ID: 341752
Sample Name: IRS_Covid-19_Relief_Payment_Notice_pdf.exe
Cookbook: default.jbs
Time: 19:04:07
Date: 19/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

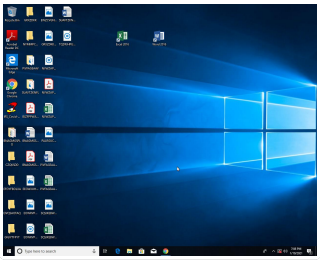
Analysis Report IRS_Covid-19_Relief_Payment_Notice_...

Overview

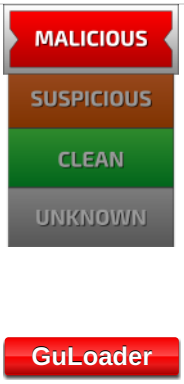
General Information

Sample Name:	IRS_Covid-19_Relief_Payment_Notice_pdf.exe
Analysis ID:	341752
MD5:	5525bb8a978d3a..
SHA1:	dcb9549ff9c290e..
SHA256:	21f49ea6e105c22.
Tags:	COVID19 exe GuLoader IRS

Most interesting Screenshot:



Detection



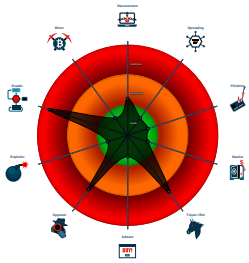
GuLoader

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Generic Dropper
- Yara detected GuLoader
- Contains functionality to detect hard...
- Contains functionality to hide a threa...
- 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...
- Yara detected VB6 Downloader Gen...
- Checks if the current process is bein...
- Contains functionality for execution ...

Classification



Startup

- **System is w10x64**
- IRS_Covid-19_Relief_Payment_Notice_pdf.exe (PID: 6124 cmdline: 'C:\Users\user\Desktop\IRS_Covid-19_Relief_Payment_Notice_pdf.exe' MD5: 5525BB8A978D3AC15812C8D8CA9B8A57)
  - IRS_Covid-19_Relief_Payment_Notice_pdf.exe (PID: 5348 cmdline: 'C:\Users\user\Desktop\IRS_Covid-19_Relief_Payment_Notice_pdf.exe' MD5: 5525BB8A978D3AC15812C8D8CA9B8A57)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

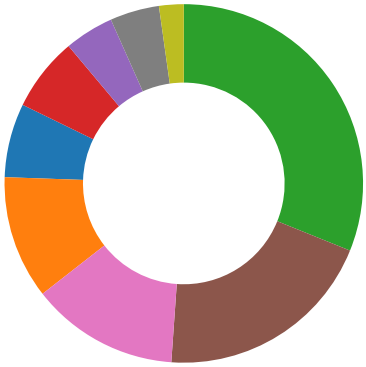
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: IRS_Covid-19_Relief_Payment_Notice_pdf.exe PID: 5348	JoeSecurity_GenericDropper	Yara detected Generic Dropper	Joe Security	
Process Memory Space: IRS_Covid-19_Relief_Payment_Notice_pdf.exe PID: 5348	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: IRS_Covid-19_Relief_Payment_Notice_pdf.exe PID: 5348	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: IRS_Covid-19_Relief_Payment_Notice_pdf.exe PID: 6124	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: IRS_Covid-19_Relief_Payment_Notice_pdf.exe PID: 6124	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- 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
- Stealing of Sensitive Information

Click to jump to signature section

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:

