ID: 337124
Cookbook: urldownload.jbs
Time: 19:40:46
Date: 07/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2

Analysis Report http://www.floridahealth.gov/_documents/newsroom/press-releases/2021/01/010421-COVID-19-main-page-vaccine-update.png 4

- Overview 4
  - General Information 4
  - Detection 4
  - Signatures 4
  - Classification 4
- Startup 4
- Malware Configuration 4
- Yara Overview 4
- Sigma Overview 4
- Signature Overview 4
- Mitre Att&ck Matrix 5
- Behavior Graph 5
- Screenshots 6
  - Thumbnails 6
- Antivirus, Machine Learning and Genetic Malware Detection 7
  - Initial Sample 7
  - Dropped Files 7
  - Unpacked PE Files 7
  - Domains 7
  - URLs 7
- Domains and IPs 8
  - Contacted Domains 8
  - Contacted URLs 8
  - URLs from Memory and Binaries 8
  - Contacted IPs 8
  - Public 8
- General Information 8
- Simulations 9
  - Behavior and APIs 9
- Joe Sandbox View / Context 10
  - IPs 10
  - Domains 10
  - ASN 10
  - JA3 Fingerprints 10
  - Dropped Files 10
- Created / dropped Files 10
- Static File Info 11
  - No static file info 11
- Network Behavior 11
  - Network Port Distribution 11
  - TCP Packets 11
  - UDP Packets 13
  - DNS Queries 14
  - DNS Answers 14
  - HTTP Request Dependency Graph 14
  - HTTP Packets 14
- Code Manipulations 15
- Statistics 15
  - Behavior 15
- System Behavior 16
  - Analysis Process: cmd.exe PID: 6596 Parent PID: 5112 16

General 16
File Activities 16
File Created 16
Analysis Process: conhost.exe PID: 6604 Parent PID: 6596 16
General 16
Analysis Process: wget.exe PID: 6636 Parent PID: 6596 16
General 16
File Activities 17
File Created 17
File Written 17
Disassembly 17
Code Analysis 17

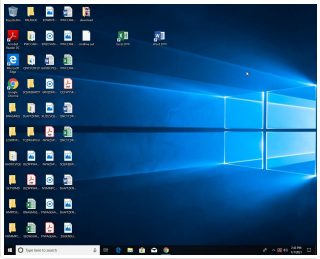
Analysis Report http://www.floridahealth.gov/_documen…

Overview

General Information

Sample URL:	http://www.floridahealth.gov/_documents/newsroom/press-releases/2021/01/010421-COVID-19-main-page-vaccine-update.png
Analysis ID:	337124

Most interesting Screenshot:



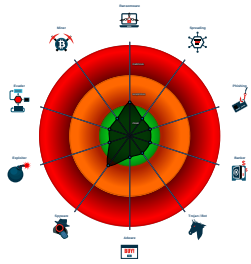
Detection

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

Signatures

Queries the volume information (nam…

Classification



Startup

- **System is w10x64**
- cmd.exe (PID: 6596 cmdline: C:\Windows\system32\cmd.exe /c wget -t 2 -v -T 60 -P 'C:\Users\user\Desktop\download' --no-check-certificate --content-disposition --user-agent='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko' 'http://www.floridahealth.gov/_documents/newsroom/press-releases/2021/01/010421-COVID-19-main-page-vaccine-update.png' > cmdline.out 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 6604 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - wget.exe (PID: 6636 cmdline: wget -t 2 -v -T 60 -P 'C:\Users\user\Desktop\download' --no-check-certificate --content-disposition --user-agent='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko' 'http://www.floridahealth.gov/_documents/newsroom/press-releases/2021/01/010421-COVID-19-main-page-vaccine-update.png' MD5: 3DADB6E2ECE9C4B3E1E322E617658B60)
- **cleanup**

Malware Configuration

No configs have been found

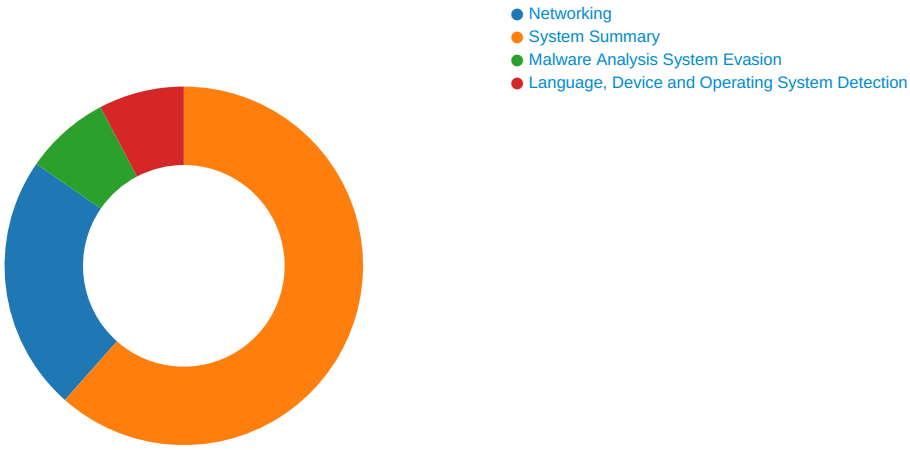
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



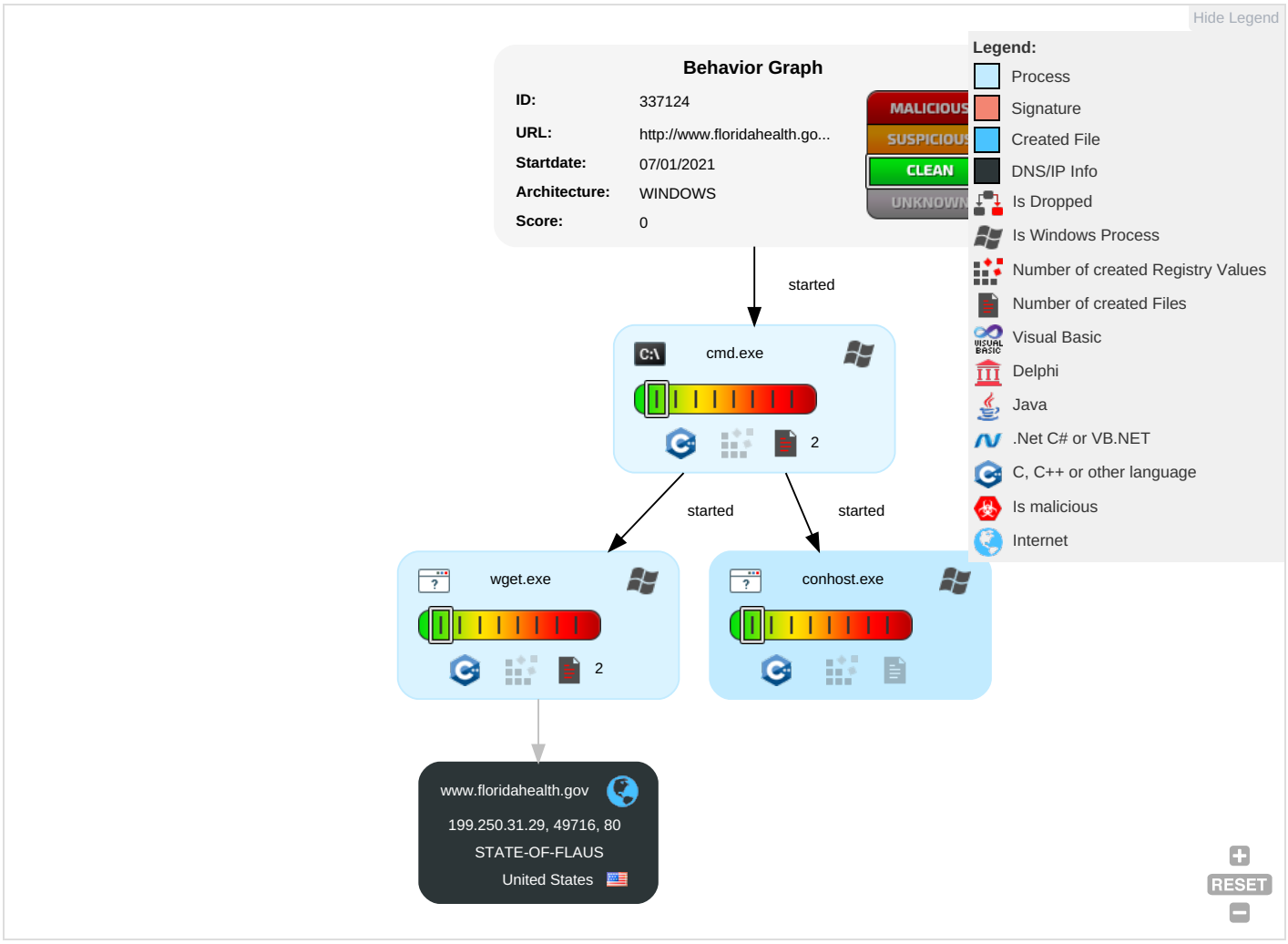
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Im
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	System Information Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Remote System Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da

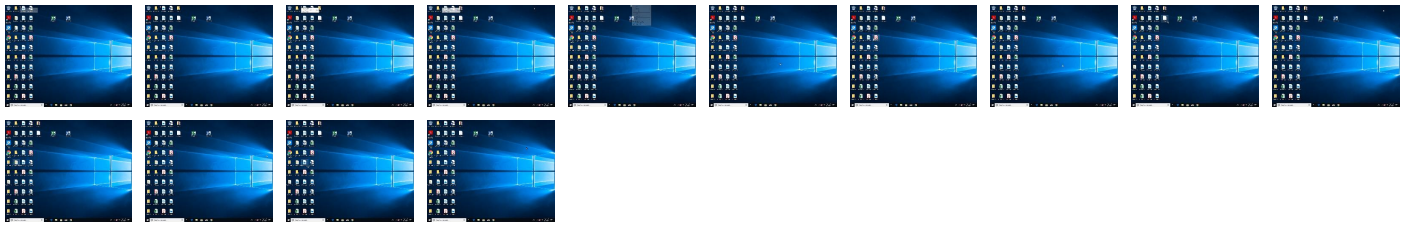
Behavior Graph



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
http://www.floridahealth.gov/_documents/newsroom/press-releases/2021/01/010421-COVID-19-main-page-vaccine-update.png	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.floridahealth.gov	199.250.31.29	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.floridahealth.gov/_documents/newsroom/press-releases/2021/01/010421-COVID-19-main-page-vaccine-update.png	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.floridahealth.gov/_documents/newsroom/press-releases/2021/01/010421-COVID-19-main-page-va	wget.exe, 00000002.00000002.260541552.0000000000BC0000.00000004.00000020.sdmp, cmdline.out.2.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.250.31.29	unknown	United States		8103	STATE-OF-FLAUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	337124
Start date:	07.01.2021
Start time:	19:40:46
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 4m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	urldownload.jbs
Sample URL:	http://www.floridahealth.gov/_documents/newsroom/press-releases/2021/01/010421-COVID-19-main-page-vaccine-update.png
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:	22
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:	CLEAN
Classification:	clean0.win@4/2@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 51.104.144.132, 23.210.248.85, 13.88.21.125, 92.122.213.247, 92.122.213.194, 104.43.193.48, 20.54.26.129, 2.20.142.209, 2.20.142.210, 51.103.5.186, 13.64.90.137, 51.11.168.160 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, skypedataprdcoleus15.cloudapp.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, client.wns.windows.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • VT rate limit hit for: http://www.floridahealth.gov/_documents/newsroom/press-releases/2021/01/010421-COVID-19-main-page-vaccine-update.png

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\Desktop\cmdline.out	
Process:	C:\Windows\SysWOW64\wget.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	11652
Entropy (8bit):	2.4659804002549706
Encrypted:	false
SSDEEP:	96:AEH8J4cx/lPKWmOPrkopg7o3MftvvXXjHw:TcWcNlPvP9g7o8ftvPXjQ
MD5:	C3188FFB72FF4DB0111356D46AFB6276
SHA1:	B6D07F1DEED6AE369D2BF9E8E7F463AAFA65D441
SHA-256:	3B25D61B1FD131A8AC93176C5089E5A4E0EC1F2D6E05BBA3368FD882472C5743
SHA-512:	FC7C13089B9F49285E07437D23CA17DADD59749BB2FBD2E5759E227FB0178CBAEC7AF6040E5BBA94D22A2D696FD7FC7C130C67102B1173414FDAE0A57CE680D
Malicious:	false
Reputation:	low
Preview:	--2021-01-07 19:41:37-- http://www.floridahealth.gov/_documents/newsroom/press-releases/2021/01/010421-COVID-19-main-page-vaccine-update.png..Resolving www.floridahealth.gov (www.floridahealth.gov)... 199.250.31.29..Connecting to www.floridahealth.gov (www.floridahealth.gov)|199.250.31.29|:80... connected...HTTP request sent, awaiting response... 200 OK..Length: 7231526 (6.9M) [image/png]..Saving to: 'C:/Users/user/Desktop/download/010421-COVID-19-main-page-vaccine-update.png'.... 0K .... 0% 315K 22s.. 50K .... 1% 327K 22s.. 100K .... 2% 2.79M 15s.. 150K .... 2% 324K 17s.. 200K .... 3% 322K 17s.. 250K .... 4% 320K 18s.. 300K ....

C:\Users\user\Desktop\download\010421-COVID-19-main-page-vaccine-update.png	
Process:	C:\Windows\SysWOW64\wget.exe
File Type:	PNG image data, 2500 x 1406, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	7231526
Entropy (8bit):	**7.99385770297276**
Encrypted:	**true**
SSDEEP:	196608:2odRUO/50SHCnVuc4RcQb1msbYRYOpkXsE61ZO00NC:7r/qSIb4HATeOpz18C
MD5:	EB291984053FE16E974E2EE38BC6F30F
SHA1:	C7A635D60E12F08AB0BC3D02FCF1D99729FD7AA3
SHA-256:	A8BD5004377B770F90B4530D0042A3A2099567288718D84D8AD3C8AD887FF4EC
SHA-512:	B8698FE86AD89934A3A2665AFFFC3D6C8911259BEA9873F6716EEC797DB31B0C08A40B85A46DF3989AA76FF67173179E59856062A731A7A203D760C6795C8845
Malicious:	false

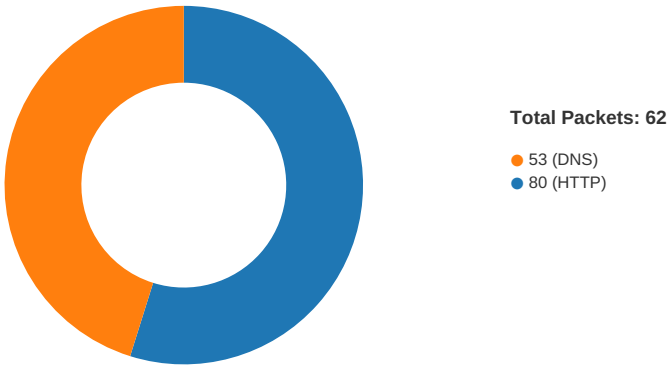
C:\Users\user\Desktop\download\010421-COVID-19-main-page-vaccine-update.png	
Reputation:	low
Preview:	.PNG.....IHDR.....~.....R..Z....IDATx^l.gs.K.....j.$... .B.Z.U(.P.Z..8..w.....8/;....2+3.UxxxxxE.....:v.>..3.....k...?.O~.....?O./~.....'Q..3:}..N.<..'N$.Z[[u..e].xQ.N.... .6...o._.*..l...^.....u.....]..Wu.....\.C{....G..?.!)..7p.=.+W...k.m..O....7o..[..B.h?w..G...x..&....#...%...`.....G?....?.S.._.._.....+.....<...../.....z.....3.E]..;.P.cy./..... .....w..m=x.@O.<Q[[....<G....|....._....9..>.:.9..G..Q..;h.>d..Mx.....{.....;w.$.xg.E..+.!.h.....G_Ph.N..&..^.E.r...D....4..+.M+4B+.8<.-...=0.?~...qQ.8\.....7.70i..Y..0Oi..... ...c.\...{...<....-..o.....e..=..\]]]...OJ{{{.....'.(...B...'.....0>.w..k.[..=SGG.^.|...^.....#]..ggg.z..F...mXO.>M.Rhky@....\.u.%...}O.T.=&.Z.....;h. o.tQ..{.iy.-p....+r./2..zzz...7...<..... ....x.\..<t...../^.H.#.....8...i....e...<..u.9::.b..r..L&.....I.@.y.L-_.[_=.....dE=x0.~.....m.....C{...}..<G~.illL....?.b.4.....G.....V.....x.....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 19:41:37.881246090 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.040030003 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.040200949 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.044315100 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.204691887 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.218875885 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.218924046 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.218960047 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.218993902 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.220006943 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.220047951 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.220068932 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.220350027 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.220400095 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.220417023 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.220442057 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.220479012 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.220499992 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.221086979 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.221126080 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.221162081 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.221163988 CET	80	49716	199.250.31.29	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 19:41:38.221221924 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.221290112 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.221731901 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.221798897 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.221869946 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.221992016 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.222040892 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.222048998 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.222083092 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.222121954 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.222141027 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.222161055 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.222199917 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.222215891 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.222883940 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.222924948 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.222954988 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.222965002 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.222996950 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.223021984 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.276576042 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.377497911 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.377562046 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.377609015 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.377645016 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.377813101 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.378353119 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.378395081 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.378405094 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.378432989 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.378460884 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.378614902 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.378678083 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.379244089 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.379282951 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.379329920 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.379347086 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.379373074 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.379410982 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.379434109 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.379448891 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.379487991 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.379508018 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.379523039 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.379584074 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.379852057 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.379890919 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.379939079 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.379954100 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.379981041 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.380017996 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.380037069 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.380055904 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.380094051 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.380111933 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.380131006 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.380188942 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.380570889 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.380610943 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.380657911 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.380673885 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.380701065 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.380760908 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.381020069 CET	80	49716	199.250.31.29	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 19:41:38.381061077 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.381099939 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.381118059 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.381136894 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.381196976 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.381272078 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.381314039 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.381350040 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.381370068 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.381441116 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.381506920 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.381509066 CET	49716	80	192.168.2.3	199.250.31.29
Jan 7, 2021 19:41:38.381550074 CET	80	49716	199.250.31.29	192.168.2.3
Jan 7, 2021 19:41:38.381586075 CET	80	49716	199.250.31.29	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 19:41:35.926644087 CET	63492	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:41:35.977524996 CET	53	63492	8.8.8.8	192.168.2.3
Jan 7, 2021 19:41:37.805464983 CET	60831	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:41:37.866866112 CET	53	60831	8.8.8.8	192.168.2.3
Jan 7, 2021 19:41:40.065128088 CET	60100	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:41:40.126593113 CET	53	60100	8.8.8.8	192.168.2.3
Jan 7, 2021 19:41:40.869623899 CET	53195	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:41:40.917330980 CET	53	53195	8.8.8.8	192.168.2.3
Jan 7, 2021 19:41:42.120404005 CET	50141	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:41:42.179692030 CET	53	50141	8.8.8.8	192.168.2.3
Jan 7, 2021 19:42:03.062124968 CET	53023	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:42:03.066608906 CET	49563	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:42:03.114187956 CET	53	49563	8.8.8.8	192.168.2.3
Jan 7, 2021 19:42:03.120074987 CET	53	53023	8.8.8.8	192.168.2.3
Jan 7, 2021 19:42:03.334567070 CET	51352	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:42:03.392709970 CET	53	51352	8.8.8.8	192.168.2.3
Jan 7, 2021 19:42:04.650490999 CET	59349	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:42:04.698414087 CET	53	59349	8.8.8.8	192.168.2.3
Jan 7, 2021 19:42:05.488507032 CET	57084	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:42:05.536725044 CET	53	57084	8.8.8.8	192.168.2.3
Jan 7, 2021 19:42:07.487225056 CET	58823	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:42:07.544760942 CET	53	58823	8.8.8.8	192.168.2.3
Jan 7, 2021 19:42:18.077493906 CET	57568	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:42:18.136221886 CET	53	57568	8.8.8.8	192.168.2.3
Jan 7, 2021 19:42:21.317991018 CET	50540	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:42:21.386866093 CET	53	50540	8.8.8.8	192.168.2.3
Jan 7, 2021 19:42:21.470585108 CET	54366	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:42:21.528199911 CET	53	54366	8.8.8.8	192.168.2.3
Jan 7, 2021 19:42:21.624723911 CET	53034	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:42:21.683057070 CET	53	53034	8.8.8.8	192.168.2.3
Jan 7, 2021 19:42:21.927383900 CET	57762	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:42:21.983834028 CET	53	57762	8.8.8.8	192.168.2.3
Jan 7, 2021 19:42:25.035299063 CET	55435	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:42:25.092992067 CET	53	55435	8.8.8.8	192.168.2.3
Jan 7, 2021 19:42:48.327457905 CET	50713	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:42:48.378437996 CET	53	50713	8.8.8.8	192.168.2.3
Jan 7, 2021 19:43:18.704225063 CET	56132	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:43:18.763413906 CET	53	56132	8.8.8.8	192.168.2.3
Jan 7, 2021 19:43:19.855571985 CET	58987	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:43:19.903388977 CET	53	58987	8.8.8.8	192.168.2.3
Jan 7, 2021 19:43:25.489734888 CET	56579	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:43:25.538353920 CET	53	56579	8.8.8.8	192.168.2.3
Jan 7, 2021 19:43:45.939918995 CET	60633	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:43:45.987740993 CET	53	60633	8.8.8.8	192.168.2.3
Jan 7, 2021 19:43:47.587908983 CET	61292	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:43:47.644289017 CET	53	61292	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 19:43:49.560034990 CET	63619	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:43:49.608005047 CET	53	63619	8.8.8.8	192.168.2.3
Jan 7, 2021 19:43:52.375869036 CET	64938	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:43:52.424043894 CET	53	64938	8.8.8.8	192.168.2.3
Jan 7, 2021 19:43:53.512101889 CET	61946	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:43:53.563786030 CET	53	61946	8.8.8.8	192.168.2.3
Jan 7, 2021 19:43:59.274230003 CET	64910	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:43:59.323167086 CET	53	64910	8.8.8.8	192.168.2.3
Jan 7, 2021 19:43:59.744782925 CET	52123	53	192.168.2.3	8.8.8.8
Jan 7, 2021 19:43:59.819566011 CET	53	52123	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 7, 2021 19:41:37.805464983 CET	192.168.2.3	8.8.8.8	0xa4bc	Standard query (0)	www.floridahealth.gov	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 7, 2021 19:41:37.866866112 CET	8.8.8.8	192.168.2.3	0xa4bc	No error (0)	www.floridahealth.gov		199.250.31.29	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.floridahealth.gov

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49716	199.250.31.29	80	C:\Windows\SysWOW64\wget.exe

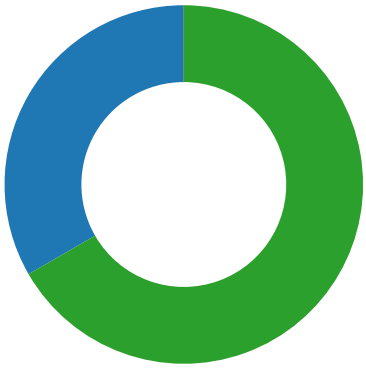
Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 19:41:38.044315100 CET	13	OUT	GET /_documents/newsroom/press-releases/2021/01/010421-COVID-19-main-page-vaccine-update.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko Accept: */* Accept-Encoding: identity Host: www.floridahealth.gov Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 19:41:38.218875885 CET	15	IN	HTTP/1.1 200 OK Content-Type: image/png Last-Modified: Thu, 07 Jan 2021 01:27:17 GMT Accept-Ranges: bytes ETag: "bb1daa3c94e4d61:0" Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Thu, 07 Jan 2021 18:41:37 GMT Content-Length: 7231526 Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 09 c4 00 00 05 7e 08 06 00 00 00 52 82 af 5a 00 00 80 00 49 44 41 54 78 5e 6c bd 67 73 1c 4b 92 a6 db ff e7 9a dd 1d 9b 9e 99 9e de ee 9e d6 f2 1c 6a 12 24 a8 b5 96 20 09 42 10 5a 03 55 28 ad 50 d0 5a 11 a0 38 e4 91 ad a6 77 ed fe ac f7 fa 93 38 2f 3b 97 b6 1f c2 32 2b 33 c2 55 78 78 78 78 78 45 fe e0 f8 f1 e3 3a 76 ec 98 3e fb ec 33 fd fe f7 bf d7 af 7f fd 6b fd f4 a7 3f d5 4f 7e f2 13 fd fc e7 3f 4f ca 2f 7e f1 8b e4 dd 9f fe f4 27 51 ff cc 99 33 3a 7d fa b4 4e 9e 3c a9 13 27 4e 24 cf 5a 5b 5b 75 f9 f2 65 5d bc 78 51 a7 4e 9d d2 e1 c3 87 93 36 bf f9 cd 6f f4 ab 5f fd 2a 81 03 6c f0 d0 86 02 5e e3 ff fc f3 cf 75 e8 d0 a1 e4 1e d8 97 2e 5d d2 d5 ab 57 75 e1 c2 85 04 0f f0 5c a8 43 7b e8 00 ef d1 a3 47 f5 87 3f fc 21 29 c0 e1 37 70 cf 9e 3d ab 2b 57 ae e8 da b5 6b 09 6d e7 cf 9f 4f ea 03 13 d8 37 6f de d4 ad 5b b7 92 42 1d 68 3f 77 ee dc 47 fe e0 c3 78 b8 07 26 b4 80 ff c8 91 23 c9 b5 a5 a5 25 81 07 1e 60 82 03 1a e1 f7 47 3f fa 91 fe f3 3f ff 53 ff f5 5f ff a5 5f fe f2 97 09 ff c8 04 19 c0 2b f4 f2 ec 7f fe cf ff a9 1f fe f0 87 fa f7 7f ff f7 a4 1e 3c 00 1b 9c c0 07 2f f8 a0 05 9e a0 13 f9 80 17 7a a9 07 cc df fe f6 b7 fa e3 1f ff 98 f0 cf 33 d3 45 5d f3 c5 3b ea 50 c0 63 79 c2 2f ef 8d cf bc 19 17 ed c1 8f 0e c0 83 fb 14 de b8 c2 0b f5 c1 77 fb f6 6d 3d 78 f0 40 4f 9e 3c 51 5b 5b 9b ee df bf 9f 3c 47 f6 d4 01 0f 7c 00 f7 c6 8d 1b 89 fc af 5f bf 9e d4 e1 39 b2 01 3e 05 3a 91 39 bc d0 47 14 da 51 80 c7 3b 68 87 3e 64 9f d6 4d 78 e5 1e b8 f4 f5 bd 7b f7 f4 e8 d1 a3 84 b6 3b 77 ee 24 cf 78 67 9d 45 86 e8 2b fc 21 17 68 05 07 b8 a8 03 0d d0 47 5f 50 68 03 4e 9e 9b 26 f4 0c 5e c0 45 e1 9e 72 f7 ee dd 44 2e e8 88 f5 cc 34 03 93 2b cf 4d 2b 34 42 2b 05 38 3c a3 2d f0 c1 c3 3d 30 1f 3f 7e 9c d4 e5 bd 71 51 07 38 5c 81 0d 1f e0 e2 37 ed 90 37 30 69 cf 15 59 f0 cc b2 30 4f 69 b9 81 e3 e1 c3 87 c9 d5 f8 0c cf 63 07 5c c8 0b 99 7b 9c f1 0e 3c f0 81 2e b8 2d ef dc 6f 96 19 f5 a0 05 98 96 93 65 82 0e 3d 7f fe 5c 5d 5d 5d ea ef ef 4f 4a 7b 7b 7b 02 13 ba a0 11 1e d0 27 ea bb af 28 dc 83 d3 fc 42 03 f0 dc 27 14 e8 84 16 d3 8f ee 30 3e d0 77 ae ee 6b e0 5b ee cf 9e 3d 53 47 47 87 5e be 7c a9 de de 5e f5 f5 f5 a9 bb bb fb 23 5d e8 7f 67 67 67 f2 8e 7a b4 81 46 e3 a1 1f f9 6d 58 4f 9f 3e 4d da 52 68 6b 79 40 9f fb cc ba 80 5c d0 75 8f 25 eb 10 b0 7d 4f f9 54 f7 3d 26 b9 5a 0e c8 8f df d0 c1 3b 68 a1 20 6f 0a 74 51 07 de ad 7b 86 69 79 ba 2d 70 80 09 bd f4 2b 72 05 2f 32 a2 cf 7a 7a 7a 12 d8 d4 81 37 da d2 0e 3c be 02 8b f7 e0 00 9f f9 04 16 f8 78 8f 5c 81 09 3c 74 02 99 f1 1c fc 2f 5e bc 48 9e 23 f7 81 81 81 8f 38 e1 01 b8 69 db c4 d5 b2 e7 b9 65 ed 02 0d 3c a3 1d 75 c0 39 3a 3a aa 62 b1 a8 72 b9 ac 4c 26 93 fc 1e 19 19 49 f0 40 87 79 b1 4c 2d 5f da 5b 5f 3d de d2 fd 04 1e 64 45 3d 78 30 1c 7e f3 1c 1a e0 df ba 0b 6d f4 09 ed ac db d4 a3 1d fa 86 8c 80 43 7b 8a fb d5 7d 04 1d 3c 47 7e c8 69 6c 6c 4c 13 13 13 09 3f f0 62 1d 34 1e c6 a8 ed b5 af c0 81 47 f8 06 06 f2 98 9e 9e 56 2e 97 d3 f8 f8 78 f2 cc e3 15 98 c8 0f 1a 0c 37 4d 3b fa c0 3d 25 8d 83 e7 d6 33 8a f5 ce b8 e1 17 3e e1 c3 3a c1 38 f4 58 74 1f 70 a5 1e 34 4d 4d 4d 25 34 4e 4e 4e 26 e3 16 79 21 bb b4 4d e0 9e 76 e9 31 e1 3a a6 c9 74 58 96 c0 47 ee e0 f5 bc e7 39 89 31 6b db ce 7b e8 84 96 c1 c1 c1 a4 8d f5 d3 Data Ascii: PNGIHDR~RZIDATx^lgsKj$ BZU(PZ8w8/;2+3UxxxxxE:v>3k?O~?O/~'Q3:}N<'N$Z[[ue]xQN6o_*I^u.]Wu\C {G?!)7p=+WkmO7o[Bh?wGx&#%`G??S__+</z3E];Pcy/wm=x@O<Q[[<G|_9>:9GQ;h>dMx{;w$xgE+!hG_PhN&^ErD .4+M+4B+8<-=0?~qQ8\770iY0Oic\{<.-oe=\]]]OJ{{{'(B'0>wk[=SGG^|^#]gggzFmXO>MRhky@\u%}OT=&Z;h otQ{iy-p+r /2zzz7<x\<t/^H#8ie<u9::brL&I@yL-_[_=dE=x0~mC{}<G~illL?b4GV.x7M;=%3>:8Xtp4MMM%4NNN&y!Mv1:tXG91k{

Code Manipulations

Statistics

Behavior



cmd.exe
conhost.exe
wget.exe

Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: 6596 Parent PID: 5112

General

Start time:	19:41:36
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c wget -t 2 -v -T 60 -P 'C:\Users\user\Desktop\download' --no-check-certificate --content-disposition --user-agent='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko' 'http://www.floridahealth.gov/_documents/newsroom/press-releases/2021/01/010421-COVID-19-main-page-vaccine-update.png' > cmdline.out 2>&1
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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\Desktop\cmdline.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	BDD194	CreateFileW

Analysis Process: conhost.exe PID: 6604 Parent PID: 6596

General

Start time:	19:41:36
Start date:	07/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: wget.exe PID: 6636 Parent PID: 6596

General

Start time:	19:41:37
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\wget.exe
Wow64 process (32bit):	true

Commandline:	wget -t 2 -v -T 60 -P 'C:\Users\user\Desktop\download' --no-check-certificate --content-disposition --user-agent='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko' 'http://www.floridahealth.gov/_documents/newsroom/press-releases/2021/01/010421-COVID-19-main-page-vaccine-update.png'
Imagebase:	0x400000
File size:	3895184 bytes
MD5 hash:	3DADB6E2ECE9C4B3E1E322E617658B60
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\Desktop\download\010421-COVID-19-main-page-vaccine-update.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	46596C	fopen

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\download\010421-COVID-19-main-page-vaccine-update.png	unknown	8192	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 09 c4 00 00 05 7e 08 06 00 00 00 52 82 af 5a 00 00 80 00 49 44 41 54 78 5e 6c bd 67 73 1c 4b 92 a6 db ff e7 9a dd 1d 9b 9e 99 9e de ee 9e d6 f2 1c 6a 12 24 a8 b5 96 20 09 42 10 5a 03 55 28 ad 50 d0 5a 11 a0 38 e4 91 ad a6 77 ed fe ac f7 fa 93 38 2f 3b 97 b6 1f c2 32 2b 33 c2 55 78 78 78 78 78 45 fe e0 f8 f1 e3 3a 76 ec 98 3e fb ec 33 fd fe f7 bf d7 af 7f fd 6b fd f4 a7 3f d5 4f 7e f2 13 fd fc e7 3f 4f ca 2f 7e f1 8b e4 dd 9f fe f4 27 51 ff cc 99 33 3a 7d fa b4 4e 9e 3c a9 13 27 4e 24 cf 5a 5b 5b 75 f9 f2 65 5d bc 78 51 a7 4e 9d d2 e1 c3 87 93 36 bf f9 cd 6f f4 ab 5f fd 2a 81 03 6c f0 d0 86 02 5e e3 ff fc f3 cf 75 e8 d0 a1 e4 1e d8 97 2e 5d d2 d5 ab 57 75 e1 c2 85 04 0f f0 5c a8 43 7b e8 00 ef d1 a3 47	.PNG.....IHDR.....~.....R ..Z....IDATx^l.gs.K..... .....j.$... .B.Z.U(.P.Z..8.. ..w.....8/;....2+3.UxxxxxE... ..:v..>..3.....k...?.O~.....? O./~.....'Q...3:}..N.<..'N $.Z[[u..e].xQ.N.....6...o.._. *..l....^.....u.....]...Wu. .....\.C{.....G	success or wait	856	47F21C	fwrite

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis