ID: 344014
Sample Name: IRS_Covid-19_Relief_Payment_Notice_pdf.exe
Cookbook: default.jbs
Time: 21:11:27
Date: 25/01/2021
Version: 31.0.0 Emerald

Table of Contents

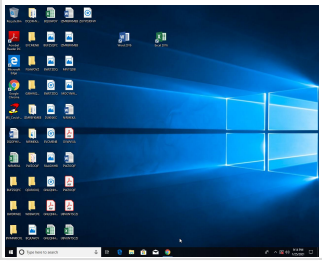
Analysis Report IRS_Covid-19_Relief_Payment_Notice_...

Overview

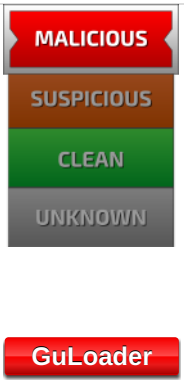
General Information

Sample Name:	IRS_Covid-19_Relief_Payment_Notice_pdf.exe
Analysis ID:	344014
MD5:	5525bb8a978d3a..
SHA1:	dcb9549ff9c290e..
SHA256:	21f49ea6e105c22.

Most interesting Screenshot:



Detection



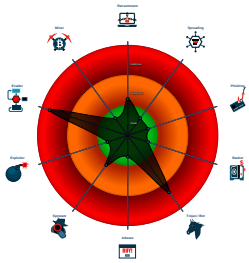
GuLoader

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

Signatures

- Multi AV Scanner detection for doma...
- Multi AV Scanner detection for subm...
- 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...

Classification



Startup

- **System is w10x64**
- IRS_Covid-19_Relief_Payment_Notice_pdf.exe (PID: 7120 cmdline: 'C:\Users\user\Desktop\IRS_Covid-19_Relief_Payment_Notice_pdf.exe' MD5: 5525BB8A978D3AC15812C8D8CA9B8A57)
  - IRS_Covid-19_Relief_Payment_Notice_pdf.exe (PID: 4168 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

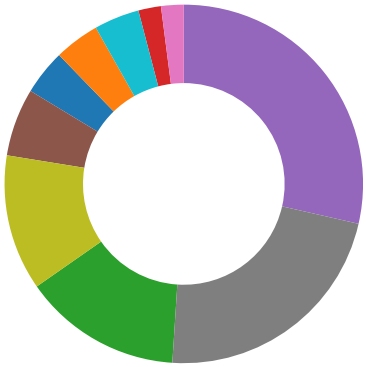
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: IRS_Covid-19_Relief_Payment_Notice_pdf.exe PID: 7120	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: IRS_Covid-19_Relief_Payment_Notice_pdf.exe PID: 7120	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: IRS_Covid-19_Relief_Payment_Notice_pdf.exe PID: 4168	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: IRS_Covid-19_Relief_Payment_Notice_pdf.exe PID: 4168	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion

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

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:

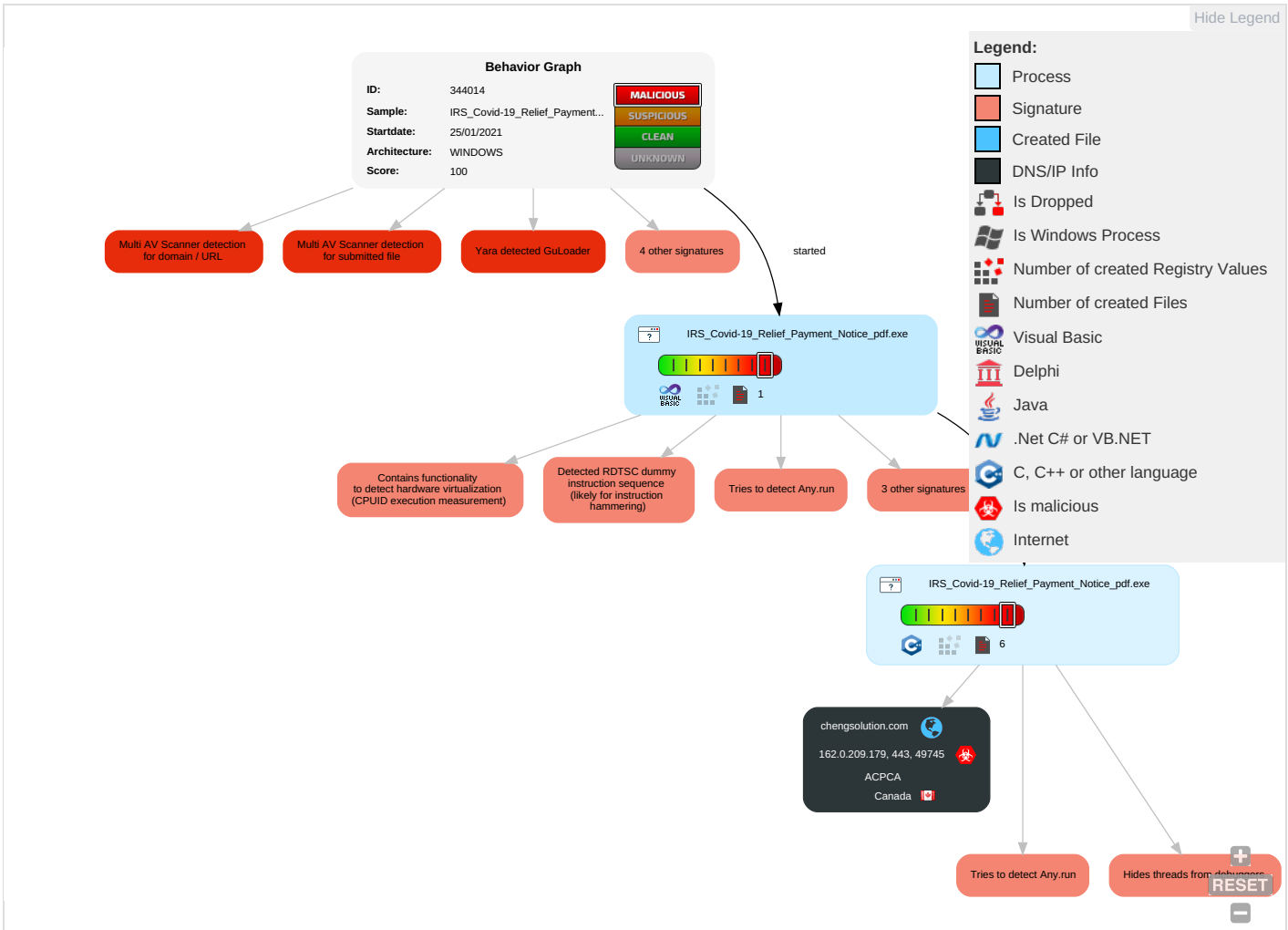
Contains functionality to hide a thread from the debugger

Hides threads from debuggers

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 2	Input Capture 1	Security Software Discovery 7 2 1	Remote Services	Input Capture 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 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 t Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	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)	Binary Padding	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	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