Contains functionality to hide a thread from the debugger

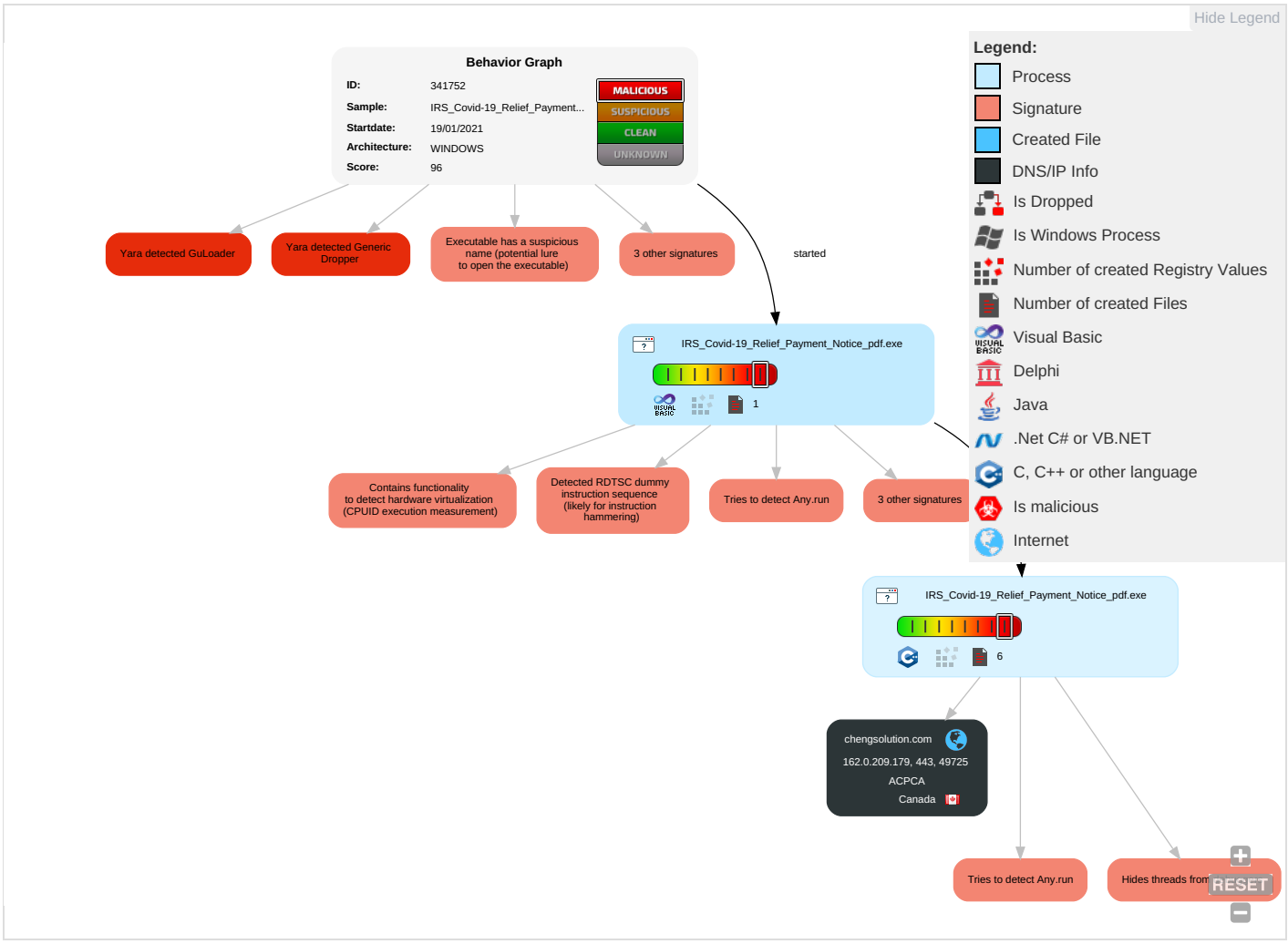
Hides threads from debuggers

Stealing of Sensitive Information:

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	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop o Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Security Software Discovery 7 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Application Window 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	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point

