


**ID:** 337125
**Cookbook:** urldownload.jbs
**Time:** 19:41:09
**Date:** 07/01/2021
**Version:** 31.0.0 Red Diamond

# Table of Contents

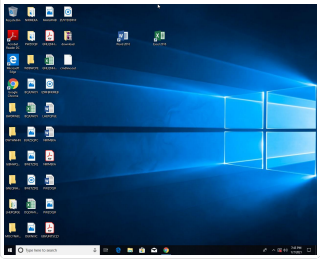
# Analysis Report http://www.floridahealth.gov/_documen…

## 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: | 337125 |

Most interesting Screenshot:



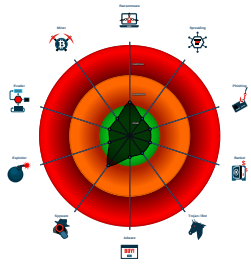
### Detection


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

### Signatures

Queries the volume information (nam…

### Classification



## Startup

- **System is w10x64**
- cmd.exe (PID: 7144 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: 7152 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - wget.exe (PID: 6252 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**

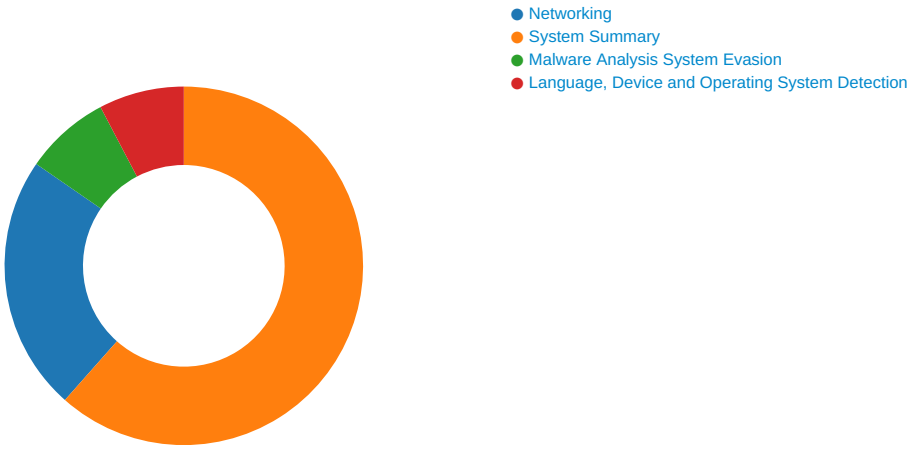
## Yara Overview

**No yara matches**

## Sigma Overview

**No Sigma rule has matched**

## Signature Overview



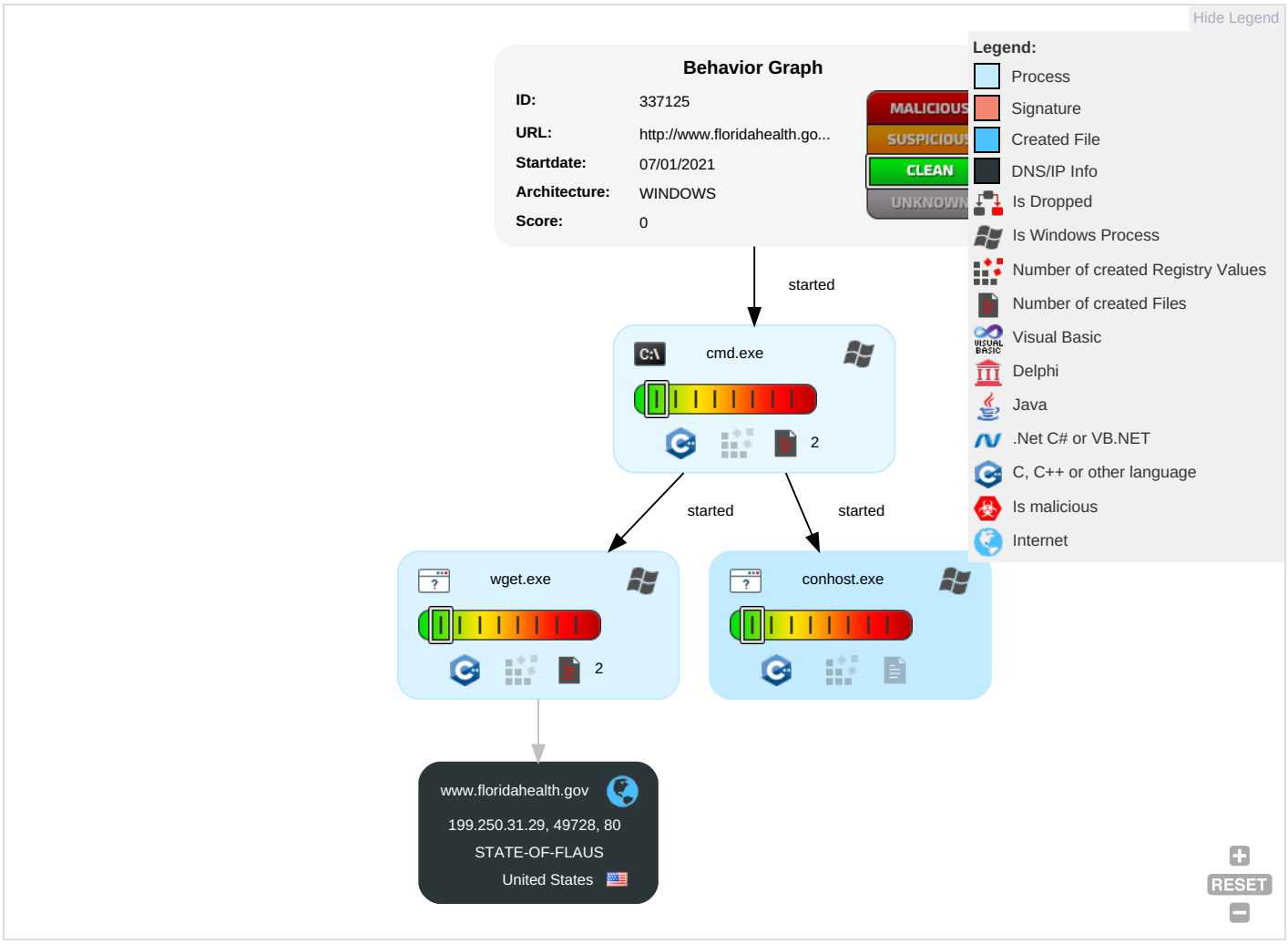

Click to jump to signature section

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, 00000002.00000002.686089547.0000000000D56000.00000004.00000040.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: | 337125 |
| Start date: | 07.01.2021 |
| Start time: | 19:41:09 |
| Joe Sandbox Product: | CloudBasic |

| | |
|---|---|
| Overall analysis duration: | 0h 3m 48s |
| 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: | 17 |
| 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<br>• EGA enabled<br>• HDC enabled<br>• 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%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Stop behavior analysis, all processes terminated |
| Warnings: | Show All<br>• Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe<br>• TCP Packets have been reduced to 100<br>• Excluded IPs from analysis (whitelisted): 13.88.21.125, 40.88.32.150, 51.11.168.160, 92.122.213.247, 92.122.213.194, 104.43.193.48, 52.155.217.156, 20.54.26.129, 2.20.142.209, 2.20.142.210, 13.64.90.137<br>• Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, au.download.windowsupdate.com.edgesuite.net, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net |

# 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): | 11630 |
| Entropy (8bit): | 2.4625978128204817 |
| Encrypted: | false |
| SSDEEP: | 96:1Et8u7ege+HMFPQr/u0jmlPV3LfPuZkb2q4KgZkpmJ0w:qOOegFHBnRWbd4ZZkgz |
| MD5: | BA9DD7F2BB6A740F8B4B853583801959 |
| SHA1: | D47A380205C72CC340D87C157449799CEF72BD1D |
| SHA-256: | 7E2FE1E23D24A8F3795E7FC005A5DF09DA880107CD034065E31862A8CC9B3E3C |
| SHA-512: | DED86EB06C792F65EB0B63571F8ADD8133D6D1F4B57C6836EB25A48355CFEC8DCDD23813E3799D933DE0056F4F83C03377679483A7EFB52BCB6871973BEDFC7 |
| Malicious: | false |
| Reputation: | low |
| Preview: | --2021-01-07 19:41:56-- 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% 304K 23s.. 50K ..... ..... ..... ..... ..... 1% 324K 22s.. 100K ..... ..... ..... ..... ..... .... 2% 2.51M 16s.. 150K ..... ..... ..... ..... ..... 2% 323K 17s.. 200K ..... ..... ..... ..... ..... 3% 327K 18s.. 250K ..... ..... ..... ... ..... ..... 4% 311K 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 |
| Reputation: | low |

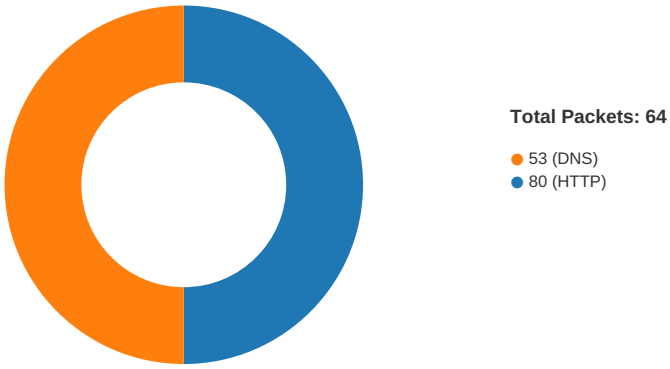
| C:\Users\user\Desktop\download\010421-COVID-19-main-page-vaccine-update.png | |
|---|---|
| Preview: | .PNG.....IHDR.....~.....R..Z....IDATx^l.gs.K.....j.$... .B.Z.U(.P.Z..8..w.....8/;....2+3.UxxxxxE.....:v.>..3.....k...?.O~.....?O./~.....'Q..3:}..N.<..'N$.Z[[u..e].xQ.N....<br>.6...o._.*..l...^.....u.....]..Wu.....\.C{....G..?.!)..7p.=.+W...k.m..O....7o..[..B.h?w..G...x..&....#...%...`.....G?....?.S..._..._.....+.....<...../.....z.....3.E]..;.P.cy./.....<br>.....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.....<br>...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...<.....<br>....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 19:41:56.929569006 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.087825060 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.087958097 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.090178967 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.249206066 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.261367083 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.261439085 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.261467934 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.261497974 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.261533976 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.261548996 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.261571884 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.261603117 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.261610985 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.261641026 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.261646986 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.261684895 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.261720896 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.261725903 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.261768103 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.261796951 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.261809111 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.261846066 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.261869907 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Jan 7, 2021 19:41:57.261883020 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.261920929 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.261940002 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.261956930 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.261993885 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.262010098 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.262031078 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.262078047 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.262084007 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.262120008 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.262156010 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.262191057 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.262479067 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.262561083 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.262640953 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.262682915 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.262715101 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.262763023 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.309098005 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.420747042 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.420804977 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.420842886 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.420888901 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.420926094 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.420965910 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421003103 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.421005011 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421042919 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421078920 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421114922 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421152115 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421191931 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.421197891 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421233892 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.421241045 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421278954 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421315908 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421327114 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.421358109 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421417952 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.421431065 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421471119 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421473980 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.421509981 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421546936 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421561956 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.421593904 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421634912 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421650887 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.421674013 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421711922 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421725988 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.421750069 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421785116 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421785116 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.421823025 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421859980 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421892881 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.421906948 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421950102 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.421984911 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.421987057 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.422025919 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.422039032 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Jan 7, 2021 19:41:57.422063112 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.422100067 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.422117949 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.422138929 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.422174931 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.422209024 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.422219992 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.422261953 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.422262907 CET | 49728 | 80 | 192.168.2.4 | 199.250.31.29 |
| Jan 7, 2021 19:41:57.422297955 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.422334909 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |
| Jan 7, 2021 19:41:57.422373056 CET | 80 | 49728 | 199.250.31.29 | 192.168.2.4 |

## UDP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Jan 7, 2021 19:41:53.896713018 CET | 58028 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:41:53.944441080 CET | 53 | 58028 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:41:55.075021029 CET | 53097 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:41:55.123085976 CET | 53 | 53097 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:41:56.548675060 CET | 49257 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:41:56.599298954 CET | 53 | 49257 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:41:56.857256889 CET | 62389 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:41:56.916568041 CET | 53 | 62389 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:41:59.079382896 CET | 49910 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:41:59.127067089 CET | 53 | 49910 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:00.226696014 CET | 55854 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:00.282979965 CET | 53 | 55854 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:15.348512888 CET | 64549 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:15.396636009 CET | 53 | 64549 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:19.142081976 CET | 63153 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:19.198641062 CET | 53 | 63153 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:21.408607960 CET | 52991 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:21.456469059 CET | 53 | 52991 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:31.584877968 CET | 53700 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:31.633009911 CET | 53 | 53700 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:32.190071106 CET | 51726 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:32.305135965 CET | 53 | 51726 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:32.813360929 CET | 56794 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:32.861336946 CET | 53 | 56794 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:33.096755981 CET | 56534 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:33.167295933 CET | 53 | 56534 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:33.341839075 CET | 56627 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:33.435868025 CET | 53 | 56627 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:33.867034912 CET | 56621 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:33.926106930 CET | 53 | 56621 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:34.444879055 CET | 63116 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:34.501204014 CET | 53 | 63116 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:35.038664103 CET | 64078 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:35.097956896 CET | 53 | 64078 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:35.808624983 CET | 64801 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:35.856571913 CET | 53 | 64801 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:36.655544996 CET | 61721 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:36.711973906 CET | 53 | 61721 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:37.164089918 CET | 51255 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:37.228976011 CET | 53 | 51255 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:40.735948086 CET | 61522 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:40.796710014 CET | 53 | 61522 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:47.005906105 CET | 52337 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:47.053909063 CET | 53 | 52337 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:50.234685898 CET | 55046 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:50.282708883 CET | 53 | 55046 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:42:50.528043985 CET | 49612 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:50.584724903 CET | 53 | 49612 | 8.8.8.8 | 192.168.2.4 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Jan 7, 2021 19:42:52.812066078 CET | 49285 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:42:52.872512102 CET | 53 | 49285 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:43:14.896277905 CET | 50601 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:43:14.946980953 CET | 53 | 50601 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:43:16.565649033 CET | 60875 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:43:16.616429090 CET | 53 | 60875 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:43:17.702032089 CET | 56448 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:43:17.749960899 CET | 53 | 56448 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:43:18.929966927 CET | 59172 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:43:18.980719090 CET | 53 | 59172 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:43:20.075464964 CET | 62420 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:43:20.123347044 CET | 53 | 62420 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:43:23.877351046 CET | 60579 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:43:23.925316095 CET | 53 | 60579 | 8.8.8.8 | 192.168.2.4 |
| Jan 7, 2021 19:43:25.706520081 CET | 50183 | 53 | 192.168.2.4 | 8.8.8.8 |
| Jan 7, 2021 19:43:25.762687922 CET | 53 | 50183 | 8.8.8.8 | 192.168.2.4 |

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Jan 7, 2021 19:41:56.857256889 CET | 192.168.2.4 | 8.8.8.8 | 0x43ca | 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 19:41:56.916568041 CET | 8.8.8.8 | 192.168.2.4 | 0x43ca | 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 | 192.168.2.4 | 49728 | 199.250.31.29 | 80 | C:\Windows\SysWOW64\wget.exe |

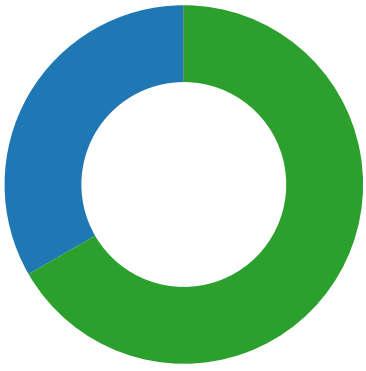
| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jan 7, 2021 19:41:57.090178967 CET | 52 | OUT | GET /_documents/newsroom/press-releases/2021/01/010421-COVID-19-main-page-vaccine-update.png HTTP/1.1<br>User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko<br>Accept: */*<br>Accept-Encoding: identity<br>Host: www.floridahealth.gov<br>Connection: Keep-Alive |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jan 7, 2021 19:41:57.261367083 CET | 57 | IN | HTTP/1.1 200 OK<br>Content-Type: image/png<br>Last-Modified: Thu, 07 Jan 2021 01:27:17 GMT<br>Accept-Ranges: bytes<br>ETag: "bb1daa3c94e4d61:0"<br>Server: Microsoft-IIS/8.5<br>X-Powered-By: ASP.NET<br>Date: Thu, 07 Jan 2021 18:41:56 GMT<br>Content-Length: 7231526<br>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<br>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




Click to jump to process

# System Behavior

## Analysis Process: cmd.exe PID: 7144 Parent PID: 4940

### General

| | |
|---|---|
| Start time: | 19:41:54 |
| 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: | 0x11d0000 |
| 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 | 11DD194 | CreateFileW |

## Analysis Process: conhost.exe PID: 7152 Parent PID: 7144

### General

| | |
|---|---|
| Start time: | 19:41:55 |
| Start date: | 07/01/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff724c50000 |
| 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: 6252 Parent PID: 7144

### General

| | |
|---|---|
| Start time: | 19:41:56 |
| 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 | 851 | 47F21C | fwrite |

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Disassembly

### Code Analysis