ID: 755965
Sample Name: SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe
Cookbook: default.jbs
Time: 11:43:57
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

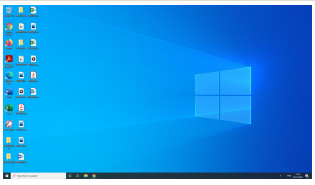
Windows Analysis Report

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

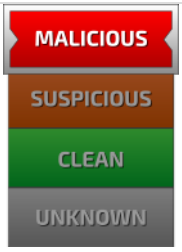
Overview

General Information

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



Detection



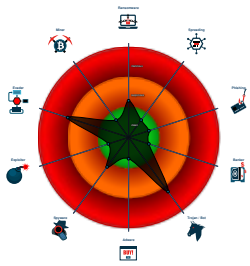
GuLoader

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect Any.run
- Uses 32bit PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Detected potential crypto function
- Found potential string decryption / a…
- Stores files to the Windows start me…
- Contains functionality to call native …
- Contains functionality to dynamicall…

Classification



Process Tree

- **System is w10x64native**
- SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe (PID: 6064 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe MD5: 7081C4822CF1C7572DD82822B8F27C49)
  - SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe (PID: 6832 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe MD5: 7081C4822CF1C7572DD82822B8F27C49)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.39673477269.0000000003320000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000005.00000000.39479578905.0000000001660000.00000040.00000400.00020000.00000000.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

Multi AV Scanner detection for submitted file

Data Obfuscation

Yara detected GuLoader

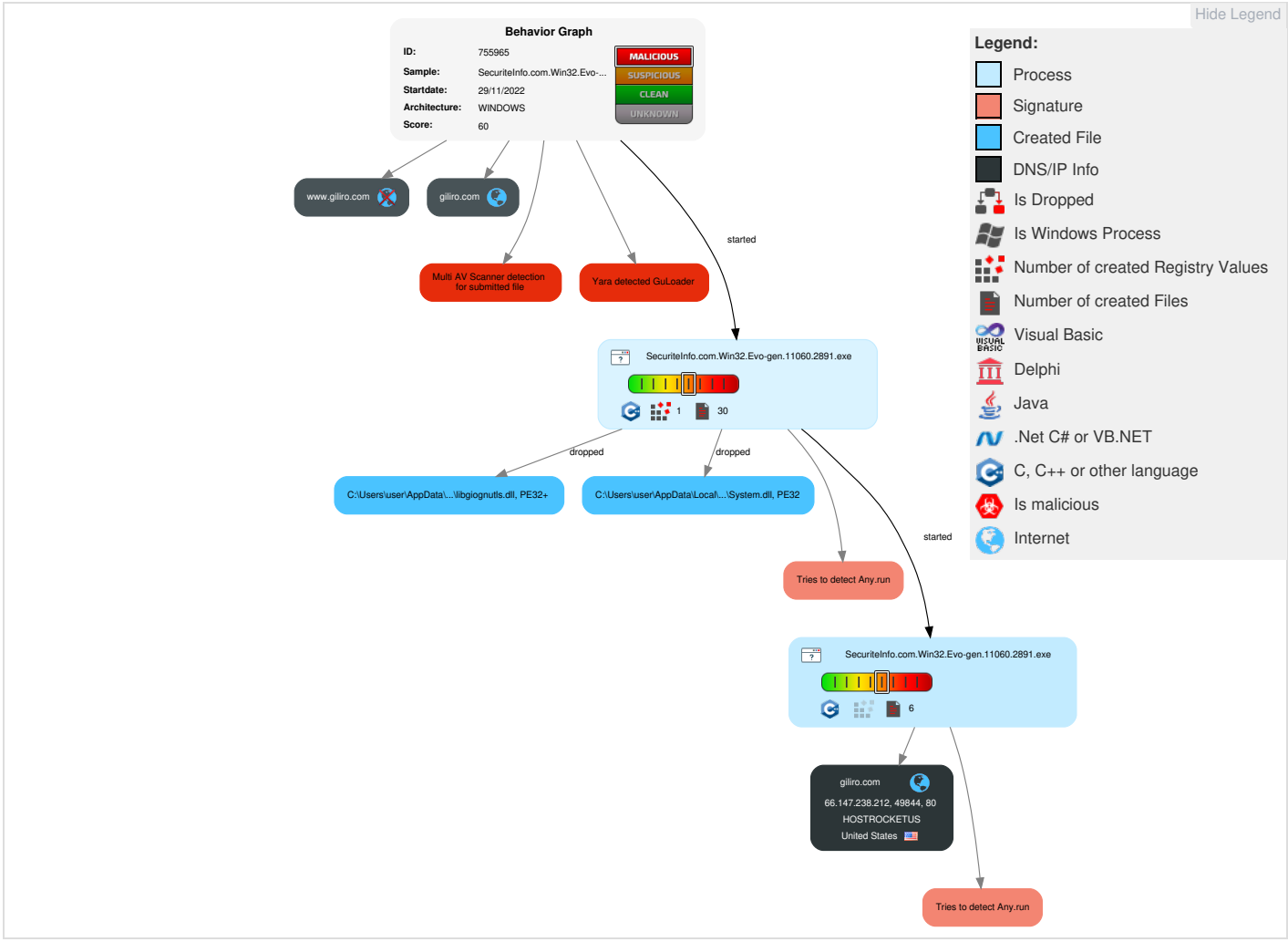
Malware Analysis System Evasion

Tries to detect Any.run

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	1 1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 2 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	1 DLL Side-Loading	1 1 Process Injection	1 Access Token Manipulation	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 Registry Run Keys / Startup Folder	1 1 Process Injection	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 Deobfuscate/Decode Files or Information	NTDS	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Obfuscated Files or Information	LSA Secrets	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	1 DLL Side-Loading	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

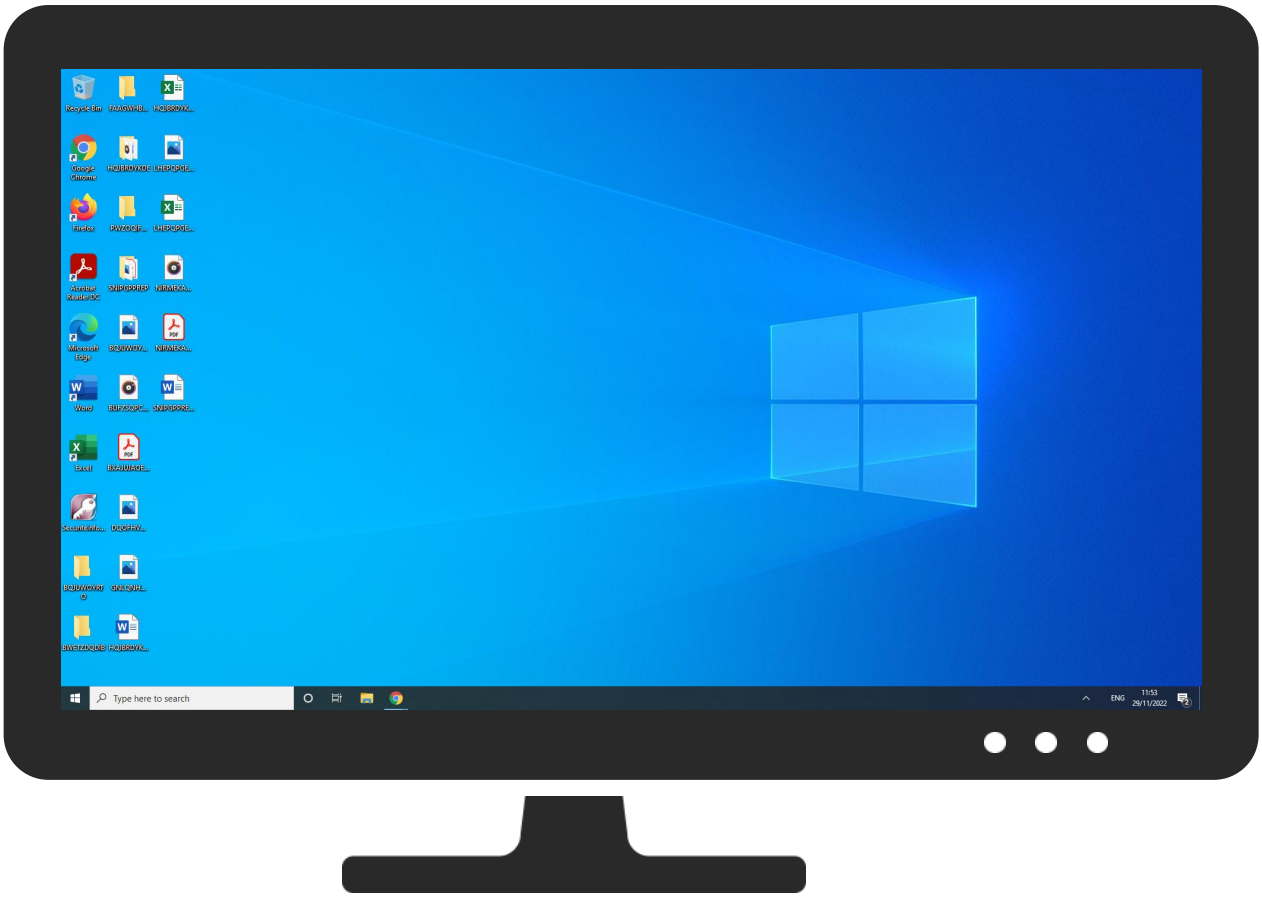
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe	29%	Virustotal		Browse
SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe	20%	ReversingLabs	Win32.Trojan.Nemesis	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsg51C2.tmp\System.dll	2%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Vatersotiges\Knoglemarvsundersgelsen\Armoniac\libgiognutls.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
www.giliro.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Avira URL Cloud	safe	
http://www.giliro.com/wnioMvShFMvcw54.emz32w	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	0%	Avira URL Cloud	safe	
http://www.giliro.com/wnioMvShFMvcw54.emz	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%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://www.giliro.com/wnioMvShFMvcw54.emzV	0%	Avira URL Cloud	safe	
http://www.gopher.ftp://ftp.	0%	Avira URL Cloud	safe	
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	0%	Avira URL Cloud	safe	
http://www.giliro.com/wnioMvShFMvcw54.emzG	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
giliro.com	66.147.238.212	true	false		unknown
www.giliro.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