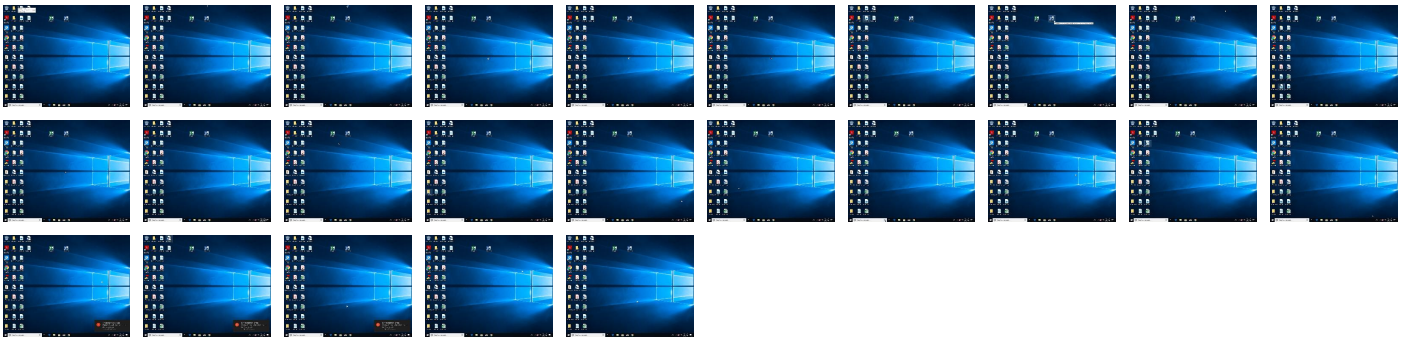
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://chengsolution.com/vr/tembin_AbNFdk131.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		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://chengsolution.com/vr/tembin_AbNFdk131.bin	IRS_Covid-19_Relief_Payment_Notice_pdf.exe	false	• 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:	341752
Start date:	19.01.2021
Start time:	19:04:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IRS_Covid-19_Relief_Payment_Notice_pdf.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:	33
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:	mal96.troj.spyw.evad.winEXE@3/0@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 27.1% (good quality ratio 21.4%) • Quality average: 62.4% • Quality standard deviation: 37.7%
HCA Information:	• Successful, ratio: 60% • 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, UsoClient.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.43.193.48, 52.255.188.83, 2.18.68.82, 51.11.168.160, 2.20.142.210, 2.20.142.209, 92.122.213.194, 92.122.213.247, 20.54.26.129, 52.254.96.93, 52.251.11.100 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, bn2eap.displaycatalog.md.mp.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/341752/sample/IRS_Covid-19_Relief_Payment_Notice_pdf.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ACPCA	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%2flfCk7ZE6GWq&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
	http://https://faxdocument.sn.am/lZgQs0mCCuq	Get hash	malicious	Browse	• 162.0.209.115
	http://https://rmnboxvoices.website/	Get hash	malicious	Browse	• 162.0.209.142
	http://https://bodyfexeen.ga/000/index.php	Get hash	malicious	Browse	• 162.0.209.25
	vnaSKDMnLG.dll	Get hash	malicious	Browse	• 162.0.213.230
	Yarranton.co.uk.htm	Get hash	malicious	Browse	• 162.0.209.27
	MIT-MULTA5600415258.msi	Get hash	malicious	Browse	• 162.0.209.72

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Qt_1186.xls	Get hash	malicious	Browse	• 162.0.209.179
	INV-4215.xls	Get hash	malicious	Browse	• 162.0.209.179
	wp-cryn.dll	Get hash	malicious	Browse	• 162.0.209.179
	P8ob8zaRpi.exe	Get hash	malicious	Browse	• 162.0.209.179
	Jcantele.HTM	Get hash	malicious	Browse	• 162.0.209.179
	Payment Confirmation Paper - Customer Copy_pdf.exe	Get hash	malicious	Browse	• 162.0.209.179
	1_cr.exe	Get hash	malicious	Browse	• 162.0.209.179
	Symptomaticshon5.exe	Get hash	malicious	Browse	• 162.0.209.179
	1_cr.exe	Get hash	malicious	Browse	• 162.0.209.179
	PO-00172020.html	Get hash	malicious	Browse	• 162.0.209.179
	atikmdag-patcher 1.4.7.exe	Get hash	malicious	Browse	• 162.0.209.179
	Dboom.HTM	Get hash	malicious	Browse	• 162.0.209.179
	vS8yVO8py0.exe	Get hash	malicious	Browse	• 162.0.209.179
	DOCUMENT FILE.exe	Get hash	malicious	Browse	• 162.0.209.179
	6VEoBuy32f.xls	Get hash	malicious	Browse	• 162.0.209.179
	Uh7eQhnS1m.doc	Get hash	malicious	Browse	• 162.0.209.179
	6fAjRmbM4P.exe	Get hash	malicious	Browse	• 162.0.209.179
	5IpRu2zSfu.dll	Get hash	malicious	Browse	• 162.0.209.179

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	zuwmbstItB.dll	Get hash	malicious	Browse	• 162.0.209.179
	HPScanner_1889752021_Signed_jpg.exe	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):	5.442072374572181
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_Payment_Notice_pdf.exe
File size:	86016
MD5:	5525bb8a978d3ac15812c8d8ca9b8a57
SHA1:	dcb9549ff9c290e056f83639ad546b03206a0806
SHA256:	21f49ea6e105c22882a9fb0065803deee18eddb76767a3(ddade2e2725eb65d9
SHA512:	0e5504ee2fc22ce87c1cac663e0c4cd76227025da20c29 03d63ddafc0fc8a270d56a90b89c31d8ee448a61f881ace 27037beb623f4409b9d1020a6b2a0a9f35b
SSDEEP:	768:bwSsRk+UMfhoeoCm0TI4Y4az55+mGMZkNS8+E MaybN1hBuKYR6mTLktPV9lIBtyd:JzTMoCnbO5+mG4i etbzhBuKYT3yVQm
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....#...B...B ...B..L^...B...`...B...d...B..Rich.B.....PE..L...5..`..... ....0.....0....@.....

File Icon

Icon Hash:	c0c4c26270faec04

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:	0x6006B035 [Tue Jan 19 10:11:01 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0

General

File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	98834e8b1c22ed6d1484c39b625780c4

Entrypoint Preview

Instruction
push 00401AD0h
call 00007FCBD493E363h
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 [edx], cl
inc ecx
hlt
or cl, 00000019h
fimul word ptr [ecx-53h]
out dx, eax
adc dword ptr [edi-2Fh], 0Dh
mov al, byte ptr [000000DBh]
add byte ptr [eax], al
add byte ptr [ecx], 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+61h], ch
outsb
insb
imul ebp, dword ptr [esi+67h], 6E616C70h
jc 00007FCBD493E3E1h
add byte ptr [eax], ch
js 00007FCBD493E3AAh
sub dword ptr [edx+00h], ebx
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
or dword ptr [edx+3ADED508h], esp
or ecx, dword ptr [edx-6Ch]
pop ds
pop ds
xchg eax, ecx
les ebp, fword ptr [esi]
retf
xor al, 10h
inc esi
cmp dword ptr [ebx+69h], edi
mov eax, dword ptr [AD989B4Ch]
cmp cl, byte ptr [ecx]
test eax, 4F3AF830h
lodsd
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
fiadd word ptr [eax+eax]
add byte ptr [eax+03h], dl
add byte ptr [eax], al
add byte ptr [edi], al
add byte ptr [esi+69h], al
arpl word ptr [ebp+73h], si
jnc 00007FCBD493E373h
or eax, 00000801h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x129b4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x15000	0x614	.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	0x11ebc	0x12000	False	0.396335177951	data	5.91456759437	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	0x614	0x1000	False	0.159423828125	data	1.53535569768	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1532c	0x2e8	data		
RT_GROUP_ICON	0x15318	0x14	data		
RT_VERSION	0x150f0	0x228	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

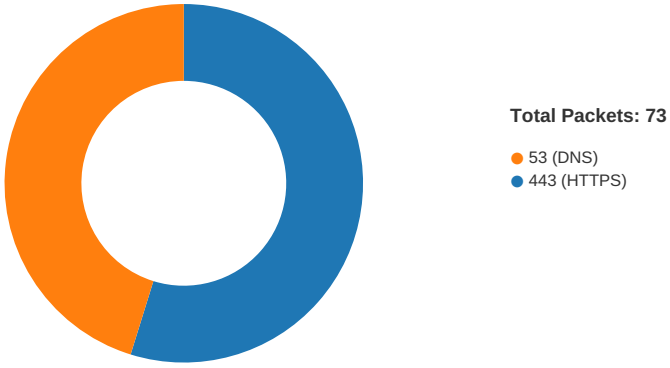
Description	Data
Translation	0x0409 0x04b0
InternalName	auricular
FileVersion	2.00
CompanyName	ViralCherry
ProductName	ViralCherry
ProductVersion	2.00
OriginalFilename	auricular.exe

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 19:05:35.671945095 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:35.867238998 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:35.867331982 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:35.897017956 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.090732098 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.090768099 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.090789080 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.090804100 CET	443	49725	162.0.209.179	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 19:05:36.090816975 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.090857029 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.090892076 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.096060991 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.096149921 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.224873066 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.421293020 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.421397924 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.454593897 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.653346062 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.653410912 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.653438091 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.653461933 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.653487921 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.653507948 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.653512001 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.653536081 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.653548002 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.653572083 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.653573990 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.653599024 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.653600931 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.653635979 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.653666973 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.653703928 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.654711962 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.846869946 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.846916914 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.846936941 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.846961975 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.846986055 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.847009897 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.847035885 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.847062111 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.847079039 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.847088099 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.847115993 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.847141981 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.847167015 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.847166061 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.847188950 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.847193956 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.847224951 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:36.848038912 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.848081112 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:36.848133087 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:37.040530920 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.040569067 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.040591002 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.040607929 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.040622950 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.040638924 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.040637970 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:37.040656090 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.040667057 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:37.040672064 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:37.040673971 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.040693045 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.040707111 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:37.040712118 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.040729046 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:37.040730953 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.040749073 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.040759087 CET	49725	443	192.168.2.3	162.0.209.179

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 19:05:37.040766001 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.040782928 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.040787935 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:37.040801048 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.040817022 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.040819883 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:37.040833950 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.040838957 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:37.040868044 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:37.040965080 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.040982962 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.041003942 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:37.041033983 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:37.234117031 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.234184027 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.234226942 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.234272003 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.234301090 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:37.234313011 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.234343052 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:37.234357119 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.234380007 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:37.234401941 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:37.234400988 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.234445095 CET	49725	443	192.168.2.3	162.0.209.179
Jan 19, 2021 19:05:37.234452963 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.234503984 CET	443	49725	162.0.209.179	192.168.2.3
Jan 19, 2021 19:05:37.234546900 CET	443	49725	162.0.209.179	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 19:04:57.162681103 CET	58361	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:04:57.221368074 CET	53	58361	8.8.8.8	192.168.2.3
Jan 19, 2021 19:04:58.217526913 CET	63492	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:04:58.268284082 CET	53	63492	8.8.8.8	192.168.2.3
Jan 19, 2021 19:04:59.531814098 CET	60831	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:04:59.582775116 CET	53	60831	8.8.8.8	192.168.2.3
Jan 19, 2021 19:05:00.658184052 CET	60100	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:05:00.709003925 CET	53	60100	8.8.8.8	192.168.2.3
Jan 19, 2021 19:05:05.854151011 CET	53195	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:05:05.902390957 CET	53	53195	8.8.8.8	192.168.2.3
Jan 19, 2021 19:05:06.835242987 CET	50141	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:05:06.886193991 CET	53	50141	8.8.8.8	192.168.2.3
Jan 19, 2021 19:05:07.624830008 CET	53023	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:05:07.672684908 CET	53	53023	8.8.8.8	192.168.2.3
Jan 19, 2021 19:05:08.424705982 CET	49563	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:05:08.472641945 CET	53	49563	8.8.8.8	192.168.2.3
Jan 19, 2021 19:05:09.410857916 CET	51352	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:05:09.467432022 CET	53	51352	8.8.8.8	192.168.2.3
Jan 19, 2021 19:05:10.623665094 CET	59349	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:05:10.671462059 CET	53	59349	8.8.8.8	192.168.2.3
Jan 19, 2021 19:05:11.406970978 CET	57084	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:05:11.455020905 CET	53	57084	8.8.8.8	192.168.2.3
Jan 19, 2021 19:05:12.216387033 CET	58823	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:05:12.264552116 CET	53	58823	8.8.8.8	192.168.2.3
Jan 19, 2021 19:05:26.185189962 CET	57568	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:05:26.243479013 CET	53	57568	8.8.8.8	192.168.2.3
Jan 19, 2021 19:05:35.571042061 CET	50540	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:05:35.634639025 CET	53	50540	8.8.8.8	192.168.2.3
Jan 19, 2021 19:05:41.281246901 CET	54366	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:05:41.329204082 CET	53	54366	8.8.8.8	192.168.2.3
Jan 19, 2021 19:05:46.049727917 CET	53034	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:05:46.112493992 CET	53	53034	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 19:05:47.226560116 CET	57762	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:05:47.282752991 CET	53	57762	8.8.8.8	192.168.2.3
Jan 19, 2021 19:05:47.602919102 CET	55435	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:05:47.661106110 CET	53	55435	8.8.8.8	192.168.2.3
Jan 19, 2021 19:06:02.330107927 CET	50713	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:06:02.389588118 CET	53	50713	8.8.8.8	192.168.2.3
Jan 19, 2021 19:06:15.829989910 CET	56132	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:06:15.880850077 CET	53	56132	8.8.8.8	192.168.2.3
Jan 19, 2021 19:06:19.428741932 CET	58987	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:06:19.486742020 CET	53	58987	8.8.8.8	192.168.2.3
Jan 19, 2021 19:06:51.298798084 CET	56579	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:06:51.346765995 CET	53	56579	8.8.8.8	192.168.2.3
Jan 19, 2021 19:06:53.023474932 CET	60633	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:06:53.079869986 CET	53	60633	8.8.8.8	192.168.2.3
Jan 19, 2021 19:07:45.461467981 CET	61292	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:07:45.517836094 CET	53	61292	8.8.8.8	192.168.2.3
Jan 19, 2021 19:07:46.513546944 CET	63619	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:07:46.575645924 CET	53	63619	8.8.8.8	192.168.2.3
Jan 19, 2021 19:07:47.870642900 CET	64938	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:07:47.929498911 CET	53	64938	8.8.8.8	192.168.2.3
Jan 19, 2021 19:07:49.383142948 CET	61946	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:07:49.447613001 CET	53	61946	8.8.8.8	192.168.2.3
Jan 19, 2021 19:07:50.286160946 CET	64910	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:07:50.342813969 CET	53	64910	8.8.8.8	192.168.2.3
Jan 19, 2021 19:07:51.322047949 CET	52123	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:07:51.383259058 CET	53	52123	8.8.8.8	192.168.2.3
Jan 19, 2021 19:07:53.507177114 CET	56130	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:07:53.566209078 CET	53	56130	8.8.8.8	192.168.2.3
Jan 19, 2021 19:07:56.467189074 CET	56338	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:07:56.523395061 CET	53	56338	8.8.8.8	192.168.2.3
Jan 19, 2021 19:07:58.288005114 CET	59420	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:07:58.349138975 CET	53	59420	8.8.8.8	192.168.2.3
Jan 19, 2021 19:07:59.514334917 CET	58784	53	192.168.2.3	8.8.8.8
Jan 19, 2021 19:07:59.562504053 CET	53	58784	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 19, 2021 19:05:35.571042061 CET	192.168.2.3	8.8.8.8	0xc302	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 19, 2021 19:05:35.634639025 CET	8.8.8.8	192.168.2.3	0xc302	No error (0)	chengsolution.com		162.0.209.179	A (IP address)	IN (0x0001)

