
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

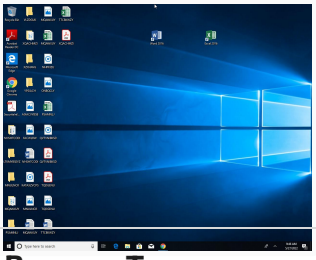
Windows Analysis Report

SecuriteInfo.com.W32.AIDetect.malware2.5627.14109

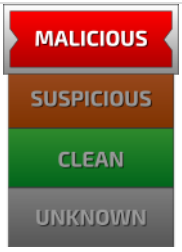
Overview

General Information

Sample Name:	SecuriteInfo.com.W32.AIDetect.malware2.5627.14109 (renamed file extension from 14109 to exe)
Analysis ID:	634994
MD5:	7f369d460c8414..
SHA1:	29ea3441429d55.
SHA256:	a5e095edbdf743..
Tags:	exe
Infos:	



Detection



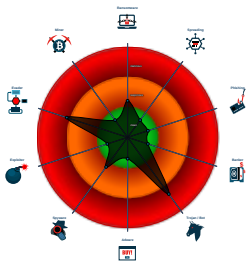
GuLoader

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Icon mismatch, binary includes an i…
- 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 an invalid checksum
- PE file contains strange resources
- Drops PE files

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.W32.AIDetect.malware2.5627.exe (PID: 6548 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.exe" MD5: 7F369D460C84146944C3C12BF83901AF)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://hustlecreate.com/a1/binned_SsGEV34.bin"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.898389983.0000000002BB7000.00000040.00000800.00020000.00000000.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

Hooking and other Techniques for Hiding and Protection

Icon mismatch, binary includes an icon from a different legit application in order to fool users

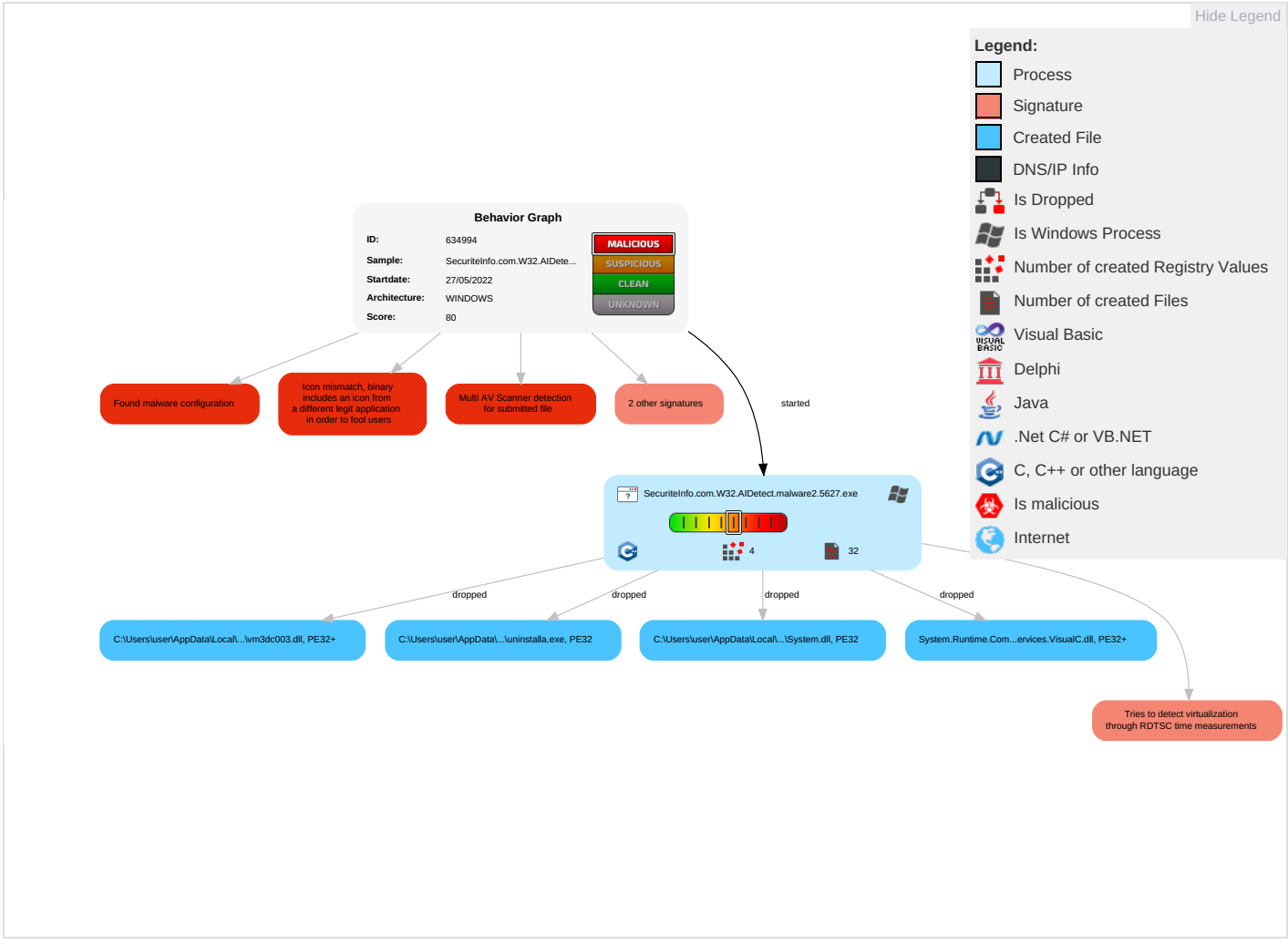
Malware Analysis System Evasion

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 Masquerading	OS Credential Dumping	1 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 Access Token Manipulation	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)	1 Obfuscated Files or Information	Security Account Manager	1 3 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Timestomp	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

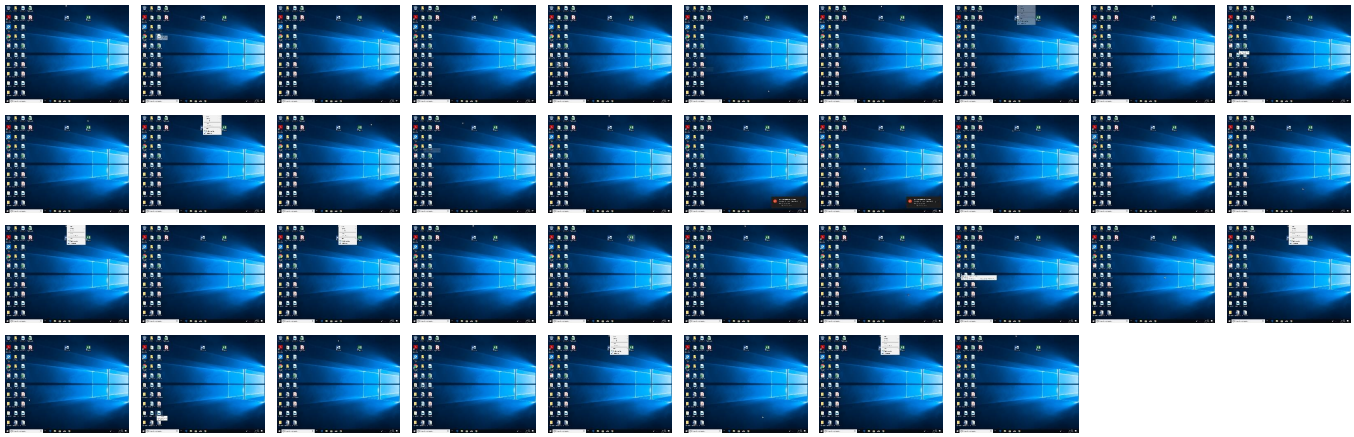
Behavior Graph



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.W32.AIDetect.malware2.5627.exe	19%	Virustotal		Browse
SecuriteInfo.com.W32.AIDetect.malware2.5627.exe	12%	ReversingLabs	Win32.Trojan.Shelsy	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\System.Runtime.CompilerServices.VisualC.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\System.Runtime.CompilerServices.VisualC.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nse4A46.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nse4A46.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\uninstalla.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\uninstalla.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\vm3dc003.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://hustlecreate.com/a1/binned_SsGEV34.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://hustlecreate.com/a1/binned_SsGEV34.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.vmware.com/0/	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe, 00000001.00000002.897861144.000000000040A000.00000004.00000001.01000000.00000005.sdmp, vm3dc003.dll.1.dr	false		high
http://https://github.com/dotnet/runtimeBSJB	System.Runtime.CompilerServices.VisualC.dll.1.dr	false		high
http://www.vmware.com/0	vm3dc003.dll.1.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe, uninstalla.exe.1.dr	false		high
http://www.symauth.com/cps0(	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe, 00000001.00000002.897861144.000000000040A000.00000004.00000001.01000000.00000005.sdmp, vm3dc003.dll.1.dr	false		high
http://www.symauth.com/rpa00	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe, 00000001.00000002.897861144.000000000040A000.00000004.00000001.01000000.00000005.sdmp, vm3dc003.dll.1.dr	false		high
http://https://github.com/dotnet/runtime	System.Runtime.CompilerServices.VisualC.dll.1.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	634994
Start date and time: 27/05/202209:41:13	2022-05-27 09:41:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.W32.AIDetect.malware2.5627.14109 (renamed file extension from 14109 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:	mal80.troj.evad.winEXE@1/11@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 63.2% (good quality ratio 61.9%) • Quality average: 88.2% • 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, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 40.125.122.176, 52.242.101.226, 20.223.24.244, 20.54.89.106, 52.152.110.14
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
09:42:33	API Interceptor	1x Sleep call for process: SecuriteInfo.com.W32.AIDetect.malware2.5627.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\CELSIAN.Gra

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.exe
File Type:	data
Category:	dropped
Size (bytes):	402254
Entropy (8bit):	7.791539989948347
Encrypted:	false
SSDEEP:	12288:TmJZJW5QhS/VQ40QP6BE4xUARC9LsfQu2aNFtcb:ThQSVQ4SxUARC9LsfQu2aNFtw
MD5:	F042FA6C1A5A11E1E94F4C7D55F4696F
SHA1:	3A9C3519A67FD03DC3C97EEA6B04CFFD1AA38715
SHA-256:	B30D6EBFBD48675A3899E47EA4FEFD63A784CF4D291CE1CE7E805B70BB71D67D
SHA-512:	775821F4D105DED3FD6294F16640745180A40D2327EA965B325D528E31C3F8C3A1DF7CB8A28AFDA43D383264220E89EF5FAE1CD447FA44478F2C90D8DD37A98
Malicious:	false
Reputation:	low
Preview:	.>,...BgMkU..).B...H#....Y...M.6..p..6.$.4...X.*.....".3..!Q...S..wE[.(P.DhK_.....i.....[.wp>.t....U.P.Ns.Sz{2:.O.b.c.oxK=M].../P.Eqm.z....j\%.z..9.'6;?....`:HB.Od...?.I.Y.8..... n8..0...S.....#.....T.B$....._..@N.0.g.:k:...J%R.3'...Lpg..o..:f.....,x...s.8.*....q..U..)8.v.....,.en..F:....e...[.....:].:/|:..K}y...1..}..j....)W..]...!..._?d.....L.i>..i.....gk...Y....A,.....".p.m| ..#Ap..y.n.%.r.z..-|..Vh$...T.4Z..o...M.|gH@Jt!.M.....'.J.0.....iL..]Og.....&H../S.....".!{.x...".v8.4.5.|.../.!...._;9.1.gp.i3..l....Z..>'..7.5R.._.VH=C.:-...]..y.+.:Rb;.._{C.>...4M.DT ..../.Yx.!.u.#Y"..-..h..._..8...8..a.s....*I.Y..|..8.55.M..p.M..B...D.3f.!.. ...n.A...B...N.2..H.....mKn_.a.u.9....qD...Z...+....^..[..a...L....(."..S{F\....q.l..R.*.m..@RvP.w.....IHR...z.:.w..... ....)..S..@..;.C.f...I..=.....R7..D....?k..AF3.1s..n..h..../,8}...^...>..4H.-o..8..Q7...B.*.@M7.<q....<...'.h.B?... .)... .P.....%>B....D#.S,....o..:.).:kN0...^A

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	32
Entropy (8bit):	4.663909765557392
Encrypted:	false
SSDEEP:	3:Ve4KXOHXRWLkmt:LKesLkQ
MD5:	272BC34712948F6A7132DD80E17DE84E
SHA1:	461967EA55D874C28BF0999FB66CACE785D9BCA9
SHA-256:	019D3E92BF00DC7409E188A19F11AB33C31BFBAFE5B2E036632CC69B71207FE9
SHA-512:	56BE026C1DCA3326CFC165244E9F0AA6278E779D003BBD9405E4A18408B00B3AB3CBC5B779D4A315EEA43278C306AC307121BB007112A70BEC2B6CDFEE06C9 58
Malicious:	false
Reputation:	low
Preview:	[GORKUN]..Workbags141=REFRACTS..

C:\Users\user\AppData\Local\Temp\Green_Leaves_21.bmp

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.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):	10115
Entropy (8bit):	7.896422756961018
Encrypted:	false
SSDEEP:	192:oXRIG87sv/m1vnKaVSuKRXL55hOuf4dXL9J0LEvJyVVcuJ6Sj7YvKvtOJ:KRIjsW1vKPXBgdiWMEMj7YyvG
MD5:	2F12A714A50993C090C94EC2672490E1
SHA1:	4F9A319C412F1B1B251C027B1C2448BBDBB9CA6F
SHA-256:	E759639DCCA8E96864BC82EDBACFD5BB14FE37412A6F3FCE7C82BF1BB944B6E4
SHA-512:	2B349EAB24DCCE0DBD36433DE13E0B2A551E88A626D5C9A3F68B79E21ACDE4FC238DD4E280E30ACBB76B0EB0E08CE1ACC233AB1C9E2147E2DD01E0917B3 A376B
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d.....:Exif..MM.*.....Q.....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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....(..0..?l...9.l...7.....S.h..5.....!9...[..$M...E'..y.l@Xxg.i.....?..7..3M.....E...L..Z.$....B.b.@...y.y'..}._.\|c.....5....G..5-{l.-....+._Q....7.....D.\|....M.Hb..x....._ P./o...RJ0{Zr..q+.....1.....X.....G.....\|1}...}.a.}/J..Gk.[...j.....+.. .n"..X.Q..9..$....o.....8...o.|K....}

C:\Users\user\AppData\Local\Temp\System.Runtime.CompilerServices.VisualC.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	19056
Entropy (8bit):	6.442411564417779
Encrypted:	false
SSDEEP:	384:8WhLWql40uIrRDTveaVEc2gK/uPHRN7xpJ/AlGseCvy:rfl40uqDTveaVCMxv/xj4y
MD5:	E3F74999CDB00FCAAA6A40A97B8F199B
SHA1:	F3A2C8DF8E98F7DCB49CBE5C4A717A6087A656D2
SHA-256:	6929BC473DF404FCED714F345479216B66B72ACF116061DF1CDD8ACAEE961333
SHA-512:	3BE3EEAB3304EFEB9594FA516B61528587CFA8453AB7B4AF991137E3A1D7E23270DA600FC341EEF703932CCFF53571ACF3CD00AEEAE47347CC36EE69B71DB37C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...(_+......" ....P..... ..`...@.....@..... .....&..p$...@.....T.....H.....text...X..... ..... ..`.data...D....0....."..... .....@....reloc.....@.....$.....@..B.....0.....4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....y.....?.....D.....V.a.r.F. i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...h.(...C.o.m.m.e.n.t.s...S.y.s.t.e.m...R.u.n.t.i.m.e...C.o.m.p.i.l.e.r.S.e.r.v.i.c.e.s. ..V.i.s.u.a.l.C...L.....C.o.m.p.a.n.y.N.a.m.e.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...x.(...F.i.l.e.D.

C:\Users\user\AppData\Local\Temp\drive-harddisk-system-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	264
Entropy (8bit):	6.7753015109610715
Encrypted:	false
SSDEEP:	6:6v/lhPysLQNJ4BgpBly/Gj6e3ba4Dzz8fKtVp:6v/7rQb4BAlyU6mDzzoK9
MD5:	39182B562FCB2BAD93D58516462708A8
SHA1:	F9A88E1F1313BD05CDB1E962DE8170CCCFDA9151
SHA-256:	DEF4215BBA93FAED6FCF7E4687EF89AB828DB10E69171A5E14908F091302C59F
SHA-512:	ECEC5D0E389293DB2977C7A7DCE8E4FAC10A3ADA7466DBA9CE4FE9712F5725D84E67A5E0ED9BE5091D68BD817186D6CFC89CA650CC5323FB8C038A14BAD3896D
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...1n.1...(.. l...h.1B.E...#\.$h....l.v...F...7.;\.b...B..w"aWq..?.@...L?qr#.F.,p...'.w.....CxV.X.....b.j...S....8v...e...l..|.\4X..f.G....+.-6....3.....{..".D...rz..-.6...nW.:o1._YVz]."N.....IEND.B`.

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	243
Entropy (8bit):	6.6375398452197
Encrypted:	false
SSDEEP:	6:6v/lhPysEFaTw0eY/5b5sap5kGC125kiUP2afunr2W7Vtljp:6v/7kgoY/7shGC1DHP24u6KtlN
MD5:	433D25AD6818DB00083CD062A16D3479
SHA1:	D4210D893E965912EA7BD45C80D359FECAB54A98
SHA-256:	3D06E8FA89BA4FA9D9BCC260F38C72D1A104FE3E6F8923A3EE553563832027CB
SHA-512:	E5095FE100F811D73196F01C732AA09E2359E5796DF38A0B3E25599F3F99CCD2ED181070463285655521199B7B084A7848E6629CB5CE0AE07FCBC17D5953FA4C
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8..M..0...vQ...BP.vZ./ .+..SD."..c.F.....f^^`....;....9...l..17...0..ML..1.M2....X..90.v..... ....Q...@.m...G.K.-`..\%D.`..B..j\.....\.....\.{....g.....7..i....\....IEND.B`.

C:\Users\user\AppData\Local\Temp\nse4A46.tmp\System.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.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: 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\scanner.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	633
Entropy (8bit):	7.5766983812463735
Encrypted:	false
SSDEEP:	12:6v/7x8QVQCJI+uIidxp+pY5f5Cqxnnu13gYdndacj/Ya+SvGpaNusvrdVJ:PxOI5I0P+2Zu13gIdR/Yla8svrfJ
MD5:	0CBA7EB7455B0DB79456C5911F12B75E
SHA1:	DAACA4FE36E4F61016D473A0A1CD4C980906872B
SHA-256:	50F4DB972320FF30D4FD98B61F58D956678F38FD1D11CA5109E5559D02A986BE
SHA-512:	D6976DC90DD3B01A7AAFDF67C5360CC75020971473F8689CA73A9931FB36FF4CC6994034664E11B4FF31146767F5B9DB898104BE814A1611C8A02260C66E11D8
Malicious:	false
Preview:	.PNG.....IHDR.....a...@IDATx.....&K..kfz..g..g...;_..'..l.....^{..6._...._/g9.B...r...$..._~..4.7@.4h..UU!.2.$A.E...Q.",2..q.[.nc.....-.....4:..C..B .c$.N....s.....0.l#..UkP IRO.e...g.D...&<jnQ..k.....k..T*.....LS,,D..Q.8.0..<...?(//...A.CCm]....e|..<...#.w..:.\{{....PP__.. .i....?..i..L...8t.(.?.....>..G.W..-.~.A9\m..z.E....L....:.l.... .4....;a...^.P.>.....s.8 6.Hq..c!.e...e..7CA).c....w.%..iZ...|.j3(..$.2.?..w.....O?.M..E..!....=\.a..o....m.+V,.Q...pA..l(.s..S.,..!.R.`t....r(.7..H....."....+.}...A..xM....L..L..cG....L$`.;K.m...h..O.r..3. cb#....IEND.B`.

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	265238
Entropy (8bit):	6.697651009316531
Encrypted:	false
SSDEEP:	6144:FR+xXYSlvF68OZGbpYByPT7lyvIco9KX25G5PGDu6WL1g:DMIvk8OvByPHly5425GDum
MD5:	1DCEAF980C4D83AE2A13BD0F047E1BD7
SHA1:	7D97E79EFB047361A8C2A8AC0A26B37127C3C7AC
SHA-256:	0C340FB13ACAAAE759215AF9C970DC6C167418534C421EB626643E20FD0AC832
SHA-512:	8FDBBBCAAC2B3188819E7F8E3ADE82E01723F27C151EDD50F4AE090339C680CE685540BCA76018BC5494CEBF5001A5FCF97C07D7FC47479BF11CEB38A3CE9 FE4
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L...$..\.....f...*.....4.....@.....?...@.....P...a.....@.>..... .....text....d.....f..... ..`.rdata.....j.....@..@.data...X.....~.....@....ndata.....rsrc....a...P...b.....@..@.....

C:\Users\user\AppData\Local\Temp\vm3dc003.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped

Size (bytes):	190624
Entropy (8bit):	6.481480370859183
Encrypted:	false
SSDEEP:	3072:o/qsfTS04VccXuMeXEVmd/AuRV9DKRSeilOA1Fafxc7Kwhbzi+iOh:oysrSDcHbNd7+xmVbP
MD5:	059BE7432DFAD92F4EA0A2E5941C52A7
SHA1:	1C1B989D6B9D0FA0808FCA8893ADDC8CD76602D9
SHA-256:	8E184A514D8716B59B24892CB425752E6D7837735C1E9F1996D66E70BFEC033B
SHA-512:	EA79397D73840AEA9E9C3AC55F2E4FFA9A10828C2BFD993AB116CC08412E690C3DE10617AC516B944DEA48D7BFCEC201404C9CF0E54A5594A247F5F202F59F7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....Qvw.Qvw.Qvw.Qvw.Pvw.E.s.Zvw.E.t.Tvw.E.r..vw.=.t.Xvw.=.s.^vw.=.r.Lvw..-r.Pvw...r.Rvw...t.Pvw.4.v.\w.Qvv..vw...s.Vvw...w.Pvw.....Pvw...u.Pvw.RichQvw.....PE..d.....`....." .....~.....1.....].....`A.....G..p....G..x.....x....z...n.....|....-..8.....,..8.....F..@.....text....}.....~..... ..`.rdata.....@..@.data.....`.....F.....@....pdata..x.....R.....@..@.didat..H.....h.....@....gehcont.....j.....@..@_RDATA.....l.....@..@.rsrc.....n.....@..@.reloc..|.....r.....@..B.....

C:\Users\user\AppData\Local\Temp\vtshim.c

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.exe
File Type:	C source, ASCII text
Category:	dropped
Size (bytes):	15782
Entropy (8bit):	5.207431068394915
Encrypted:	false
SSDEEP:	192:zu0gnPI2Z1Fylkd3cd/e5QJvWUnumPw2QJt+UnumPwhJhbjSjSHXMXzhFwqOzj5w:zYIOyaKl+uybeiHtHai
MD5:	1B00C31FF20D27F07B299063908311E0
SHA1:	1976E6DD68DD0D64508C91A6DFAB8E75F8AAF6CD
SHA-256:	EC872BB1DDC330D3F19F68D033B0706E1B78D4A91A58998674B67EAD58BEA729
SHA-512:	38B29DB2CDA85380F63C86EAAA5D7DE6657EA4C6A0B074D184F6F3218467C865B3D0B56C2844547897139F5C324792C0D3CB5AE1FB4B593AB6F8889A7C88BB30
Malicious:	false
Preview:	/*.** 2013-06-12.**.** The author disclaims copyright to this source code. In place of.** a legal notice, here is a blessing:.**.** May you do good and not evil..** May you find forgiveness for yourself and forgive others..** May you share freely, never taking more than you give..**.********** **********.**.** A shim that sits between the SQLite virtual table interface and.** runtimes with garbage collector based memory management..*/.#include "sqlite3ext.h".SQLITE_EXTENSION_INIT1.#include <assert.h>..#include <string.h>..#ifndef SQLITE_OMIT_VIRTUALTABLE../* Forward references */.typedef struct vtshim_aux vtshim_aux;.typedef struct vtshim_vtab vtshim_vtab;.typedef struct vtshim_cursor vtshim_cursor;.../* The vtshim_aux argument is the auxiliary parameter that is passed.** into sqlite3_create_module_v2()..*/.struct vtshim_aux {. void *pChildAux; /* pAux for child virtual tables */. void (*xChildDestroy)(void*);

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.518620994648534
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.W32.AIDetect.malware2.5627.exe
File size:	929272
MD5:	7f369d460c84146944c3c12bf83901af
SHA1:	29ea3441429d555ddfd0fd8d5973aab0f9ea2663
SHA256:	a5e095edbdf743431c5e866c01c3a592fc5a7ddf6bfb617d72f81181743adf3a
SHA512:	5183cb1c7173fcf8f5d30c9a5842a2e895d50d8a742e7097b7d8862d7e0e6be4a94e166bc4b7175717a18e93c194d1259cb30ed7b649b518f0d9736f66e9f3fc
SSDEEP:	12288:YbKP7r9r/+ppppppppppppppppppppppppppp0Y/e4hZJgtQ9STVQ40QPKBut6:YbK1M/e1Q4VQ4muENar+Wav5BK3c
TLSH:	7C15E0C0E94495A1ED1DAB716A36CD3546237DBDA874A81D25DE3E2B3FFB2D31026023
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...Z.Oa.....j.....