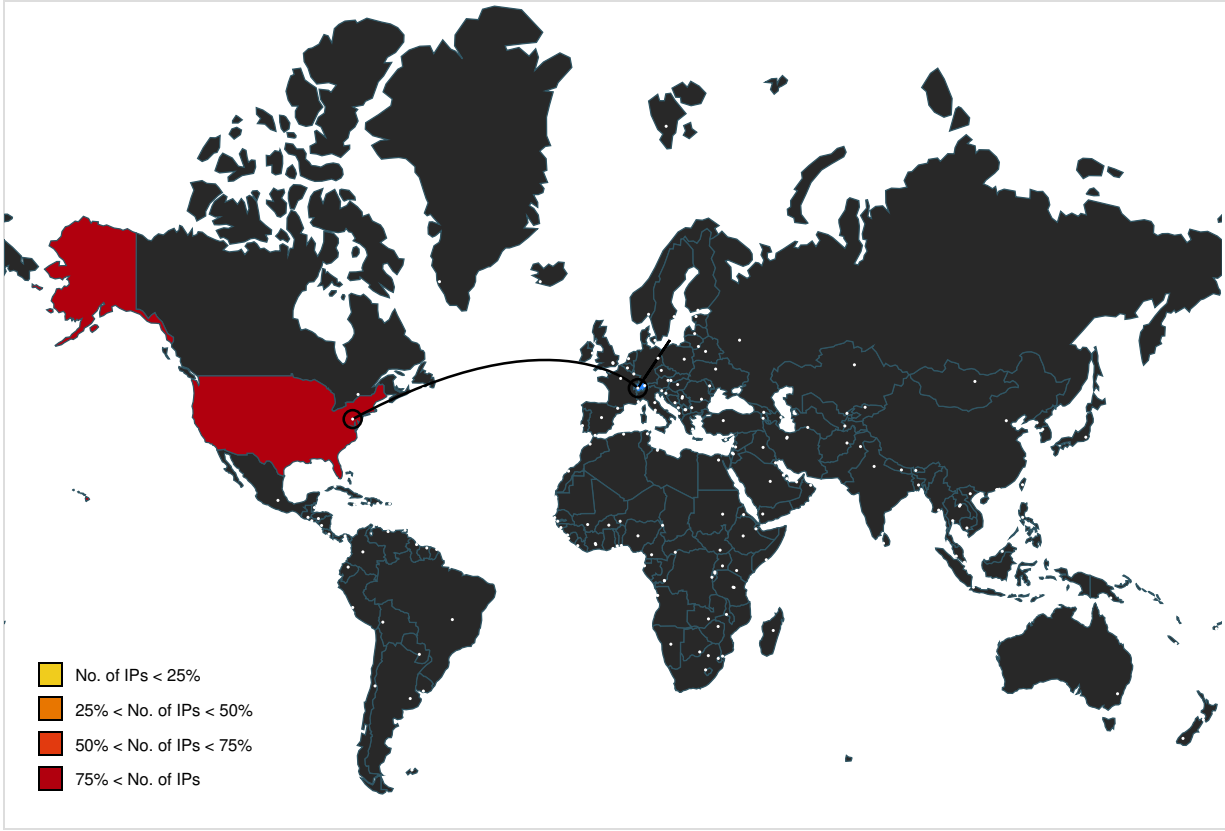
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.giliro.com/wnioMvShFMvcw54.emz	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe, 00000005.00000001.39482313722.0000000000649000.00000008.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe, 00000005.00000001.39481928947.00000000005F2000.00000008.00000001.01000000.00000005.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe, 00000005.00000001.39481928947.00000000005F2000.00000008.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.giliro.com/wnioMvShFMvcw54.emz32w	SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe, 00000005.00000002.44176068670.000000000190C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe	false		high
http://www.giliro.com/wnioMvShFMvcw54.emzV	SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe, 00000005.00000002.44176379660.0000000001936000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.giliro.com/wnioMvShFMvcw54.emzG	SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe, 00000005.00000002.44176379660.0000000001936000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd-//W3O//DTD	SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe, 00000005.00000001.39482152594.0000000000626000.00000008.00000001.01000000.00000005.sdmp	false		high
http://www.gopher.ftp://ftp.	SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe, 00000005.00000001.39482313722.0000000000649000.00000008.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe, 00000005.00000001.39482313722.0000000000649000.00000008.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.147.238.212	giliro.com	United States		23535	HOSTROCKETUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755965
Start date and time:	2022-11-29 11:43:57 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 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:	8
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:	mal60.troj.evad.winEXE@3/4@1/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 45.5% (good quality ratio 43.8%) • Quality average: 77.4% • Quality standard deviation: 24.9%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, wdcp.microsoft.com
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nsg51C2.tmp\System.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	11776
Entropy (8bit):	5.656065698421856
Encrypted:	false
SSDEEP:	192:eY24sihno00Wfl97nH6T2enXwWobpWBTU4VtHT7dmN35Ol+Sl:E8Qll975eXqlWBrz7YLOl+
MD5:	17ED1C86BD67E78ADE4712BE48A7D2BD