HTTPS Packets

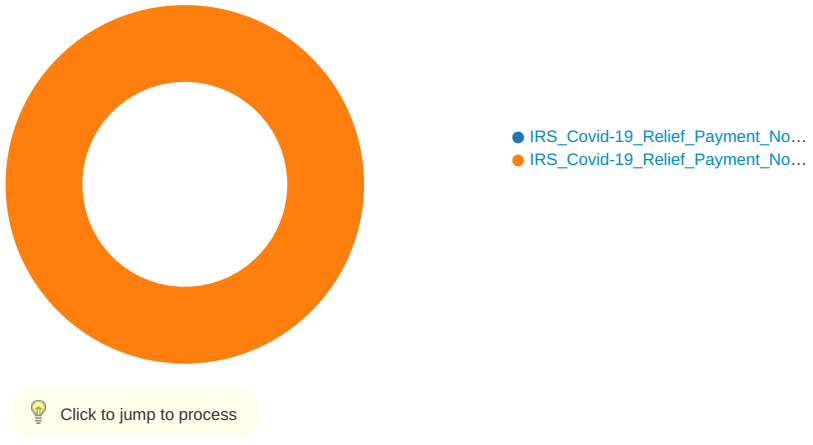
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 19, 2021 19:05:36.096060991 CET	162.0.209.179	443	192.168.2.3	49725	CN=chengsolution.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, 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_Payment_Notice_pdf.exe PID: 6124 Parent PID: 5596

General

Start time:	19:05:02
Start date:	19/01/2021
Path:	C:\Users\user\Desktop\IRS_Covid-19_Relief_Payment_Notice_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\IRS_Covid-19_Relief_Payment_Notice_pdf.exe'
Imagebase:	0x400000
File size:	86016 bytes
MD5 hash:	5525BB8A978D3AC15812C8D8CA9B8A57
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_Payment_Notice_pdf.exe PID: 5348 Parent PID: 6124

General

Start time:	19:05:25
Start date:	19/01/2021
Path:	C:\Users\user\Desktop\IRS_Covid-19_Relief_Payment_Notice_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\IRS_Covid-19_Relief_Payment_Notice_pdf.exe'
Imagebase:	0x7ff7ca4e0000
File size:	86016 bytes
MD5 hash:	5525BB8A978D3AC15812C8D8CA9B8A57
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	564CDA	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	564CDA	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	564CDA	InternetOpenUrlA

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	564CDA	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	564CDA	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	564CDA	InternetOpenUrlA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E67	NtReadFile

Disassembly

Code Analysis