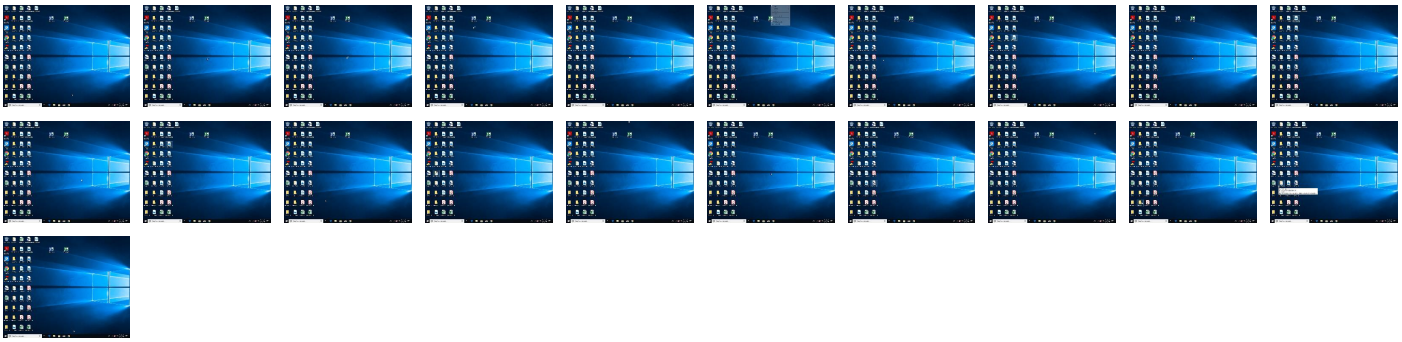
Behavior Graph



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_Payment_Notice_pdf.exe	68%	Virustotal		Browse
IRS_Covid-19_Relief_Payment_Notice_pdf.exe	41%	Metadefender		Browse
IRS_Covid-19_Relief_Payment_Notice_pdf.exe	75%	ReversingLabs	Win32.Spyware.Noon	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
chengsolution.com	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://chengsolution.com/vr/tembin_AbNFdk131.bin	11%	Virustotal		Browse
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	true	• 8%, Virustotal, Browse	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	true	• 11%, 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	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344014
Start date:	25.01.2021
Start time:	21:11:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 6s
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:	16
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.evad.winEXE@3/0@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 6.7% (good quality ratio 4.1%) • Quality average: 29.6% • Quality standard deviation: 28.9%
HCA Information:	• Successful, ratio: 77% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 51.11.168.160, 52.155.217.156, 20.54.26.129, 8.248.137.254, 8.241.11.126, 8.248.113.254, 8.241.121.254, 8.241.123.254, 95.101.22.134, 95.101.22.125 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.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

Time	Type	Description
21:12:38	API Interceptor	201x Sleep call for process: IRS_Covid-19_Relief_Payment_Notice_pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.0.209.179	IRS_Covid_19_Relief_Grant_Document_docx.exe	Get hash	malicious	Browse	
	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_Grant_Document_docx.exe	Get hash	malicious	Browse	• 162.0.209.179
	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	BENVAV31BU.html	Get hash	malicious	Browse	• 162.0.209.171
	IRS_Covid_19_Relief_Grant_Document_docx.exe	Get hash	malicious	Browse	• 162.0.209.179
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	PAYMENT INFO.xlsx	Get hash	malicious	Browse	• 162.0.209.179
	k.dll	Get hash	malicious	Browse	• 162.0.209.179
	DOCUMENTS_RECEIVED.html	Get hash	malicious	Browse	• 162.0.209.179
	case (348).xls	Get hash	malicious	Browse	• 162.0.209.179
	request_form_1611565093.xlsm	Get hash	malicious	Browse	• 162.0.209.179
	creoagent.dll	Get hash	malicious	Browse	• 162.0.209.179
	creoagent.dll	Get hash	malicious	Browse	• 162.0.209.179
	case (426).xls	Get hash	malicious	Browse	• 162.0.209.179
	case (250).xls	Get hash	malicious	Browse	• 162.0.209.179
	rvYr7FRwkG.dll	Get hash	malicious	Browse	• 162.0.209.179
	case (1447).xls	Get hash	malicious	Browse	• 162.0.209.179
	case (850).xls	Get hash	malicious	Browse	• 162.0.209.179
	SecuriteInfo.com.Heur.18472.xls	Get hash	malicious	Browse	• 162.0.209.179
	case (1543).xls	Get hash	malicious	Browse	• 162.0.209.179
	SecuriteInfo.com.FileRepMalware.dll	Get hash	malicious	Browse	• 162.0.209.179
	case_1581.xls	Get hash	malicious	Browse	• 162.0.209.179
	case (435).xls	Get hash	malicious	Browse	• 162.0.209.179
	case (426).xls	Get hash	malicious	Browse	• 162.0.209.179
	case (61).xls	Get hash	malicious	Browse	• 162.0.209.179
	BENVAV31BU.html	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

General

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 MaybN1hBuKYR6mTLktPV9llBtyd: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
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 00007F1084753633h
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

Instruction
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 00007F10847536B1h
add byte ptr [eax], ch
js 00007F108475367Ah
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
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
add byte ptr [eax], al
fiadd word ptr [eax+eax]
add byte ptr [eax+03h], dl

Instruction
add byte ptr [eax], al
add byte ptr [edi], al
add byte ptr [esi+69h], al
arpl word ptr [ebp+73h], si
jnc 00007F1084753643h
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

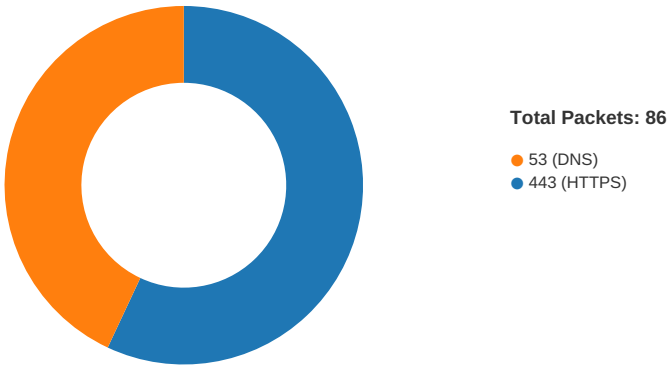
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/25/21-21:13:16.006774	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 21:12:37.163822889 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:37.370588064 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:37.370753050 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:37.387664080 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:37.593071938 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:37.593127012 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:37.593166113 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:37.593189001 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:37.593291998 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:37.593463898 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:37.593763113 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:37.593851089 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:37.723326921 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:37.929546118 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:37.929732084 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:37.952332973 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:38.161600113 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:38.161936045 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:38.165251017 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:38.409738064 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:38.502199888 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:38.502262115 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:38.502304077 CET	49745	443	192.168.2.4	162.0.209.179

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 21:12:38.502319098 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:38.502332926 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:38.502391100 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:38.502404928 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:38.502451897 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:38.502465010 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:38.502504110 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:38.502521038 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:38.502577066 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:38.504307032 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:38.504407883 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:38.612926006 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:38.817199945 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:38.823016882 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:38.823117971 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:38.825042963 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:39.069766045 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:39.154299974 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:39.154360056 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:39.154412031 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:39.154422998 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:39.154463053 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:39.154478073 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:39.154512882 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:39.154553890 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:39.154561996 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:39.154633999 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:39.155539989 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:39.155623913 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:39.268781900 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:39.475152016 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:39.480762005 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:39.480901003 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:39.481908083 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:39.732598066 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:39.818527937 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:39.818579912 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:39.818646908 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:39.818650961 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:39.818691969 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:39.818696976 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:39.818711996 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:39.818732977 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:39.818748951 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:39.818778038 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:39.818783045 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:39.818839073 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:39.820482969 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:39.820561886 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:39.926428080 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:40.133285999 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:40.137948036 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:40.138056040 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:40.138873100 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:40.387552977 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:40.459985018 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:40.460031986 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:40.460088015 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:40.460091114 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:40.460123062 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:40.460131884 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:40.460172892 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:40.460191965 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:40.460202932 CET	49745	443	192.168.2.4	162.0.209.179