SHA1:	1CC9FE86D6D6030B4DAE45ECDDCE5907991C01A0
SHA-256:	BD046E6497B304E4EA4AB102CAB2B1F94CE09BDE0EEBBA4C59942A732679E4EB
SHA-512:	0CBED521E7D6D1F85977B3F7D3CA7AC34E1B5495B69FD8C7BFA1A846BAF53B0ECD06FE1AD02A3599082FFACAF8C71A3BB4E32DEC05F8E24859D736B828092CD5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...u.u.u...s.u.a....r.!..q....t....t.Richu.....PE..L.....MX.. .....!..... .....'.....0.....`.....2.....0..P.....P.....0..X.....text..... ..... ..... ..`.rdata..S....0.....$.....@..@.data...x....@.....(.....@....reloc..b....P.....*.....@..B..... .....

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe
File Type:	data
Category:	dropped
Size (bytes):	178824
Entropy (8bit):	6.515135274289935
Encrypted:	false
SSDEEP:	1536:Aqnh3ZWvlivpBh2LoIEVEF+F2MVQ454gp3cHE6xBiP29vpAX5D57DwVaDXW:RkYzh2Lol/FdUJNfPgk5DVDUd
MD5:	52F571D999E9DD5B6ABFFE0CC9BF8DF3
SHA1:	67743CD31368EA4C7C350C5071A6B1D8A5AF400B
SHA-256:	7CC58916DBEADFF389E9375FD1F8973DB606156E953F309C55C40384E54765E3
SHA-512:	0BA04B8CDA196099229824B65348B71483D50377D10660AF8CD70A10919A310D88DDBA80D1F595524F71764BB2A765C87B9E5E2276391B11A272A52E3BBA7C11
Malicious:	false
Reputation:	low
Preview:	...6.{..N..p2...H.=L.]......l..b.0..2).v..X..~..q..nm.9..$h....YZ..}..V.u..E.a(M.....q.....@9.n.`7.....z.N...<...&..h..\.....&.h@p.....%.~5._b..b.....B(....:.4.....t.S0..J..0.h.&. .H.t.gV.&..y.,J.3...m..\.....~n..L.AnI.....C.a.7w^!9.D.]J.....p...C8..Hn.....14.|.. ...k....._9.....@%.....S..d.>.*I.9.@.....I.....,4G.I.}..e....<.....]...wj.Z.^..j.Fv.#..9n.c{.`..4U...,Q... v.g.t)..o...g.....E.}..9...1....Wbl..JT%8..m[x.a.u.7.i).....1+..$l@...x$.~.....6q.BE.x..7...n.n..gOZ.V.7..6.a!.c....`.vGm).."L#~..E.....tV.....DjX.....Z.>..Z.).c.....D7}d.v.. . .%...v.fH.....Cw..x.^.....b\ct....Y.*.g.b...1*cR..%6F'.....Q-.....GH....L!?1...<.^Rf.G.H[O.<.Ke.....R..._e..1..s.....y.~..x!...Tl.... .a .;..KG.]%:."%.O..X.S..b..t.o{.....#..9...b. .J.e..w...<~b.....5.....XC....Z....E.zE.g.k.X.^.=.W)...>.'K.h<.C\././.7.d.....~./.a~.Yc.....4...{....d..m."...v.....v".....iY....9..ka.....M...m.})....Y..f..-..4..

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

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

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	131991
Entropy (8bit):	5.8780987492725405
Encrypted:	false
SSDEEP:	1536:v6J1cdTEl2OzvUtevCuoCW9fPr+vo9F5J7YWv3vbRnBycYWOGWSeaGymtYWOGWSS:VdW2OLgNCwXKSH8WPvVBjA+KE8S5

MD5:	10D998CF80B4437C2979B25EBCBE16D1
SHA1:	79C99DD2ABB99253E41C5E40DAB29522F93345BB
SHA-256:	A0A87BC30F4B39D7B642841A10208CE5286C6CA712B28B9D921E1EA6F547AEE6
SHA-512:	44863645B48815C3C248111F86440E3A0C515AF61B5A17D15B5A6C7304277F76056BCEB6C579E7824E11ADCA4DB3E385FA8019D602C40FA527E725C09B6AA523
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....&"...%.....P.....@.....g}.. ..`... .....IE.....0..... i..(.....text...X.....`..`.data..... .....@. ...rdata...A...0...B.....@..@.pdata.....R.....@..@.xdata..X.....`.....@..@.bss....p.....edata.....n.....@..@.idata.. IE.....F...p.....@....CRT....X.....@....tls..... .....@....reloc.....0.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.505402259729816
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe
File size:	477800
MD5:	7081c4822cf1c7572dd82822b8f27c49
SHA1:	4ee3b6c423b1c9ebf5befbc73d1eef0c576cf026
SHA256:	b5330f82f3c5c3f223ae9decd3ebdcd74d1a13d95b1c42bd7b2de4e6c6cb0083
SHA512:	6e3377e6a47518f2267cd38646e2cec576d41fd8a67c8c2590f43bf353c0b1f322fc229e70bc98e9c7dfaa1a11cf872a0c8e2c15a31ee90ef1c4e65eac98ee3a
SSDEEP:	12288:Lz772qgvq2nLm4W2RPLKb+nFzIQ3Ja8TA:gXnS4W2RPLKm/of
TLSH:	4DA4D096F74155D6CC24177259BB9D3702B3BD7E14B10B5F61AE32322F332828A07A2E
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...P...P...P..*_...P...P..OP..*_...P...s...P...V...P..Rich.P.....PE..L...8.MX.....b...*.....J4.....@

File Icon

Icon Hash:	b8eee6a4c0c8c6c2

Static PE Info

General

Entrypoint:	0x40344a
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x584DCA38 [Sun Dec 11 21:50:48 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	4ea4df5d94204fc550be1874e1b77ea7

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN=Warrambool, OU="Gennembryde Catbrier ", E=Lrerforsamlingen@Resoneres187.ti, O=Warrambool, L=Betpouy, S=Occitanie, C=FR
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 16/05/2022 14:16:58 15/05/2025 14:16:58
Subject Chain	• CN=Warrambool, OU="Gennembryde Catbrier ", E=Lrerforsamlingen@Resoneres187.ti, O=Warrambool, L=Betpouy, S=Occitanie, C=FR
Version:	3
Thumbprint MD5:	50955086B951A7063EA053252647D196
Thumbprint SHA-1:	B2C1191B987021E62094F55BD9D8BCF9138BF3A6
Thumbprint SHA-256:	26FCB244ABFE2816CFB307605DB0353DBE6BE089ACEC8D49A63FDE728C428741
Serial:	D479F570518060D0

Entrypoint Preview
Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A230h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080B4h]
call dword ptr [004080B0h]
cmp ax, 00000006h
je 00007EFC28FA74F3h
push ebx
call 00007EFC28FAA64Ch
cmp eax, ebx
je 00007EFC28FA74E9h
push 00000C00h
call eax
mov esi, 004082B8h
push esi
call 00007EFC28FAA5C6h
push esi
call dword ptr [0040815Ch]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007EFC28FA74CCh
push ebp
push 00000009h
call 00007EFC28FAA61Eh
push 00000007h
call 00007EFC28FAA617h
mov dword ptr [0042A244h], eax
call dword ptr [0040803Ch]
push ebx
call dword ptr [004082A4h]
mov dword ptr [0042A2F8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx

Instruction
push 004216E8h
call dword ptr [00408188h]
push 0040A384h
push 00429240h
call 00007EFC28FAA200h
call dword ptr [004080ACh]
mov ebp, 00435000h
push eax
push ebp
call 00007EFC28FAA1EEh
push ebx
call dword ptr [00408174h]
add word ptr [eax], 0000h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6e000	0x28868	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x73510	0x1558	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b4	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x61f1	0x6200	False	0.6656967474489796	data	6.477074763411717	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x13a4	0x1400	False	0.4529296875	data	5.163001655755973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20338	0x600	False	0.501953125	data	3.9745558434885093	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x43000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x6e000	0x28868	0x28a00	False	0.4693269230769231	data	6.072692072533226	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x6e3b8	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States
RT_ICON	0x6e720	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x7ef48	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 36864	English	United States
RT_ICON	0x883f0	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 20736	English	United States
RT_ICON	0x8d878	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384	English	United States
RT_ICON	0x91aa0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	English	United States
RT_ICON	0x94048	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	English	United States
RT_ICON	0x950f0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	English	United States
RT_ICON	0x95a78	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	English	United States
RT_DIALOG	0x95ee0	0x144	data	English	United States
RT_DIALOG	0x96028	0x13c	data	English	United States
RT_DIALOG	0x96168	0x100	data	English	United States
RT_DIALOG	0x96268	0x11c	data	English	United States
RT_DIALOG	0x96388	0xc4	data	English	United States
RT_DIALOG	0x96450	0x60	data	English	United States
RT_GROUP_ICON	0x964b0	0x76	data	English	United States
RT_MANIFEST	0x96528	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

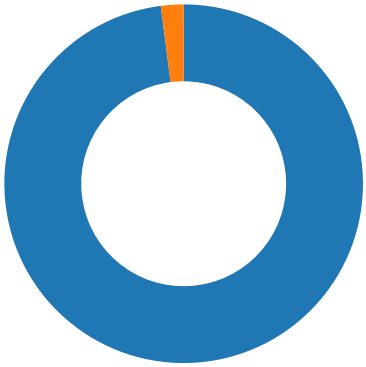
DLL	Import
KERNEL32.dll	SetCurrentDirectoryW, GetFileAttributesW, GetFullPathNameW, Sleep, GetTickCount, CreateFileW, GetFileSize, MoveFileW, SetFileAttributesW, GetModuleFileNameW, CopyFileW, ExitProcess, SetEnvironmentVariableW, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, GetVersion, SetErrorMode,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

Possible Origin

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

Network Behavior

Network Port Distribution



Total Packets: 49

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 11:46:42.054048061 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.148497105 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.148823977 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.149955034 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.244431973 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.244541883 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.244872093 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.255182981 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.255256891 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.255314112 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.255362988 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.255367041 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.255418062 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.255425930 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.255481958 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.255536079 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.255542994 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.255589962 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.255616903 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.255645990 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.255649090 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.255695105 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.255743980 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.255793095 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.339199066 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.339277983 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.339426041 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.339488029 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.349769115 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.349843979 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.349900961 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.349956036 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.349958897 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.350009918 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.350013018 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.350013018 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.350064039 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.350119114 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.350157022 CET	49844	80	192.168.11.20	66.147.238.212

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 11:46:42.350172997 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.350208044 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.350208044 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.350229979 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.350285053 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.350305080 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.350338936 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.350353956 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.350393057 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.350402117 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.350447893 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.350451946 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.350452900 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.350501060 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.350548983 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.350555897 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.350600958 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.350610971 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.350646973 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.350665092 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.350704908 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.350718975 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.350814104 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.350902081 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.433693886 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.433739901 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.433778048 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.433815002 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.433886051 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.433886051 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.433940887 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.433980942 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.444833040 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.444906950 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.444966078 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.445008039 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.445024014 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.445081949 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.445097923 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.445097923 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.445138931 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.445197105 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.445197105 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.445254087 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.445303917 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.445311069 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.445355892 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.445368052 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.445405006 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.445425034 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.445473909 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.445473909 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.445480108 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.445537090 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.445584059 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.445584059 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.445594072 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.445652008 CET	80	49844	66.147.238.212	192.168.11.20
Nov 29, 2022 11:46:42.445700884 CET	49844	80	192.168.11.20	66.147.238.212

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 11:46:42.445700884 CET	49844	80	192.168.11.20	66.147.238.212
Nov 29, 2022 11:46:42.445708990 CET	80	49844	66.147.238.212	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 11:46:41.745608091 CET	50511	53	192.168.11.20	1.1.1.1
Nov 29, 2022 11:46:42.034929037 CET	53	50511	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 11:46:41.745608091 CET	192.168.11.20	1.1.1.1	0x5fa6	Standard query (0)	www.giliro.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 11:46:42.034929037 CET	1.1.1.1	192.168.11.20	0x5fa6	No error (0)	www.giliro.com	giliro.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 11:46:42.034929037 CET	1.1.1.1	192.168.11.20	0x5fa6	No error (0)	giliro.com		66.147.238.212	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.giliro.com

Statistics

Behavior

System Behavior

Analysis Process: SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe PID: 6064, Parent PID: 4656

General

Target ID:	1
Start time:	11:45:50
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe
Imagebase:	0x400000
File size:	477800 bytes
MD5 hash:	7081C4822CF1C7572DD82822B8F27C49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.39673477269.0000000003320000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Stempelpligtig93\Obeyeo.Bib	unknown	1052672	success or wait	1	10002965	ReadFile

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.Win32.Evo-gen.11060.2891.exe PID: 6832, Parent PID: 6064

General

Target ID:	5
Start time:	11:46:24
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Evo-gen.11060.2891.exe
Imagebase:	0x400000
File size:	477800 bytes
MD5 hash:	7081C4822CF1C7572DD82822B8F27C49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000005.00000000.39479578905.0000000001660000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1696752	success or wait	1	41A447	NtReadFile

Disassembly

No disassembly