File Icon

Icon Hash:	c4c4c4c8ccd4d0c4

Static PE Info

General

Entrypoint:	0x40352d
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:	0x614F9B5A [Sat Sep 25 21:57:46 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:	56a78d55f3f7af51443e58e0ce2fb5f6

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], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
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 00007F800518DDFAh
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

Instruction
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F800518DDCAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [00434FB8h], 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	0x8610	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x58000	0x354c8	.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	0x6897	0x6a00	False	0.666126179245	data	6.45839821493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a6	0x1600	False	0.439275568182	data	5.02410928126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.521484375	data	4.15458210409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x36000	0x22000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x58000	0x354c8	0x35600	False	0.212867754684	data	4.44760586334	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x58538	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	0x68d60	0x94a8	data	English	United States
RT_ICON	0x72208	0x67e8	data	English	United States
RT_ICON	0x789f0	0x5488	data	English	United States
RT_ICON	0x7de78	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 254, next used block 2130706432	English	United States
RT_ICON	0x820a0	0x35e0	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x85680	0x25a8	data	English	United States
RT_ICON	0x87c28	0x10a8	data	English	United States
RT_ICON	0x88cd0	0xea8	data	English	United States
RT_ICON	0x89b78	0x988	data	English	United States
RT_ICON	0x8a500	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x8ada8	0x6c8	data	English	United States
RT_ICON	0x8b470	0x668	data	English	United States
RT_ICON	0x8bad8	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x8c040	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x8c4a8	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 4294965391, next used block 7403512	English	United States
RT_ICON	0x8c790	0x1e8	data	English	United States
RT_ICON	0x8c978	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x8caa0	0x100	data	English	United States
RT_DIALOG	0x8cba0	0x11c	data	English	United States
RT_DIALOG	0x8ccc0	0xc4	data	English	United States
RT_DIALOG	0x8cd88	0x60	data	English	United States
RT_GROUP_ICON	0x8cde8	0x102	data	English	United States
RT_VERSION	0x8cef0	0x298	data	English	United States
RT_MANIFEST	0x8d188	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, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, 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	SELVFORKL
FileVersion	14.32.29
CompanyName	xanthopicr
LegalTrademarks	UDSLUTTETGABSTE
Comments	Svolvdioxidemiss200
ProductName	frstedirektrenta
FileDescription	SKESSONGLANDSKUM
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.W32.AIDetect.malware2.5627.exe PID: 6548, Parent PID: 1448

General

Target ID:	1
Start time:	09:42:31
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.exe"
Imagebase:	0x400000
File size:	929272 bytes
MD5 hash:	7F369D460C84146944C3C12BF83901AF
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: 00000001.00000002.898389983.0000000002BB7000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nse22A8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsf2568.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405AF7	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405AF7	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405AF7	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	3	405AF7	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	3	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\BUFFWARE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\BUFFWARE\Forewinning14	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\BUFFWARE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\BUFFWARE\Forewinning14	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\CELSIAN.Gra	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\Green_Leaves_21.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\System.Runtime.CompilerServices.VisualC.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\drive-harddisk-system-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mail-unread-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\scanner.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\uninstalla.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\vm3dc003.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\vtshim.c	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nse4A46.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	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	405AF7	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	405AF7	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	405AF7	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	405AF7	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	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nse4A46.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	405AB7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nse4A46.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nse4A46.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	5	406059	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nse22A8.tmp	success or wait	1	403875	DeleteFileW
C:\Users\user\AppData\Local\Temp\nse4A46.tmp	success or wait	1	405C78	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CELSIAN.Gra	0	16379	fd 3e 2c 01 05 fd 42 67 4d 6b 55 56 fd 29 fd 42 fd fd fd 48 23 fd fd fd fd 59 fd fd fd 4d fd 36 fd fd 70 fd fd 36 fd 24 fd 34 fd fd dc 58 fd 2a fd fd 17 fd 1d fd 22 fd 33 fd fd 21 51 fd 11 fd 53 fd 2e 77 45 5b 1a 28 50 0f 44 68 4b 5f fd fd fd 0a fd 69 fd fd fd 01 88 fd 5b fd 77 70 3e fd 74 fd fd 02 fd 55 fd 50 fd 4e 73 fd 53 7a 7b 32 3a fd 4f 0f 62 fd 63 0f 6f 78 4b 3d 4d 5d 04 fd fd 2f 50 fd 45 71 6d fd 7a 06 56 fd 7f 6a 5c 25 fd 7a 10 0f 39 05 27 36 3b 3f fd fd fd fd 60 3a 48 42 fd 4f 64 fd fd fd 3f fd 6c fd 59 fd 38 fd fd 0a 1d fd 6e 38 fd fd 30 fd fd fd 53 fd 04 1c fd 03 23 fd fd 12 fd fd 54 17 42 24 fd fd fd fd fd 5f fd 10 40 4e 10 30 fd 67 fd 3a 6b 3a fd 0a fd 4a 25 52 1c 33 27 fd fd fd 4c 70 67 8c fd 6f 17 fd 3a	>,BgMkU)BH#YM6p6$4X *"3!QS.wE[(PDhK_i[wp>tUPNsSz{2: ObcoxK=M]/ PEqmzj\%z9'6;?`:HBOd? lY8n80S#T B$_@N0g:k:J%R3'Lpgo:	success or wait	23	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\Green_Leaves_21.bmp	0	10115	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 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*QQaQaC Cnn"	success or wait	1	4060F9	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\System.Runtime.CompilerServices.VisualC.dll</td><td>0</td><td>19056</td><td>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 03 00 28 5f 2b fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0b 00 00 20 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 50 00 00 00 02 00 00 fd 15 01 00 03 00 60 fd 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 20 00 00 00 00 00</td><td>MZ@!L!This program cannot be run in DOS mode.$PEd(_+" P`@@</td><td>success or wait</td><td>1</td><td>4060F9</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\drive-harddisk-system-symbolic.symbolic.png</td><td>0</td><td>264</td><td>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 31 6e 02 31 10 fd fd 28 fd fd 20 6c fd fd 06 68 fd 31 42 0a 45 04 fd fd 23 5c 03 24 68 fd 14 fd fd 6c 0c 76 fd fd fd 46 fd fd fd 37 fd 3b 5c fd 62 fd 16 fd 42 fd fd 77 22 61 57 71 fd 1b 3f fd 40 fd fd fd 4c 3f 71 72 23 fd 46 1a 2c 70 0a fd fd 27 fd 77 fd 06 fd fd fd 43 78 56 14 58 fd fd 1b 1f 18 62 15 6a fd 1a fd 53 07 fd fd 2e 38 76 fd fd fd 65 fd fd 15 49 1d fd 7c 15 5c 34 58 fd b2 66 fd 47 fd fd fd fd 2b 02 2d 36 fd fd fd fd 33 fd fd 0a fd 91 7b fd fd 22 0a 44 fd fd fd 72 7a 06 fd 2d fd 36 15 fd fd 6e 57 fd 3a 6f 31 fd 5f 59 56 7a 5d fd 22 4e fd 00 00 00</td><td>PNGIHDRasBIT|dIDAT81n1(lh1BE#\$hlvF7;\bBw"aWq?@L?qr#F,p'wCxVXbjS.8veI|\4XfG+-63{"Drz-6nW:o1_YVz]"N</td><td>success or wait</td><td>1</td><td>4060F9</td><td>WriteFile</td></tr>
</table>

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\mail-unread-symbolic.symbolic.png</td><td>0</td><td>243</td><td>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 52 4d 0a fd 30 14 fd fd 76 51 fd fd fd 42 50 fd 76 5a 05 2f 20 ab 2b fd fd 53 44 fd 22 fd 1a 63 fd 46 10 1c 18 fd fd 66 5e 5e 60 fd 1f fd 00 3b fd 02 fd 0f 39 02 fd fd 6c 0b fd 31 37 fd fd fd 30 fd fd 4d 4c fd fd 31 13 4d 32 1d fd fd 09 58 05 fd 39 30 fd 76 05 0e fd 89 fd 06 0b fd fd 20 0d fd 06 fd 51 fd fd fd 40 fd 6d fd fd 01 47 fd 4b fd 2d 60 fd fd 5c 25 44 fd 60 01 fd 42 fd 13 6a 5c fd 00 16 05 fd fd fd 11 5c fd fd 0d fd 1a 5c 1c 7b 1e 03 fd fd 67 fd fd fd fd fd 06 37 fd fd 69 fd 7f fd 0f 5c 00 00 00 00 49 45 4e 44 fd 42 60 fd</td><td>PNGIHDRasBIT|dIDAT8 M0vQBPvZ/ + SD"cFf^^`;9l170ML1M2X 90v Q@mGK-`\%D`Bj\\\ {g7i\IENDB`</td><td>success or wait</td><td>1</td><td>4060F9</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\scanner.png</td><td>0</td><td>633</td><td>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 40 49 44 41 54 78 01 fd fd 03 fd 26 4b 1c fd 6b 66 7a 35 fd 67 ca fd 67 c7 fd 18 3b 5f fd 1d 27 fd fd 6c f6 fd de fd fd 5e 7b fd fd 36 fd 5f 0d fd fd fd 5f 2f 67 39 fd 42 fd fd 72 fd fd fd 24 fd fd fd 5f 7e fd fd 34 fd 37 40 fd 34 68 fd 06 55 55 21 fd 32 fd 24 41 14 45 08 fd 10 51 18 22 2c 32 fd fd 71 fd 5b fd 6e 63 fd fd fd fd fd 1f fd 0b 16 2d fd 1b fd fd 06 fd 34 3a fd 19 43 fd fd 42 20 fd 63 24 fd 4e fd 14 fd 14 73 fd fd fd fd fd a1 fd fd 30 fd 6c 23 fd fd 55 6b 50 20 49 52 4f fd 65 fd 7f fd 67 fd 44 fd fd 86 26 3c 6a 6e 51 fd fd 6b fd fd fd fd fd fd 6b fd fd 54 2a fd ef fd fd 70 4c 53 2c 2c 44 18 fd</td><td>PNGIHDRa@IDATx&Kkf zgg;_'l^{6__ /g9Br$_~47@4hUU!2$AE Q",2q[nc-4:CB c$Ns0l#UkP IROegD& <jnQkkT*LS,,D</td><td>success or wait</td><td>1</td><td>4060F9</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\uninstalla.exe</td><td>0</td><td>24311</td><td>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 fd 31 08 fd fd 50 66 fd fd 50 66 fd fd 50 66 fd 2a 5f 39 fd fd 50 66 fd fd 50 67 fd 4c 50 66 fd 2a 5f 3b fd fd 50 66 bd 73 56 fd fd 50 66 fd 2e 56 60 fd fd 50 66 fd 52 69 63 68 fd 50 66 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 24 7f 15 5c 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 66 00 00 00 2a 02 00 00 08 00</td><td>MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPg LPf*_;PfsVPf.V`PfRichPf PEL$\f*</td><td>success or wait</td><td>13</td><td>4060F9</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vm3dc003.dll	0	29050	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 20 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 15 17 19 fd 51 76 77 fd 51 76 77 fd 51 76 77 fd 51 76 77 fd 50 76 77 fd 45 1d 73 fd 5a 76 77 fd 45 1d 74 fd 54 76 77 fd 45 1d 72 fd fd 76 77 fd 3d 02 74 fd 58 76 77 fd 3d 02 73 fd 5e 76 77 fd 3d 02 72 fd 4c 76 77 fd fd 2d 72 fd 50 76 77 fd 03 1e 72 fd 52 76 77 fd fd 1f 74 fd 50 76 77 fd 34 10 76 fd 5c 76 77 fd 51 76 76 fd fd 76 77 fd fd 1f 73 fd 56 76 77 fd fd 1f 77 fd 50 76 77	MZ@ !L!This program cannot be run in DOS mode.$QvwQvwQvwQvwP vwEsZvwEtTvwErvw=tXvw=s^vw=rLvw-rPvwrRvwtPvw4v\vwQvvvwsVvwwPvw	success or wait	8	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\vtshim.c	0	15782	2f 2a 0a 2a 2a 20 32 30 31 33 2d 30 36 2d 31 32 0a 2a 2a 0a 2a 2a 20 54 68 65 20 61 75 74 68 6f 72 20 64 69 73 63 6c 61 69 6d 73 20 63 6f 70 79 72 69 67 68 74 20 74 6f 20 74 68 69 73 20 73 6f 75 72 63 65 20 63 6f 64 65 2e 20 20 49 6e 20 70 6c 61 63 65 20 6f 66 0a 2a 2a 20 61 20 6c 65 67 61 6c 20 6e 6f 74 69 63 65 2c 20 68 65 72 65 20 69 73 20 61 20 62 6c 65 73 73 69 6e 67 3a 0a 2a 2a 0a 2a 2a 20 20 20 20 4d 61 79 20 79 6f 75 20 64 6f 20 67 6f 6f 64 20 61 6e 64 20 6e 6f 74 20 65 76 69 6c 2e 0a 2a 2a 20 20 20 20 4d 61 79 20 79 6f 75 20 66 69 6e 64 20 66 6f 72 67 69 76 65 6e 65 73 73 20 66 6f 72 20 79 6f 75 72 73 65 6c 66 20 61 6e 64 20 66 6f 72 67 69 76 65 20 6f 74 68 65 72 73 2e 0a 2a 2a 20 20 20 20 4d 61 79 20 79 6f 75 20 73 68 61 72 65 20 66 72 65 65 6c	/*** 2013-06-12**** The author disclaims copyright to this source code. In place of** a legal notice, here is a blessing:**** May you do good and not evil.** May you find forgiveness for yourself and forgive others.** May you share freel	success or wait	1	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nse4A46.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	4060F9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.exe	unknown	512	success or wait	519	4060CA	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.exe	unknown	4	success or wait	2	4060CA	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.exe	unknown	4	success or wait	4	4060CA	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.exe	unknown	4	success or wait	58	4060CA	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\chirpier	success or wait	1	406407	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\chirpier\Malone	success or wait	1	406407	RegCreateKeyExW
HKEY_CURRENT_USER\Software\UNDERGRENS	success or wait	1	406407	RegCreateKeyExW
HKEY_CURRENT_USER\Software\UNDERGRENS\CRYSTALLING	success or wait	1	406407	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Hardheartedly12	success or wait	1	406407	RegCreateKeyExW
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Tnker81	success or wait	1	406407	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\chirpier\Malone	Expand String Value	expand unicode	%WINDIR%\Gymnonoti.log	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\UNDERGRENS\CRYSTALLING	BARNEFADERS	binary	FF 9B 29 B0	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Hardheartedly12	DANNY	dword	0	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Tnker81	Gorbag	dword	1	success or wait	1	40251B	RegSetValueExW

Disassembly

No disassembly