ID: 626513
Sample Name: SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.8895
Cookbook: default.jbs
Time: 06:29:06
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report

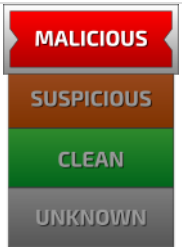
SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.8895

Overview

General Information

Sample Name:	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.8895 (renamed file extension from 8895 to exe)
Analysis ID:	626513
MD5:	6f790a9e28d73d..
SHA1:	1ec63e32364359..
SHA256:	2241716c3ddff7b..
Tags:	exe
Infos:	

Detection



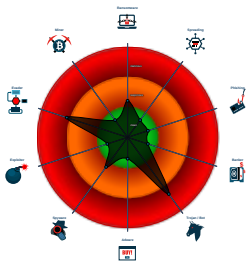
GuLoader

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Icon mismatch, binary includes an i…
- Antivirus detection for URL or domain
- Yara detected GuLoader
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- 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.17738.exe (PID: 6516 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe" MD5: 6F790A9E28D73D498C89A19CFE941D1B)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://185.236.228.217/private/Spread.bin"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.784638235.0000000003221000.00000040.00001000.00020000.00000000.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

Antivirus detection for URL or domain

Networking

C2 URLs / IPs found in malware configuration

Data Obfuscation

Yara detected GuLoader

Hooking and other Techniques for Hiding and Protection

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

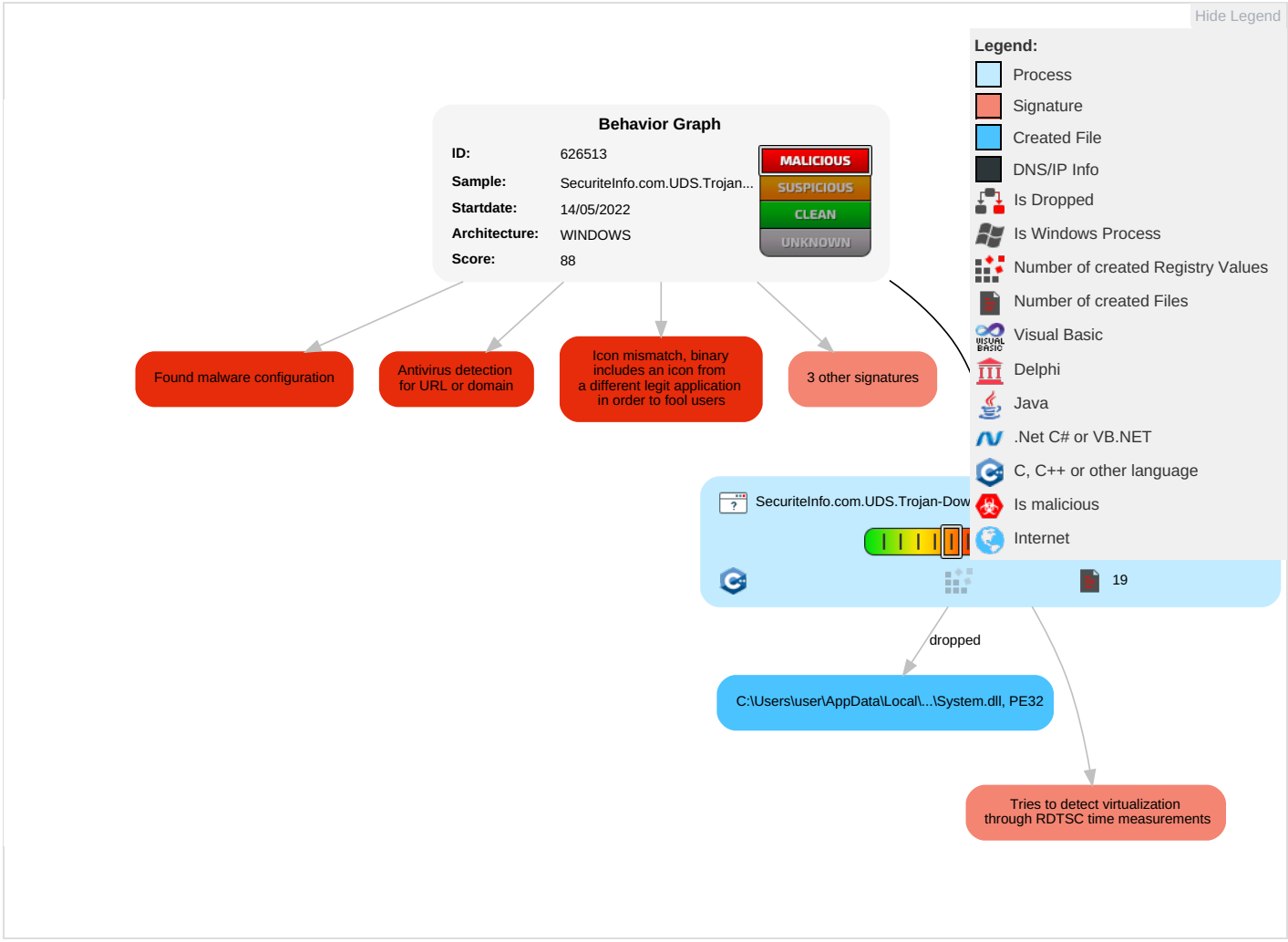
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	1 Access Token Manipulation	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Access Token Manipulation	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.17738.exe	7%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsj528F.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsj528F.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.mesince.com/ms.crl0	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://crl.mesince.com/ms.crl0	0%	Avira URL Cloud	safe	
http://aia.mesince.com/ms.cer0	0%	Virustotal		Browse
http://aia.mesince.com/ms.cer0	0%	Avira URL Cloud	safe	
http://ocsp.mesince.com0)	0%	Avira URL Cloud	safe	
http://aia.mesince.com/ms-tsa.cer02	0%	Avira URL Cloud	safe	
http://crl.mesince.com/ms-tsa.crl0F	0%	Avira URL Cloud	safe	
http://ocsp.mesince.com0-	0%	Avira URL Cloud	safe	
http://185.236.228.217/private/Spread.bin	100%	Avira URL Cloud	malware	
http://www.mesince.com/policy/0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.236.228.217/private/Spread.bin	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	false		high
http://crl.mesince.com/ms.crl0	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://aia.mesince.com/ms.cer0	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://ocsp.mesince.com0)	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	false	• Avira URL Cloud: safe	low
http://aia.mesince.com/ms-tsa.cer02	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	false	• Avira URL Cloud: safe	unknown
http://crl.mesince.com/ms-tsa.crl0F	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	false	• Avira URL Cloud: safe	unknown
http://ocsp.mesince.com0-	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	false	• Avira URL Cloud: safe	low
http://www.mesince.com/policy/0	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626513
Start date and time: 14/05/202206:29:06	2022-05-14 06:29:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.8895 (renamed file extension from 8895 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:	29

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:	mal88.troj.evad.winEXE@1/2@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.8% (good quality ratio 61.6%) • Quality average: 88.9% • Quality standard deviation: 21.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, backgroundTaskHost.exe, audiodg.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, go.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

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\fusionstilladelsen.non

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	data
Category:	modified
Size (bytes):	133962
Entropy (8bit):	4.059734244679519
Encrypted:	false
SSDEEP:	1536:MW4WxxOB6uKuOf6kud5XgijP24kMF45nabdqZ/Ajmq+JMp:MW4WxxOB6uK3fnOK9MF45naJqZ4Kq+6p
MD5:	2BEC7F2714A969960C94CACE0059FBE3
SHA1:	174CA98CAF1712DA6C15388558ED877AEDE01DA0
SHA-256:	428033E459073FC4B0F2949945CBBA5C2C15BF4216AD5D39E42755BBA1A1AA0A
SHA-512:	E39D22586BA990876943DBDEB75976C51616EAD1F281A2492E60D411281E0451766A8BDAF2E15BA4DE06E54919C650E9196885F3A47A677128FFA274225E1E7E
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Temp\nsj528F.tmp\System.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.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: 0%, 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..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	5.641019034220834
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.17738.exe
File size:	307224
MD5:	6f790a9e28d73d498c89a19cfe941d1b
SHA1:	1ec63e32364359f656b29eb37e3a2af11ecc62a8
SHA256:	2241716c3ddff7b1f771a6e3c91b67ded01e9f78026ecc124863099dbe5ac405
SHA512:	d4e27129849dab65c30061a44c699bb62212acae4512df173f45607d7407fcb8dfc9afcf0fe3fe28b72fc9f2a615b9554f67c4482827454931780ff43ffb50ec
SSDEEP:	6144:OYa6VBAkzL7r9r/EDpppppppppppppppppppppppppppppp0Y2OVKmXZszK15P7Ld:OYnDP7r9r/+pppppppppppppppppppz
TLSH:	F46405C5E98455A1EC19AB306A36CD3592237EFDA874A41D29DE3E273FFB2D35026013

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:	c4c4c4c8ccd4d0c4

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="kldes RDKLKENS Flutenes2 ", O=LANDBRUGSREGNSKAB, L=Saint-Jean-des-Essartiers, S=Normandie, 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	• 5/13/2022 5:07:29 PM 5/13/2023 5:07:29 PM
Subject Chain	• CN="kldes RDKLKENS Flutenes2 ", O=LANDBRUGSREGNSKAB, L=Saint-Jean-des-Essartiers, S=Normandie, C=FR
Version:	3
Thumbprint MD5:	4EC87CDF2DF0AFCC2B070E5661FE0646
Thumbprint SHA-1:	8B231E760D9179231C08845B226C6806EF514F03
Thumbprint SHA-256:	400DCEECD1D42BCF4E70517635DD2DE0E5468B6E0513C3100B7CF61E63A2A981
Serial:	D869F5D5F1A19BDA

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]

Instruction
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 00007FE38CEB8D4Ah
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 00007FE38CEB8D1Ah
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	0x4b000	0x35b28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x496f0	0x1928	
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	

Name	Virtual Address	Virtual Size	Is in Section
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	0x20000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x4b000	0x35b28	0x35c00	False	0.2130859375	data	4.46068570463	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x4b5e0	0x368	data	English	United States
RT_ICON	0x4b948	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	0x5c170	0x94a8	data	English	United States
RT_ICON	0x65618	0x67e8	data	English	United States
RT_ICON	0x6be00	0x5488	data	English	United States
RT_ICON	0x71288	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	0x754b0	0x35e0	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x78a90	0x25a8	data	English	United States
RT_ICON	0x7b038	0x10a8	data	English	United States
RT_ICON	0x7c0e0	0xea8	data	English	United States
RT_ICON	0x7cf88	0x988	data	English	United States
RT_ICON	0x7d910	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	0x7e1b8	0x6c8	data	English	United States
RT_ICON	0x7e880	0x668	data	English	United States
RT_ICON	0x7eee8	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x7f450	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x7f8b8	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	0x7fba0	0x1e8	data	English	United States
RT_ICON	0x7fd88	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x7feb0	0xb8	data	English	United States
RT_DIALOG	0x7ff68	0x144	data	English	United States
RT_DIALOG	0x800b0	0x13c	data	English	United States
RT_DIALOG	0x801f0	0x100	data	English	United States
RT_DIALOG	0x802f0	0x11c	data	English	United States
RT_DIALOG	0x80410	0x60	data	English	United States
RT_GROUP_ICON	0x80470	0x102	data	English	United States
RT_VERSION	0x80578	0x26c	data	English	United States
RT_MANIFEST	0x807e8	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import

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	2015-2020 Adobe. All rights reserved.
FileVersion	5.3.5
CompanyName	Adobe Inc.
LegalTrademarks	
Comments	
ProductName	Adobe PDF
FileDescription	Adobe PDF
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe PID: **6516**, Parent PID: **2368**

General

Target ID:	0
Start time:	06:30:12
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe"
Imagebase:	0x400000
File size:	307224 bytes
MD5 hash:	6F790A9E28D73D498C89A19CFE941D1B
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: 00000000.00000002.784638235.0000000003221000.00000040.00001000.00020000.00000000.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\nst5193.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\nst5194.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\nsj528F.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\nsj528F.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405BE2	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsj528F.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\nsj528F.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	8	406184	CreateFileW
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\fusionstilladelsen.non	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nst5193.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsj528F.tmp	success or wait	1	405DA3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	32768	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	406224	WriteFile
C:\Users\user\AppData\Local\Temp\nsj528F.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 Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	106812	25803	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	406224	WriteFile
C:\Users\user\AppData\Local\Temp\fusionstilladelsen.non	0	16384	fd fd		success or wait	9	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.17738.exe	unknown	512	success or wait	501	4061F5	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	unknown	16384	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nst5194.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nst5194.tmp	unknown	10206	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nst5194.tmp	unknown	4	success or wait	2	4061F5	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	unknown	16384	success or wait	2	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\fusionstilladelsen.non	unknown	1048576	success or wait	1	6FD62C59	ReadFile

Disassembly

No disassembly