ID: 632533
Sample Name: SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.6225
Cookbook: default.jbs
Time: 18:46:50
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report

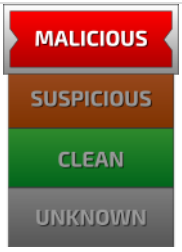
SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.6225

Overview

General Information

Sample Name:	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.6225 (renamed file extension from 6225 to exe)
Analysis ID:	632533
MD5:	c1863e820a135d..
SHA1:	e0846c1117045f..
SHA256:	feb8a71e0b6bb9..
Tags:	exe
Infos:	

Detection



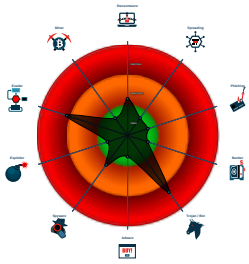
GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Antivirus or Machine Learning detec…
- Sample file is different than original …
- PE file contains strange resources
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe (PID: 6516 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe" MD5: C1863E820A135D468E9787F1F78970E2)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=16-ZmAFjeTzH9DAbqoP0u2zSq7p2C4wzm"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.545755937.00000000030B0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

Data Obfuscation

Yara detected GuLoader

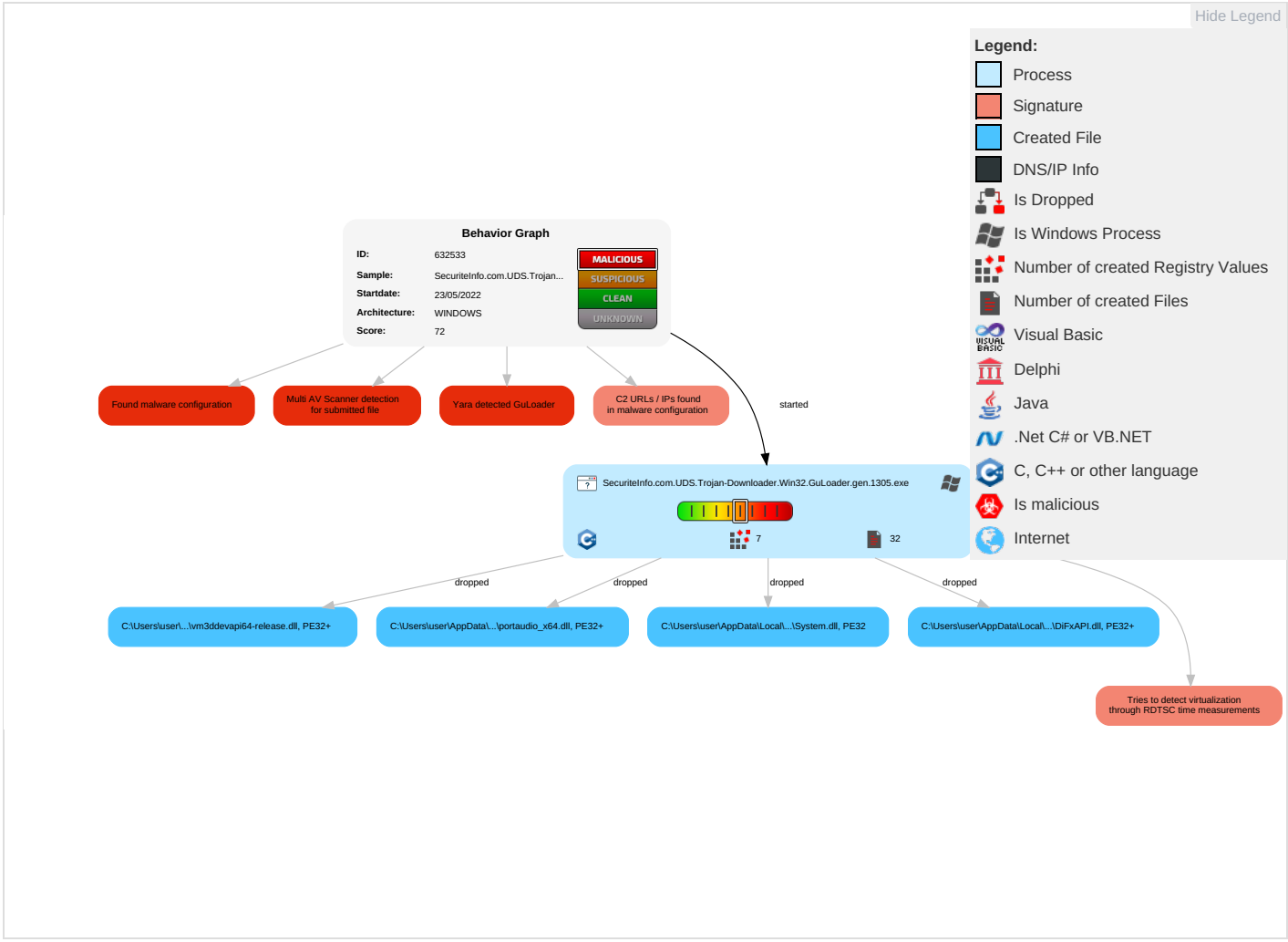
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	1 Access Token Manipulation	1 Access Token Manipulation	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Software Packing	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	1 3 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

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.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe	14%	Virustotal		Browse
SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe	7%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\DiFxAPI.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\DiFxAPI.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsl5F49.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsl5F49.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\portaudio_x64.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\vm3ddevapi64-release.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe.410c71.1.unpack	100%	Avira	ADWARE/Patched.Ren.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://subca.ocsp-certum.com05	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com02	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.certum.pl/ctsca2021.crl0o	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe	false		high
http://repository.certum.pl/ctnca.cer09	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe	false		high
http://www.vmware.com/0	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe, 00000000.00000002.545391405.000000000280D000.00000004.00000800.00020000.00000000.sdmp, vm3ddevapi64-release.dll.0.dr	false		high
http://repository.certum.pl/ctsca2021.cer0	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe	false		high
http://crl.certum.pl/ctnca.crl0k	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe	false		high
http://subca.ocsp-certum.com05	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe	false	• Avira URL Cloud: safe	unknown
http://www.symauth.com/rpa00	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe, 00000000.00000002.544470071.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe, 00000000.00000002.545391405.000000000280D000.00000004.00000800.00020000.00000000.sdmp, vm3ddevapi64-release.dll.0.dr	false		high
http://subca.ocsp-certum.com02	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe	false	• URL Reputation: safe	unknown
http://subca.ocsp-certum.com01	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe	false	• URL Reputation: safe	unknown
http://crl.certum.pl/ctnca2.crl0l	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe	false		high
http://repository.certum.pl/ctnca2.cer09	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe	false		high
http://www.vmware.com/0/	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe, 00000000.00000002.544470071.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe, 00000000.00000002.545391405.000000000280D000.00000004.00000800.00020000.00000000.sdmp, vm3ddevapi64-release.dll.0.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.symauth.com/cps0(	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe, 00000000.00000002.544470071.000000000040A000.00000004.00000001.01000000.00000003.sdmp, SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe, 00000000.00000002.545391405.000000000280D000.00000004.00000800.00020000.00000000.sdmp, vm3ddevapi64-release.dll.0.dr	false		high
http://www.certum.pl/CPS0	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632533
Start date and time: 23/05/202218:46:50	2022-05-23 18:46:50 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.6225 (renamed file extension from 6225 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.troj.evad.winEXE@1/8@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 86% (good quality ratio 84.7%) • Quality average: 87.8% • Quality standard deviation: 21.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, store-images.s-microsoft.com, login.live.com, ctldl.windowsupdate.com, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- 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\DiFxAPI.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	526456
Entropy (8bit):	6.008806658212827
Encrypted:	false
SSDEEP:	12288:5sxYL+kJmoPdVp6s3EJBjCvuF17+2NdJfh:5sxwSoPdVoBjCvuF17+2NdJfh
MD5:	52672A1E48BC8BE4035D8A4F345DFE44
SHA1:	4F7EB09FF33DFACE6CE24BEB33E51D1DA5A3ABA1
SHA-256:	87BA988A4858079CADCA5EAA760482CC5F1F05830EE62BBC5FDD9BF7B181F0D0
SHA-512:	4F589CE3FC97F1DBDB575510924B5AEA58061B2D95F909456ACDB170414282A081C18CA9945E604FBCE6F17D626B02B178E66294927C5350B91072357DABAEF
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....$.....T1...P.F.P.F.P.F7..F.P.F.P.F#Q.F7..F.P.F7..F.P.F7..F/P.F7..F.P .F7..F.P.F7..F.P.F7..F.P.F7..F.P.FRich.P.F.....PE..d.....IE....." ....$.....a.....0.....x....@.....0.....P.....`.. .....x.... .....p.....(.....text...L".....$..... ..`.data...0....@.....(.....@....pdata.....`.....0.....@..@.rsrc..... .....@..@.reloc..$.... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\Forbudenes2.MON

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe
File Type:	data
Category:	dropped
Size (bytes):	85376
Entropy (8bit):	6.4589932976051125

Encrypted:	false
SSDEEP:	1536:6ybWiSppvqBzm4gSPbgnNjbZl9IJ9ISQRyQWG:dbbOpGzm4gSPwZK3ISWWG
MD5:	F0B06E29DCFE977FC30F6CD15CC4962B
SHA1:	7A3F4FEA84FDE5D28E35915E5D3EDC74D3D7E1A8
SHA-256:	107B2444699BBD4FB8BAF65EDB23F1AA7B082B8C08F2FDD1F608DEBC43857B6C
SHA-512:	1C68088B84847545A2CD527FC5EC14F05D5884AFFBC7EC6EAEB5B426DC3079A50A29822790015E8A8C7FC5744A95C4F075BE12BAB108BD5AF9954E3CB4B03B78
Malicious:	false
Reputation:	low
Preview:	.....f.....1...fffffffffffffffffffffffffffffffffffffffff.f.....`..,.-l.vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv.....f.n.,..X.....f.h.f.e...../vs.....7'..[..... .f...f.b.f.r....3..e;```.....c.. ..7nEEEEEEEEEEEEEEEEEEEEEEEEEEE.&.)i.. .....$.D7<.....f.....f.j.....f....5w..-.....J.-@JJJJJJJJJJJJJJJJJJJJJJJJ<#.....0M%._<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<f.....f.c..u.....!..Z?.....f...wf.d.....3}.LB1111111111111111111111111111111111111111111111111.....~.....%*..!555555555555555555555555555555555.....$..!wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww.....f.u.....c..e.....f.....f.c.....9.}.....f.....

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide
Category:	dropped
Size (bytes):	912
Entropy (8bit):	3.0099451499929035
Encrypted:	false
SSDEEP:	12:8gl00sXou41w/tz+7RafgKD7A6K5wKNLkwKNeg/3NJkKAd4t2Y+xIBjK:8Df4eaRMgKfAh5JNoJNe49HAv7aB
MD5:	01DF88835AF6086863EF4F022BD18DF3
SHA1:	58B994BF0E9D425CB807F5D1FEB258BF6F904D8E
SHA-256:	2978C4613981F35AE451A7FD20C06854ED7AC5306EBDC77DCDB71A457A65414D
SHA-512:	4FEF45A8B203F1B425CF180CEBDFAAF128A25A0A1FC5EC10C91D875157282B7F94331B79CE843112946D7007C4F5DA2D8719908350A0A1FF68A43597B17E3FC
Malicious:	false
Reputation:	low
Preview:	L.....F.....G....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....P.1.....user.<.....h.a.r.d.z.....V.1.....AppData.@.....A.p.p.D.a.t.a.....P.1.....Local.<.....L.o.c.a.l.....N.1.....Temp..:.....T.e.m.p.....2.....Prologfortolkernes.exe..^.....P.r.o.l.o.g.f.o.r.t.o.l.k.e.r.n.e.s...e.x.e...&.....\.P.r.o.l.o.g.f.o.r.t.o.l.k.e.r.n.e.s...e.x.e.....(.....l^".`G...3..qs.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2...

C:\Users\user\AppData\Local\Temp\Standardiserede7.sma

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	28538
Entropy (8bit):	3.99969839684347
Encrypted:	false
SSDEEP:	384:ack3J1V0v3sPqlYpd5b+QnSp9RSa4k75yUXkv0kE6QlV6uU1KeKQHZ6wlmcM6qTx:acqwxWpbhnyGSEU65KAAwl4aZizuupd
MD5:	D929AC69DE308581CF1CC35EBBFA488B
SHA1:	BE7C776F3E7AF782A8B2DD02C34711357A131853
SHA-256:	B5AA2FA0DA767023E6B44DC3F0EC6746D4F8BDE83A36223055671139F4BE7E38
SHA-512:	4495A77C13B10DA4DA8C525D6D21BFB0A3EC3245592BA7132519B4547294A3EF9182C8B6E08BE1E1BEA2D366DF8F70D1DE9F0B8842A3910294271C5D9D00830
Malicious:	false
Reputation:	low
Preview:	595A6E42D27573DAF244E9FF390E425A98D4710BA207C3408B31B159DED32A559FE8811B49009154652C0D8507476DA6F1B639EEB4E3E21F77963258 680F6D82867D723BFC23C6C08889335E61BB60568740FA09AC6E1937458B4B395C62E068FA12D284D10999D444B51ADC8C7288619BAAD010935F5AB5 94454C0371BF03E0149D543A3EA33501B3BF46E253685A732172441578B7FDC897E03645C4150E9F17FA4CAF59752F11091D862C1AD5D4CE23AB2FA6 534B9077405B3E88FBCAE8C500CC2B6DF7698BBF031D5ED427888CC51D90BE7C84719B527A7D34AD730999F6B4E46D4F3C67E2614F4FBA5656930CD0 BC6A8A20E6F147A79B78DBC19E4E022358F128FAE7FBAD69224315601EB0E92D652E58BC8317E4E3FBF6CBAAC82188593FD3ADD28C28C09A36E8F2FC 116594D494DAFE998F42B31E83F66539EC17B8C7D0F46EE4B0492FBB7874F54D1A59EC5DB4A66933C9D634303CB76716BD6B33341EC7F90E5E6011AA A1C0CE6A33FD40A7124AA016BD9D53F62E29B4D344F12394918ECCC736F1D53219A2B7A73950E858BA959F90E8D52D47F03AC44989B8CD22C4791AE1 E9D56DE17229DA7CF268C6FBD5CEB507C09D20A2C658D86BBA417B6B9ACDA3C9D65CDE47F031BDEF0049A137471BB36FC18F4DDCC0902A817A4274A0 58AD70FBEF802DA2BC9BD2EDB5FD955DC87E4B25

C:\Users\user\AppData\Local\Temp\document-open-recent-symbolic.svg

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped

Size (bytes):	856
Entropy (8bit):	5.104082637403519
Encrypted:	false
SSDEEP:	12:t4CP5GdKdj9xclSaRaUlYzXHnbt1tUg1yU2hz4AeWTjiu+1ITpLhz4AeWK:t4CBGMFklSelln4AeWoI9x4AeWK
MD5:	93721360A2E739317994A0478117B840
SHA1:	459A0D7C35526AD3E03BE62E41C2AC1BF2518F6A
SHA-256:	15322D905A2DA0DFC566C0A17E9CFB303F5EDCCDB97CF30970AAEF6249E3A67A
SHA-512:	9AEFEB4749652BD968AF4F5FB9009715E913848F8662DF54955B9D0A25AEC10F0FC6701D4E470E4C5DC2CAC3A28073DDA13E1BC57F32319D5ECF83DC588EEC62
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g color="#000" font-weight="400" font-family="Sans" fill="#474747"><path d="M8.487.02A7.492 7.492 0 001 7.507a7.492 7.492 0 007.487 7.486 7.492 7.492 0 007.486-7.486A7.492 7.492 0 008.487.02zm0 1.973A5.508 5.508 0 0114 7.507a5.508 5.508 0 01-5.513 5.513 5.508 5.508 0 01-5.514-5.513 5.508 5.508 0 015.514-5.514z" style="line-height:normal;-inkscape-font-specification:Sans;text-indent:0;text-align:start;text-decoration-line:none;text-transform:none;marker:none" overflow="visible"/><path d="M11.393 4.007a.5.5 0 00-.25.156L8.487 6.819 6.83 5.163a.5.5 0 10-.687.687l2 2a.5.5 0 00.687 0l3-3a.5.5 0 00-.437-.843z" style="line-height:normal;-inkscape-font-specification:Sans;text-indent:0;text-align:start;text-decoration-line:none;text-transform:none;marker:none" overflow="visible"/></g></svg>

C:\Users\user\AppData\Local\Temp\nsl5F49.tmp\System.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
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%
Reputation:	moderate, very likely benign file
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\portaudio_x64.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	210400
Entropy (8bit):	6.556455859693611
Encrypted:	false
SSDEEP:	3072:eNDA0+ExUEe7nocc+HBmLhE8ErHTfxWEvoMhVGNDKE7tjHZYZdH:M+E6fE+ILa8yF3voMVGVKE4H
MD5:	B38B3ABD5349D92C63D450DF34C73D4C
SHA1:	F58BA8CC0D2E9A1F0D5DF7518BB9DE39D35E224E
SHA-256:	B52F564D867924895D80019267CF3E05F5D945755096ECEBCECB77599AE36B82
SHA-512:	D35820246E48D72C060A725F792FB61F0BA86D6F0B100EF45B0C960C14D4C8DE788BA061B29A05BC9312ED7977D3B8D593024457C9DA54239ABB40DCA9CDFDE
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t..t..t.....t..u..t..q..t..p..t..w..t..p..t..u..t..u.s.t.>.p..t.>.t...t.>....t.....t.>.v...t.Rich..t.....PE..d....5`.....".....N.....H.....P.....H....`.....P.....0..h.....!...@.....T.....`.....text..... ..`.rdata.....@..@.data...p.....@....pdata.....@..@.rsrc...h....0.....@..@.reloc.....@.....@..B.....

C:\Users\user\AppData\Local\Temp\vm3ddevapi64-release.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows

Category:	dropped
Size (bytes):	272968
Entropy (8bit):	6.525125544096022
Encrypted:	false
SSDEEP:	6144:yGDcBJz3nXgJhw/171Ewc6Jlih+GtOjrLbR8XtVbQ:yGDcnAJC/1pvJXJAtVbQ
MD5:	31DC360E537F919FC03540C17539E3C1
SHA1:	33ABED31822A0F8590079C8E20A1DC3EBA7EB334
SHA-256:	1C2BF2248AC56F213B4888FC756AE26ED3E61B7D5A16C1464E421CFBB3528B03
SHA-512:	2C1FFB5FE35AD53DF3149E31ABAA32F23DFA3DA920727FEBF39D19FD728408D1C00415E8F863B795EDF37645DD8FB8DE477F2EE4EDA38DCBCD15465A7A93EF20
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....8.....!..L.!This program cannot be run in DOS mode....$.....[.....s.....s.....s.....M.....z.....z.....G.....Rich.....PE..d.....`......" .....T.....@.....PJ....`A.....t..... .....Hb...0..... m..8.....k..8.....@.....text..... ..`.rdata..2.....@..@.data...0#.....@....pdata.....@..@.didat..H.....@....gehcont$.....@..@_RDATA.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.6857232930420745
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.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe
File size:	603464
MD5:	c1863e820a135d468e9787f1f78970e2
SHA1:	e0846c1117045f4ee73a6493e2207d4f27056b9e
SHA256:	feb8a71e0b6bb912ce22c67275eba157fb10f626e18faeb5119789c7e89ecabd
SHA512:	6607743de9ca76c7d7f6a57f63b196892a510c30afccee0cef9132460eaabe145b418b9bb5c21fa48717e1353f1c91ed2fc8cc86ab42c8b64b3b80acaea92931
SSDEEP:	12288:RYCEkC0keucJfmGquXqvJStyHzPchra7PZLCyEcz1F:RYCBC04q1AUZGnXz3
TLSH:	59D4DFB2F7D48A4BFD02677895E192683DFB9CE16223E30B114D3D17BEB67693244182
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....

File Icon

Icon Hash:	f0e8ce9e96cce802

Static PE Info

General

Entrypoint:	0x403640
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B1F [Sat Sep 25 21:56:47 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4

File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	61259b55b8912888e90f516ca08dc514

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN="maskindokumentation eringen draperer prisfald ", O=Fysioterapeutskolerne5, L=Saint-Maurice-prÃ¨s-Crocq, S=Nouvelle-Aquitaine, 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	• 5/23/2022 3:56:10 AM 5/23/2023 3:56:10 AM
Subject Chain	• CN="maskindokumentation eringen draperer prisfald ", O=Fysioterapeutskolerne5, L=Saint-Maurice-prÃ¨s-Crocq, S=Nouvelle-Aquitaine, C=FR
Version:	3
Thumbprint MD5:	7735A8EAAFDB10F20731055B3C25398B
Thumbprint SHA-1:	891C6FE7C7361A0AE542A7DAA25078799E3ADDF5
Thumbprint SHA-256:	44C99CC90CD9A321BC61E47D59498840554B9C58C770B7BCF0777E7BA2193C09
Serial:	6132FE7805280AAC

Entrypoint Preview
Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F3098FCC41Ah
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

Instruction
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F3098FCC3EAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x62000	0x21848	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x91610	0x1f38	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6676	0x6800	False	0.656813401442	data	6.41745998719	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.14106681717	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.11058212765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x37000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x62000	0x21848	0x21a00	False	0.418455216078	data	5.86806441388	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x62328	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 16777216, next used block 16777216	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x72b50	0x7d38	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x7a888	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 128, next used block 16777216	English	United States
RT_ICON	0x7eab0	0x25a8	data	English	United States
RT_ICON	0x81058	0x10a8	data	English	United States
RT_ICON	0x82100	0x988	data	English	United States
RT_ICON	0x82a88	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x82ef0	0x100	data	English	United States
RT_DIALOG	0x82ff0	0x11c	data	English	United States
RT_DIALOG	0x83110	0xc4	data	English	United States
RT_DIALOG	0x831d8	0x60	data	English	United States
RT_GROUP_ICON	0x83238	0x68	data	English	United States
RT_VERSION	0x832a0	0x264	data	English	United States
RT_MANIFEST	0x83508	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

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

Version Infos

Description	Data
LegalCopyright	MAALERES
FileVersion	18.16.25
CompanyName	Easterner
LegalTrademarks	KRONISKESSKLSKR
Comments	archeressbronz
ProductName	Suber
FileDescription	Sekstifem
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map

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

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe PID: 6516, Parent PID: 6020

General

Target ID:	0
Start time:	18:48:06
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe"
Imagebase:	0x400000
File size:	603464 bytes
MD5 hash:	C1863E820A135D468E9787F1F78970E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.545755937.00000000030B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsf5DEF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsa5E1F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	405C22	CreateDirectoryW

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	3	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405C22	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Serveren77	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Serveren77\Coccic146	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsl5F49.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsl5F49.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405BE2	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Serveren77	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Serveren77\Coccic146	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Forbudenes2.MON	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\DiFxAPI.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\Standardiserede7.sma	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\document-open-recent-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\portaudio_x64.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\vm3ddevapi64-release.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\nsl5F49.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\nsl5F49.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	3	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsf5DEF.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsl5F49.tmp	success or wait	1	405DA3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	32768	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	406224	WriteFile
unknown	51712	25441	75 6e 6b 6e 6f 77 6e	unknown	success or wait	47	406224	WriteFile
C:\Users\user\AppData\Local\Temp\Forbudenes2.MON	0	16384	fd fd fd fd 0f 66 50 0f fd fd 0f fd fd fd 31 fd bd 1f 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 fd 66 0f fd fd fd fd 0f fd fd 0f 60 fd fd 2c fd 2d 6c 17 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 76 fd fd fd fd fd 0f fd fd 66 0f 6e fd fd 2c fd fd 58 1a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a fd fd 00 66 0f 68 fd 66 0f 65 fd 0f fd fd 0f fd fd fd 2f 76 73 fd 7f fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd c3 fd 00 fd fd fd	f1fffffffffffffffffffffffffff fffffffffffffffff`,-lvvvvvvvv vvvvvvvvvvvvvvvvvvvvvvvv vvvvvvvvvvvfn,Xfhfe/vs	success or wait	6	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DiFxAPI.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 54 31 fd 15 10 50 fd 46 10 50 fd 46 10 50 fd 46 37 fd fd 46 12 50 fd 46 10 50 fd 46 23 51 fd 46 37 fd fd 46 0d 50 fd 46 37 fd fd 46 03 50 fd 46 37 fd fd 46 2f 50 fd 46 37 fd fd 46 11 50 fd 46 37 fd fd 46 08 50 fd 46 37 fd fd 46 11 50 fd 46 37 fd fd 46 11 50 fd 46 37 fd fd 46 11 50 fd 46 52 69 63 68 10 50 fd 46 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$T1PFPFPF7FPF PF #QF7FPF7FPF7F/PF7FP F7FPF7FPF7F PF7FPFRichPF	success or wait	33	406224	WriteFile
C:\Users\user\AppData\Local\Temp\Standardiserede7.sma	0	16384	35 39 35 41 36 45 34 32 44 32 37 35 37 33 44 41 46 32 34 34 45 39 46 46 33 39 30 45 34 32 35 41 39 38 44 34 37 31 30 42 41 32 30 37 43 33 34 30 38 42 33 31 42 31 35 39 44 45 44 33 32 41 35 35 39 46 45 38 38 31 31 42 34 39 30 30 39 31 35 34 36 35 32 43 30 44 38 35 30 37 34 37 36 44 41 36 46 31 42 36 33 39 45 45 42 34 45 33 45 32 31 46 37 37 39 36 33 32 35 38 36 38 30 46 36 44 38 32 38 36 37 44 37 32 33 42 46 43 32 33 43 36 43 30 38 38 38 39 33 33 35 45 36 31 42 42 36 30 35 36 38 37 34 30 46 41 30 39 41 43 36 45 31 39 33 37 34 35 38 42 34 42 33 39 35 43 36 32 45 30 36 38 46 41 31 32 44 32 38 34 44 31 30 39 39 39 44 34 34 34 42 35 31 41 44 43 38 43 37 32 38 38 36 31 39 42 41 41 44 30 31 30 39 33 35 46 35 41 42 35 39 34 34 35 34 43 30 33 37 31 42 46 30 33 45	595A6E42D27573DAF24 4E9FF390E42 5A98D4710BA207C3408 B31B159DED3 2A559FE8811B49009154 652C0D8507 476DA6F1B639EEB4E3 E21F77963258 680F6D82867D723BFC2 3C6C0888933 5E61BB60568740FA09A C6E1937458B 4B395C62E068FA12D28 4D10999D444 B51ADC8C7288619BAA D010935F5AB5 94454C0371BF03E	success or wait	8	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\document-open-recent-symbolic.svg	0	856	3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 3e 3c 67 20 63 6f 6c 6f 72 3d 22 23 30 30 30 22 20 66 6f 6e 74 2d 77 65 69 67 68 74 3d 22 34 30 30 22 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3d 22 53 61 6e 73 22 20 66 69 6c 6c 3d 22 23 34 37 34 37 34 37 22 3e 3c 70 61 74 68 20 64 3d 22 4d 38 2e 34 38 37 2e 30 32 41 37 2e 34 39 32 20 37 2e 34 39 32 20 30 20 30 30 31 20 37 2e 35 30 37 61 37 2e 34 39 32 20 37 2e 34 39 32 20 30 20 30 30 37 2e 34 38 37 20 37 2e 34 38 36 20 37 2e 34 39 32 20 37 2e 34 39 32 20 30 20 30 30 37 2e 34 38 36 2d 37 2e 34 38 36 41 37 2e 34 39 32 20 37 2e 34 39 32 20 30 20 30 30 38 2e 34 38 37 2e 30 32 7a	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g color="#000" font-weight ="400" font-family="Sans" fill="#474747"><path d="M8.487.02A7.492 7.492 0 001 7.507a7.492 7.492 0 007.487 7.486 7.492 7.492 0 007.486-7.486A7.492 7.492 0 008.487.02z	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\portaudio_x64.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 1a fd fd fd 74 fd fd fd 74 fd fd fd 74 fd fd fd fd fd fd fd 74 fd fd fd 75 fd fd fd 74 fd fd fd 71 fd fd fd 74 fd fd fd 70 fd fd fd 74 fd fd fd 77 fd fd fd 74 2f fd 70 fd fd fd 74 2f fd 75 fd fd fd 74 fd fd fd 75 fd 73 fd 74 fd 3e fd 70 fd fd fd 74 fd 3e fd 74 fd fd fd 74 fd 3e fd fd fd fd fd 74 fd fd fd fd fd fd fd 74 fd 3e fd 76 fd fd fd 74 fd 52 69 63 68 fd fd 74	MZ@!L!This program cannot be run in DOS mode.$ttttutqtptwtpt utust>pt>tt>tt>vtRicht	success or wait	13	406224	WriteFile
C:\Users\user\AppData\Local\Temp\vm3ddevapi64-release.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5b fd fd fd 1f 29 1f 29 1f 29 0b fd fd fd 14 29 0b fd fd fd 1a 29 0b fd fd fd 29 1f 29 1e 29 73 fd fd fd 15 29 73 fd fd fd 11 29 73 fd fd fd 02 29 7b fd fd 1e 29 4d fd fd fd 1c 29 fd fd fd fd 1e 29 7a fd fd fd 1e 29 7a fd fd fd 10 29 1f 69 fd 29 fd fd fd fd 0f fd	MZ@8!L!This program cannot be run in DOS mode.$[sssMzz	success or wait	17	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsl5F49.tmp\System.dll	0	12288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe	unknown	512	success or wait	351	4061F5	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe	unknown	16384	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsa5E1F.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsa5E1F.tmp	unknown	28566	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nsa5E1F.tmp	unknown	4	success or wait	3	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsa5E1F.tmp	unknown	4	success or wait	9	4061F5	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.1305.exe	unknown	16384	success or wait	25	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsa5E1F.tmp	unknown	16384	success or wait	78	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\Standardiserede7.sma	unknown	2	success or wait	1023	40275E	ReadFile
C:\Users\user\AppData\Local\Temp\nsa5E1F.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\Forbudenes2.MON	unknown	1048576	success or wait	1	72E62C59	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ABSCISSAS	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ABSCISSAS\Unpauperised	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Moringaceous	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Moringaceous\Forladegevrer193	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Celioncus	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Celioncus\POLEYNE	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\dbenavnet	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\dbenavnet\rehearhearing	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Unvamped92	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Unvamped92\Universitetsdirektrernes60	success or wait	1	406532	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Counterbrace57	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Counterbrace57\monaxon	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Kollapsen117	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Kollapsen117\Margygr	success or wait	1	406532	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ABSCISSAS\Unpauperised	Hjlpeskrmen	unicode	Conjugal192	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Moringaceous\Forladegevrer193	Expand String Value	expand unicode	%WINDIR%\Spder153.log	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Celioncus\POLEYNE	Expand String Value	expand unicode	%WINDIR%\musiclike.log	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\dbenavnet\rehearhearing	Duping181	binary	FF 7A D8 A9	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\Unvamped92\Universitetsdirektrrnes60	Idyls	binary	31 05 AF	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\Counterbrace57\monaxon	Expand String Value	expand unicode	%WINDIR%\hieromnemon.log	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Kollapsen117\Margygr	dorsicolumn	binary	55 45 EB	success or wait	1	40251B	RegSetValueExW

Disassembly

No disassembly