ID: 343212
Sample Name:
IRS_Covid_19_Relief_Grant_Document_docx.exe
Cookbook: default.jbs
Time: 15:31:46
Date: 22/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

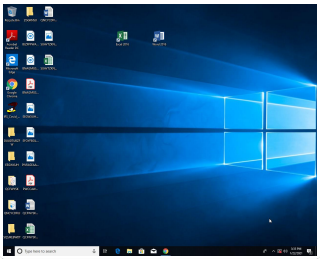
Analysis Report IRS_Covid_19_Relief_Grant_Document…

Overview

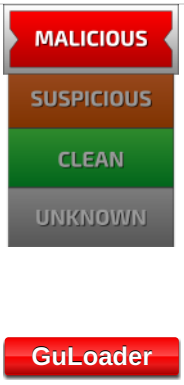
General Information

Sample Name:	IRS_Covid_19_Relief_Grant_Document_docx.exe
Analysis ID:	343212
MD5:	5f85963ecc2a1c3..
SHA1:	a97cc41833fae62..
SHA256:	b76b24380c31d4..

Most interesting Screenshot:



Detection

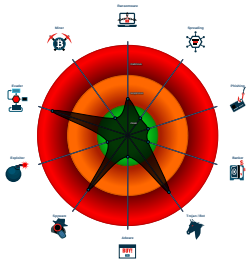


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Yara detected Generic Dropper
- Yara detected GuLoader
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Executable has a suspicious name (…
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…

Classification



Startup

- **System is w10x64**
- IRS_Covid_19_Relief_Grant_Document_docx.exe (PID: 4952 cmdline: 'C:\Users\user\Desktop\IRS_Covid_19_Relief_Grant_Document_docx.exe' MD5: 5F85963ECC2A1C3354C2E705F3E8D038)
  - IRS_Covid_19_Relief_Grant_Document_docx.exe (PID: 2220 cmdline: 'C:\Users\user\Desktop\IRS_Covid_19_Relief_Grant_Document_docx.exe' MD5: 5F85963ECC2A1C3354C2E705F3E8D038)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

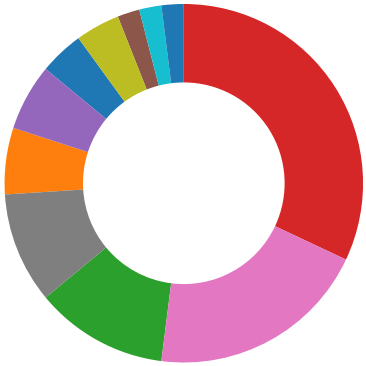
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: IRS_Covid_19_Relief_Grant_Document_docx.exe PID: 4952	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: IRS_Covid_19_Relief_Grant_Document_docx.exe PID: 4952	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: IRS_Covid_19_Relief_Grant_Document_docx.exe PID: 2220	JoeSecurity_GenericDropper	Yara detected Generic Dropper	Joe Security	
Process Memory Space: IRS_Covid_19_Relief_Grant_Document_docx.exe PID: 2220	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: IRS_Covid_19_Relief_Grant_Document_docx.exe PID: 2220	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

Uses secure TLS version for HTTPS connections

Binary contains paths to debug symbols

System Summary:

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

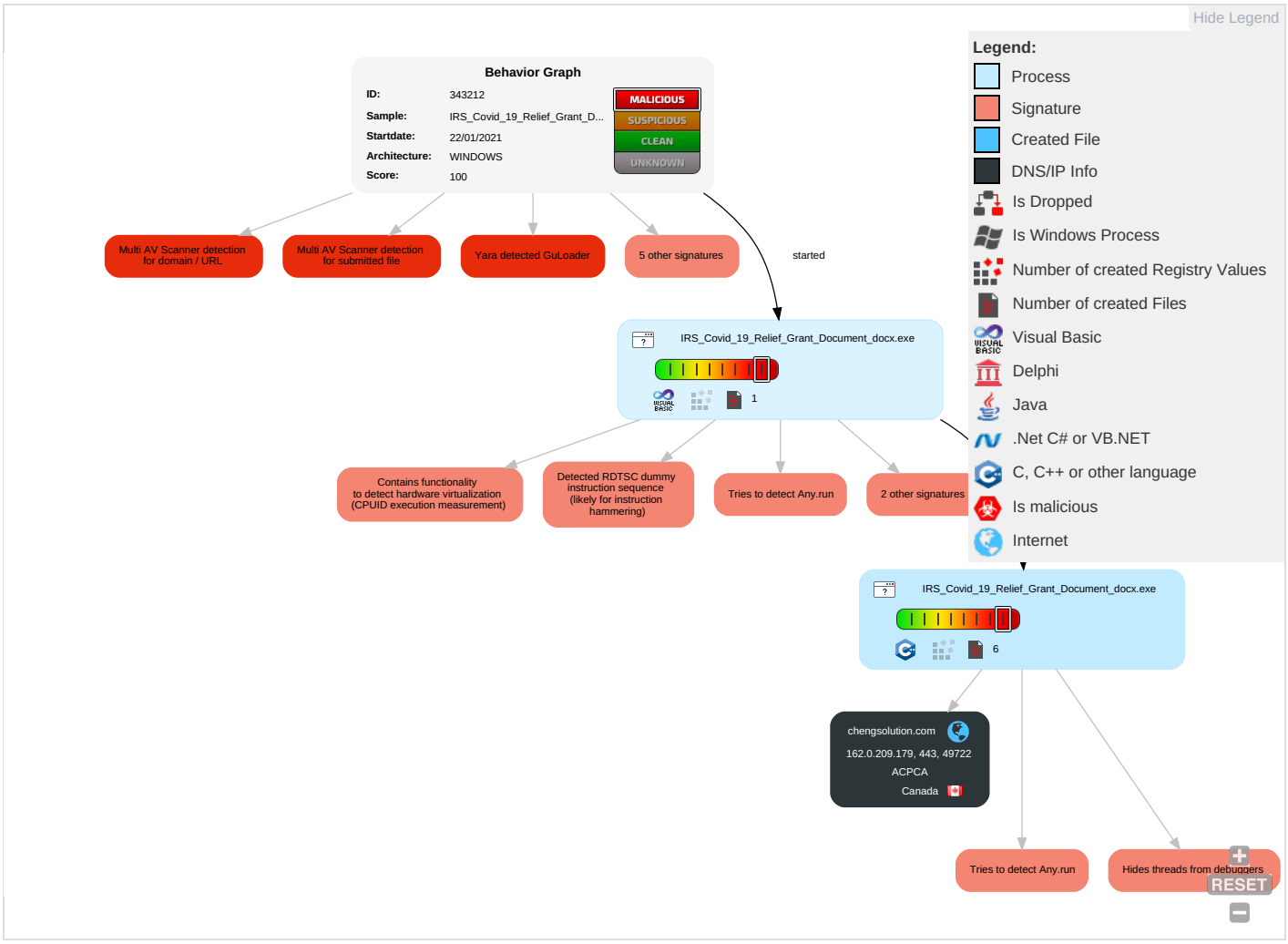
Stealing of Sensitive Information:

Yara detected Generic Dropper

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 2	Virtualization/Sandbox Evasion 2 1	OS Credential Dumping	Security Software Discovery 6 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 3 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

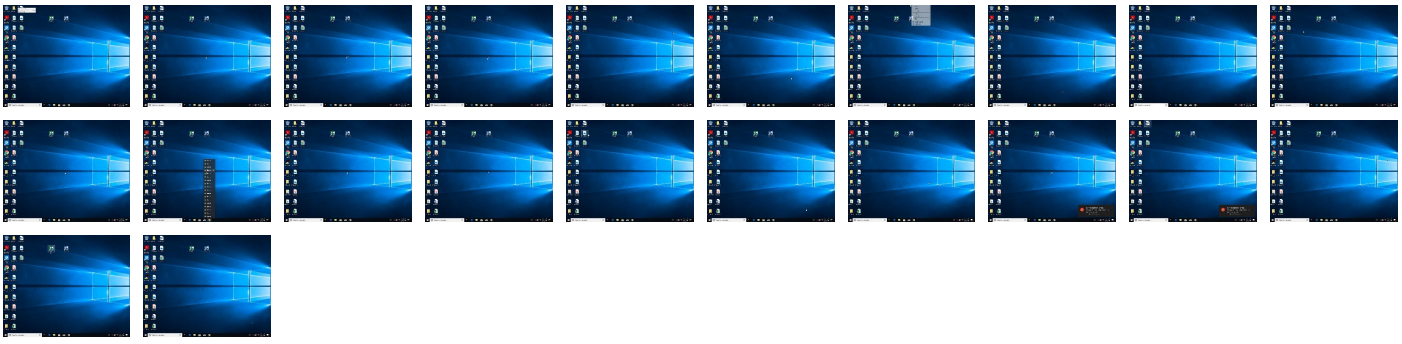
Behavior Graph



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
IRS_Covid_19_Relief_Grant_Document_docx.exe	29%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
chengsolution.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://chengsolution.com/vr/xdark_mkDaCZ89.bin	12%	Virustotal		Browse
http://https://chengsolution.com/vr/xdark_mkDaCZ89.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
chengsolution.com	162.0.209.179	true	false	• 4%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://chengsolution.com/vr/xdark_mkDaCZ89.bin	IRS_Covid_19_Relief_Grant_Document_docx.exe, 00000001.00000002.614207915.0000000000562000.00000040.00000001.sdmp	true	• 12%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.0.209.179	unknown	Canada		35893	ACPCA	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	343212
Start date:	22.01.2021
Start time:	15:31:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 11s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	IRS_Covid_19_Relief_Grant_Document_docx.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:	31
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:	mal100.troj.spyw.evad.winEXE@3/0@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 47.6% (good quality ratio 41.1%) • Quality average: 69.4% • Quality standard deviation: 33.8%
HCA Information:	• Successful, ratio: 52% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 13.88.21.125, 23.210.248.85, 51.11.168.160, 92.122.213.247, 92.122.213.194, 20.54.26.129, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.0.209.179	IRS_Covid-19_Relief_Payment_Notice_pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
chengsolution.com	IRS_Covid-19_Relief_Payment_Notice_pdf.exe	Get hash	malicious	Browse	• 162.0.209.179

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ACPCA	invoice 2021.xlsx	Get hash	malicious	Browse	• 162.0.215.9
	1ELOG8UQ4M.htm	Get hash	malicious	Browse	• 162.0.209.171
	1ELOG8UQ4M.htm	Get hash	malicious	Browse	• 162.0.209.171
	FM0DWXGE27.htm	Get hash	malicious	Browse	• 162.0.209.171
	Purchase Order and Contract Agreement Namtip THAI CO.doc	Get hash	malicious	Browse	• 162.0.209.181
	IRS_Covid-19_Relief_Payment_Notice_pdf.exe	Get hash	malicious	Browse	• 162.0.209.179
	LRGjZ3F0AO.exe	Get hash	malicious	Browse	• 162.0.219.122
	Busan Korea.exe	Get hash	malicious	Browse	• 162.0.213.60
	mssecsvc.exe	Get hash	malicious	Browse	• 162.36.93.137
	SCAN_20210115140930669.exe	Get hash	malicious	Browse	• 162.0.213.203
	Order (2021.01.06).exe	Get hash	malicious	Browse	• 162.0.213.203
	http://https://vodafone-bill-failed.com	Get hash	malicious	Browse	• 162.0.215.120
	UF14VE7MF3.htm	Get hash	malicious	Browse	• 162.0.209.142
	http://https://verify-requests.com/HSBC/	Get hash	malicious	Browse	• 162.0.209.141
	46M2B7IIGN.htm	Get hash	malicious	Browse	• 162.0.209.142
	http://recp.mkt91.net/ctt?m=804040&r=Njg0NjYxMDU1NQS2&b=0&j=NjAwMDczOTg3S0&k=NCLogo&kx=1&kt=12&kd=https://ahlhealth.com/Wednesday5029kl%23mark.tryniski@cbna.com	Get hash	malicious	Browse	• 162.0.209.130
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fin0038847990.sn.am%2fIfCk7ZE6GWq&c=E,1,XbwqZlmKwFAf_trFhDdV9wkuU6vutPEIQqN4IhE8jUbxLD3wnPPXDvKp8Jibjk9HngPAI5iRQWnG4vU_DQMKfMGkzgCqkZ-4BfRprMNSl9Nr7VoPQEtWNft5&typo=1	Get hash	malicious	Browse	• 162.0.209.25
	http://https://joom.ag/qJFC	Get hash	malicious	Browse	• 162.0.209.115
	http://https://faxdocuments.sn.am/la0TEIiIlWq	Get hash	malicious	Browse	• 162.0.209.144
	http://https://securedoc.sn.am/lZnSrsZICGq	Get hash	malicious	Browse	• 162.0.209.144

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Vivaldi.3.5.2115.87.x64.exe	Get hash	malicious	Browse	• 162.0.209.179
	8776139.docm	Get hash	malicious	Browse	• 162.0.209.179
	TeamViewer 14.exe	Get hash	malicious	Browse	• 162.0.209.179
	Jan_Order.html	Get hash	malicious	Browse	• 162.0.209.179
	open_office_2877604939.exe	Get hash	malicious	Browse	• 162.0.209.179
	SecuriteInfo.com.Trojan.Packed.196.27884.exe	Get hash	malicious	Browse	• 162.0.209.179
	6213805.docm	Get hash	malicious	Browse	• 162.0.209.179
	7653684.docm	Get hash	malicious	Browse	• 162.0.209.179
	1403181.docm	Get hash	malicious	Browse	• 162.0.209.179
	1ELOG8UQ4M.htm	Get hash	malicious	Browse	• 162.0.209.179
	2736760.docm	Get hash	malicious	Browse	• 162.0.209.179
	Notification_20443258.xls	Get hash	malicious	Browse	• 162.0.209.179
	Success_paym_info_7275986.docm	Get hash	malicious	Browse	• 162.0.209.179
	notif712.xls	Get hash	malicious	Browse	• 162.0.209.179
	Report-preview01.20.exe	Get hash	malicious	Browse	• 162.0.209.179
	notice.1459.xls	Get hash	malicious	Browse	• 162.0.209.179
	dep_det_3444608.docm	Get hash	malicious	Browse	• 162.0.209.179
	TMIJM.cpl	Get hash	malicious	Browse	• 162.0.209.179
	FM0DWXGE27.htm	Get hash	malicious	Browse	• 162.0.209.179

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.331258589216556
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	IRS_Covid_19_Relief_Grant_Document_docx.exe
File size:	86016
MD5:	5f85963ecc2a1c3354c2e705f3e8d038
SHA1:	a97cc41833fae623ff219c2dada84733329c8963
SHA256:	b76b24380c31d4be4dfc1d584d5799e1897277828ff523969f123a86f49a37db
SHA512:	edb310c7d1ecc3ecce9b45cc708e1b2b4a7175303da2d07cb9fc05736d7db7eb07191524c33a9b91d3a718cac4c791b254b4cc7db360ef2e5604a994f0a172e7
SSDEEP:	768:ejblNZiR6t0Dzlx+nffkyy16LojlL7MpVOqJpSSdGoL3KimHp:6blrWBBIfkyS6aLKOAB6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L....b.`..... ...0.....0....@.....

File Icon

Icon Hash:	a0b0cc7270daec00

Static PE Info

General

Entrypoint:	0x401498
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x6009621A [Thu Jan 21 11:14:34 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

General

Import Hash:	98834e8b1c22ed6d1484c39b625780c4

Entrypoint Preview

Instruction
push 00401AE0h
call 00007F01FC95CAE3h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
dec eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [edi+1E7C834Bh], bl
mov al, C9h
dec esp
cmpsd
into
cli
xchg eax, edx
aad E6h
mov dh, dh
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
dec eax
popad
insd
popad
insb
jne 00007F01FC95CB66h
imul ebp, dword ptr [esi+61h], 6E6F6974h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
or dword ptr [esi-7AA2F237h], esp
adc bh, byte ptr [ebp+ecx*2-6Eh]
clc
and dword ptr [esi-49DC1494h], ebx
mov dword ptr [esi-56C8461Dh], esi
out dx, al
inc ebp
mov ah, DAh
mov gs, word ptr [edi]
js 00007F01FC95CAB5h
sbb al, 26h
cmp cl, byte ptr [edi-53h]
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah

Instruction
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
in eax, dx
add al, 00h
add byte ptr [ebx+eax+00h], bl
add byte ptr [eax], al
or eax, 74616400h
jc 00007F01FC95CB5Ch
outsb
jc 00007F01FC95CB62h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x12584	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x15000	0x60c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x128	.text
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	0x11a8c	0x12000	False	0.391913519965	data	5.80205252886	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x13000	0x11c0	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x15000	0x60c	0x1000	False	0.15576171875	data	1.49893521938	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x15324	0x2e8	data		
RT_GROUP_ICON	0x15310	0x14	data		
RT_VERSION	0x150f0	0x220	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryVar, __vbaAryDestruct, __vbaLateMemSt, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, _CIsin, __vbaErase, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaObjVar, _adj_fpatan, __vbaLateIdCallLd, __vbaRedim, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaErrorOverflow, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaDerefAry1, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarDup, __vbaVarCopy, __vbaLateMemCallLd, _CIatan, __vbaStrMove, __vbaAryCopy, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	lutrin
FileVersion	2.00
CompanyName	ViralCherry
ProductName	ViralCherry
ProductVersion	2.00
OriginalFilename	lutrin.exe

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 76

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 15:33:00.659708977 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:00.852823019 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:00.853913069 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:00.909730911 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.103221893 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.103290081 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.103328943 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.103367090 CET	443	49722	162.0.209.179	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 15:33:01.103394985 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.103427887 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.104790926 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.106894970 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.211014032 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.404757977 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.404932976 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.419486046 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.618079901 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.618141890 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.618179083 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.618217945 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.618222952 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.618247986 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.618252039 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.618254900 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.618264914 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.618292093 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.618298054 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.618330002 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.618331909 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.618367910 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.618371010 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.618407011 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.618446112 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.618489027 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.618489981 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.618529081 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.811444044 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.811507940 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.811541080 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.811633110 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.811674118 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.811712027 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.811747074 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.811752081 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.811774015 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.811777115 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.811778069 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.811789989 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.811815023 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.811826944 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.811846018 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.811867952 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.811886072 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.811907053 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.811919928 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.811954021 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.811956882 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.811995983 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.812009096 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.812035084 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:01.812061071 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:01.812355995 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:02.005701065 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.005737066 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.005759001 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.005783081 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.005806923 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.005831003 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.005853891 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.005883932 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.005883932 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:02.005908966 CET	443	49722	162.0.209.179	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 15:33:02.005925894 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:02.005930901 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:02.005934000 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.005950928 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:02.005959034 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.005973101 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:02.005983114 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.006006002 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.006017923 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:02.006026030 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:02.006030083 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.006041050 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:02.006053925 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.006067038 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:02.006083012 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.006102085 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:02.006108046 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.006114960 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:02.006133080 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.006138086 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:02.006155968 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.006176949 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:02.006180048 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.006191969 CET	49722	443	192.168.2.3	162.0.209.179
Jan 22, 2021 15:33:02.006206036 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.006226063 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.006246090 CET	443	49722	162.0.209.179	192.168.2.3
Jan 22, 2021 15:33:02.006267071 CET	443	49722	162.0.209.179	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 15:32:34.237971067 CET	65110	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:32:34.286247015 CET	53	65110	8.8.8.8	192.168.2.3
Jan 22, 2021 15:32:35.173605919 CET	58361	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:32:35.221765041 CET	53	58361	8.8.8.8	192.168.2.3
Jan 22, 2021 15:32:36.174494982 CET	63492	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:32:36.233561039 CET	53	63492	8.8.8.8	192.168.2.3
Jan 22, 2021 15:32:37.617847919 CET	60831	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:32:37.668592930 CET	53	60831	8.8.8.8	192.168.2.3
Jan 22, 2021 15:32:38.644068003 CET	60100	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:32:38.694984913 CET	53	60100	8.8.8.8	192.168.2.3
Jan 22, 2021 15:32:39.598009109 CET	53195	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:32:39.646202087 CET	53	53195	8.8.8.8	192.168.2.3
Jan 22, 2021 15:32:40.696042061 CET	50141	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:32:40.747057915 CET	53	50141	8.8.8.8	192.168.2.3
Jan 22, 2021 15:32:41.642864943 CET	53023	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:32:41.692101002 CET	53	53023	8.8.8.8	192.168.2.3
Jan 22, 2021 15:32:43.216372967 CET	49563	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:32:43.265650034 CET	53	49563	8.8.8.8	192.168.2.3
Jan 22, 2021 15:32:44.330440044 CET	51352	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:32:44.378456116 CET	53	51352	8.8.8.8	192.168.2.3
Jan 22, 2021 15:32:45.258740902 CET	59349	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:32:45.315373898 CET	53	59349	8.8.8.8	192.168.2.3
Jan 22, 2021 15:32:46.413996935 CET	57084	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:32:46.462196112 CET	53	57084	8.8.8.8	192.168.2.3
Jan 22, 2021 15:33:00.584187984 CET	58823	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:33:00.645143986 CET	53	58823	8.8.8.8	192.168.2.3
Jan 22, 2021 15:33:04.220772982 CET	57568	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:33:04.278572083 CET	53	57568	8.8.8.8	192.168.2.3
Jan 22, 2021 15:33:05.489191055 CET	50540	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:33:05.539989948 CET	53	50540	8.8.8.8	192.168.2.3
Jan 22, 2021 15:33:12.129739046 CET	54366	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:33:12.189742088 CET	53	54366	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 15:33:25.372404099 CET	53034	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:33:25.442540884 CET	53	53034	8.8.8.8	192.168.2.3
Jan 22, 2021 15:33:41.798993111 CET	57762	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:33:41.846873045 CET	53	57762	8.8.8.8	192.168.2.3
Jan 22, 2021 15:33:45.806488037 CET	55435	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:33:45.873781919 CET	53	55435	8.8.8.8	192.168.2.3
Jan 22, 2021 15:34:17.203610897 CET	50713	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:34:17.254595995 CET	53	50713	8.8.8.8	192.168.2.3
Jan 22, 2021 15:34:18.724848986 CET	56132	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:34:18.784081936 CET	53	56132	8.8.8.8	192.168.2.3
Jan 22, 2021 15:35:25.828926086 CET	58987	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:35:25.885335922 CET	53	58987	8.8.8.8	192.168.2.3
Jan 22, 2021 15:35:26.591089964 CET	56579	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:35:26.639123917 CET	53	56579	8.8.8.8	192.168.2.3
Jan 22, 2021 15:35:27.381139994 CET	60633	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:35:27.428925991 CET	53	60633	8.8.8.8	192.168.2.3
Jan 22, 2021 15:35:28.028019905 CET	61292	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:35:28.086383104 CET	53	61292	8.8.8.8	192.168.2.3
Jan 22, 2021 15:35:28.656333923 CET	63619	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:35:28.712656021 CET	53	63619	8.8.8.8	192.168.2.3
Jan 22, 2021 15:35:29.404434919 CET	64938	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:35:29.460849047 CET	53	64938	8.8.8.8	192.168.2.3
Jan 22, 2021 15:35:30.186583996 CET	61946	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:35:30.245747089 CET	53	61946	8.8.8.8	192.168.2.3
Jan 22, 2021 15:35:31.344348907 CET	64910	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:35:31.401043892 CET	53	64910	8.8.8.8	192.168.2.3
Jan 22, 2021 15:35:32.696083069 CET	52123	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:35:32.746825933 CET	53	52123	8.8.8.8	192.168.2.3
Jan 22, 2021 15:35:33.200326920 CET	56130	53	192.168.2.3	8.8.8.8
Jan 22, 2021 15:35:33.251012087 CET	53	56130	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 22, 2021 15:33:00.584187984 CET	192.168.2.3	8.8.8.8	0x4807	Standard query (0)	chengsolution.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 22, 2021 15:33:00.645143986 CET	8.8.8.8	192.168.2.3	0x4807	No error (0)	chengsolution.com		162.0.209.179	A (IP address)	IN (0x0001)

HTTPS Packets

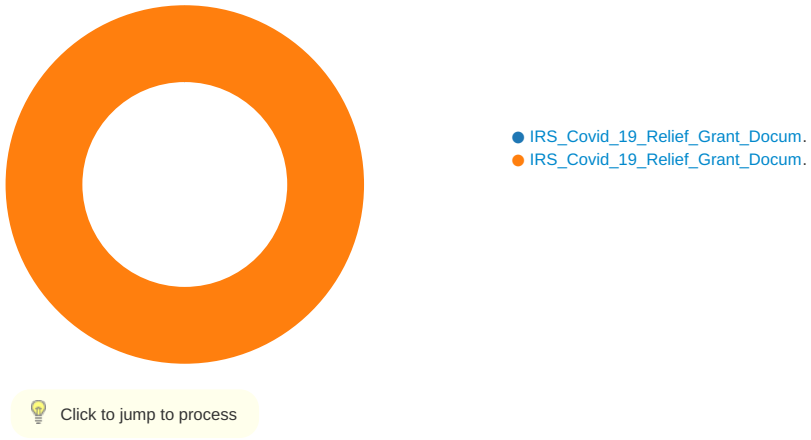
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 22, 2021 15:33:01.104790926 CET	162.0.209.179	443	192.168.2.3	49722	CN=chengsolution.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Jan 09 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jan 04 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: IRS_Covid_19_Relief_Grant_Document_docx.exe PID: 4952 Parent PID: 5652

General

Start time:	15:32:38
Start date:	22/01/2021
Path:	C:\Users\user\Desktop\IRS_Covid_19_Relief_Grant_Document_docx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\IRS_Covid_19_Relief_Grant_Document_docx.exe'
Imagebase:	0x400000
File size:	86016 bytes
MD5 hash:	5F85963ECC2A1C3354C2E705F3E8D038
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: IRS_Covid_19_Relief_Grant_Document_docx.exe PID: 2220 Parent PID: 4952

General

Start time:	15:32:52
Start date:	22/01/2021
Path:	C:\Users\user\Desktop\IRS_Covid_19_Relief_Grant_Document_docx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\IRS_Covid_19_Relief_Grant_Document_docx.exe'
Imagebase:	0x400000
File size:	86016 bytes
MD5 hash:	5F85963ECC2A1C3354C2E705F3E8D038
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564880	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564880	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564880	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564880	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564880	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564880	InternetOpenUrlA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4182A7	NtReadFile

Disassembly

Code Analysis