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 21:12:40.460243940 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:40.460272074 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:40.460319042 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:40.463000059 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:40.463140011 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:40.566030979 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:40.771478891 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:40.776566982 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:40.776731014 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:40.777399063 CET	49745	443	192.168.2.4	162.0.209.179
Jan 25, 2021 21:12:41.022336006 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:41.100502968 CET	443	49745	162.0.209.179	192.168.2.4
Jan 25, 2021 21:12:41.100568056 CET	443	49745	162.0.209.179	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 21:12:10.024382114 CET	58028	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:10.072478056 CET	53	58028	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:11.098911047 CET	53097	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:11.146888971 CET	53	53097	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:12.063375950 CET	49257	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:12.114118099 CET	53	49257	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:13.107501030 CET	62389	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:13.158426046 CET	53	62389	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:14.189584970 CET	49910	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:14.237626076 CET	53	49910	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:15.161909103 CET	55854	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:15.209882021 CET	53	55854	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:16.141916990 CET	64549	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:16.198623896 CET	53	64549	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:17.105581045 CET	63153	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:17.153500080 CET	53	63153	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:18.105876923 CET	52991	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:18.153696060 CET	53	52991	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:19.030431032 CET	53700	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:19.078537941 CET	53	53700	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:19.965902090 CET	51726	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:20.014018059 CET	53	51726	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:20.888143063 CET	56794	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:20.936084986 CET	53	56794	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:21.827239990 CET	56534	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:21.875247002 CET	53	56534	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:22.802186966 CET	56627	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:22.853049040 CET	53	56627	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:23.793986082 CET	56621	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:23.853473902 CET	53	56621	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:24.748112917 CET	63116	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:24.796101093 CET	53	63116	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:25.718065977 CET	64078	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:25.768959999 CET	53	64078	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:37.072614908 CET	64801	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:37.137470961 CET	53	64801	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:40.884989023 CET	61721	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:40.933522940 CET	53	61721	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:56.844291925 CET	51255	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:56.914582968 CET	53	51255	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:57.455681086 CET	61522	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:57.514635086 CET	53	61522	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:58.124985933 CET	52337	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:58.172801971 CET	53	52337	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:58.316804886 CET	55046	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:58.373580933 CET	53	55046	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:58.848825932 CET	49612	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 21:12:58.911843061 CET	53	49612	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:59.508490086 CET	49285	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:59.557116032 CET	50601	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:12:59.567831039 CET	53	49285	8.8.8.8	192.168.2.4
Jan 25, 2021 21:12:59.608613968 CET	53	50601	8.8.8.8	192.168.2.4
Jan 25, 2021 21:13:00.114178896 CET	60875	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:13:00.179054976 CET	53	60875	8.8.8.8	192.168.2.4
Jan 25, 2021 21:13:00.746525049 CET	56448	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:13:00.802772999 CET	53	56448	8.8.8.8	192.168.2.4
Jan 25, 2021 21:13:02.268855095 CET	59172	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:13:02.330444098 CET	53	59172	8.8.8.8	192.168.2.4
Jan 25, 2021 21:13:03.524322033 CET	62420	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:13:03.580666065 CET	53	62420	8.8.8.8	192.168.2.4
Jan 25, 2021 21:13:04.710621119 CET	60579	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:13:04.767862082 CET	53	60579	8.8.8.8	192.168.2.4
Jan 25, 2021 21:13:15.000165939 CET	50183	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:13:15.210535049 CET	61531	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:13:15.958655119 CET	50183	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:13:16.004957914 CET	53	50183	8.8.8.8	192.168.2.4
Jan 25, 2021 21:13:16.006660938 CET	53	50183	8.8.8.8	192.168.2.4
Jan 25, 2021 21:13:16.031486034 CET	53	61531	8.8.8.8	192.168.2.4
Jan 25, 2021 21:13:19.540921926 CET	49228	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:13:19.602782965 CET	53	49228	8.8.8.8	192.168.2.4
Jan 25, 2021 21:13:50.004637957 CET	59794	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:13:50.052529097 CET	53	59794	8.8.8.8	192.168.2.4
Jan 25, 2021 21:13:51.203885078 CET	55916	53	192.168.2.4	8.8.8.8
Jan 25, 2021 21:13:51.260049105 CET	53	55916	8.8.8.8	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 25, 2021 21:13:16.006773949 CET	192.168.2.4	8.8.8.8	d022	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 25, 2021 21:12:37.072614908 CET	192.168.2.4	8.8.8.8	0x9d11	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 25, 2021 21:12:37.137470961 CET	8.8.8.8	192.168.2.4	0x9d11	No error (0)	chengsolution.com		162.0.209.179	A (IP address)	IN (0x0001)

HTTPS Packets

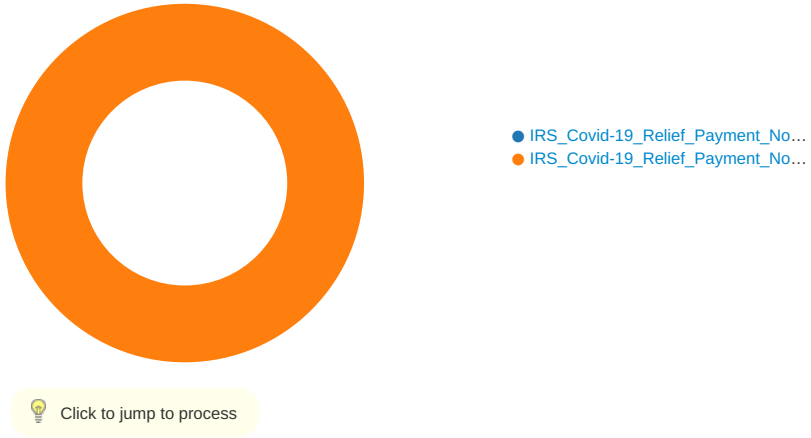
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 25, 2021 21:12:37.593763113 CET	162.0.209.179	443	192.168.2.4	49745	CN=chengsolution.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, 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: 7120 Parent PID: 6008

General

Start time:	21:12:14
Start date:	25/01/2021
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: 4168 Parent PID: 7120

General

Start time:	21:12:30
Start date:	25/01/2021
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:	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
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 Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis