ID: 354427
Cookbook: urldownload.jbs
Time: 21:04:33
Date: 17/02/2021
Version: 31.0.0 Emerald

Table of Contents

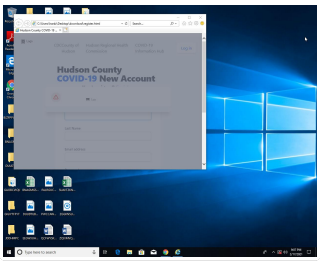
Analysis Report http://hudsoncovidvax.org/register

Overview

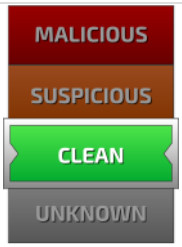
General Information

Sample URL:	http://hudsoncovidvax.org/register
Analysis ID:	354427

Most interesting Screenshot:



Detection

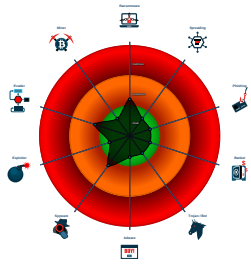


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- Detected potential crypto function
- Queries the volume information (nam…
- Uses code obfuscation techniques (…

Classification



Analysis Advice

Sample may offer command line options, please run it with the 'Execute binary with arguments' cookbook (it's possible that the command line switches require additional characters like: "-", "/", "--")

Uses HTTPS for network communication, use the 'Proxy HTTPS (port 443) to read its encrypted data' cookbook for further analysis

Startup

- **System is w10x64**
- cmd.exe (PID: 5944 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://hudsoncovidvax.org/register' > cmdline.out 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 6076 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - wget.exe (PID: 5320 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://hudsoncovidvax.org/register' MD5: 3DADB6E2ECE9C4B3E1E322E617658B60)
- iexplore.exe (PID: 752 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' C:\Users\user\Desktop\download\register.html MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4904 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:752 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

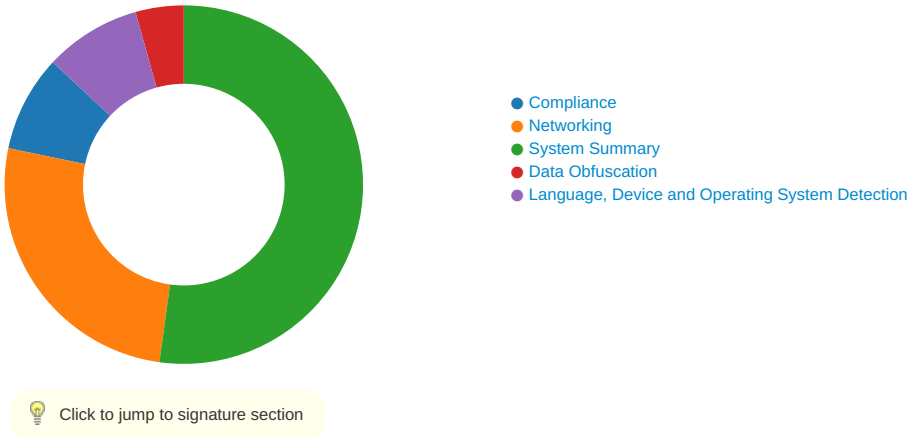
Yara Overview

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.

Compliance:

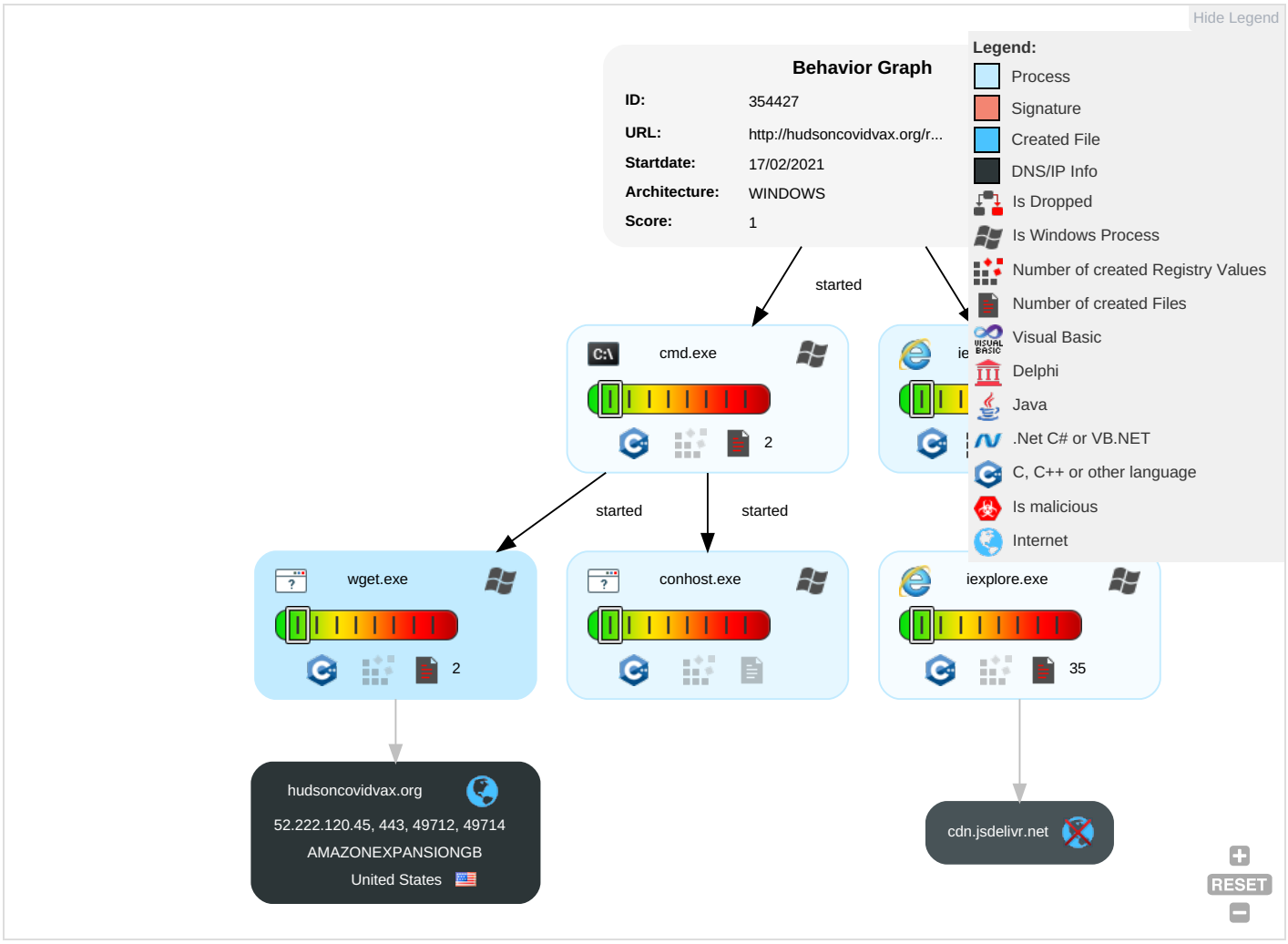
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

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	Ir
Valid Accounts	Command and Scripting Interpreter 2	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	System Information Discovery 1 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Remote System Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		C B F

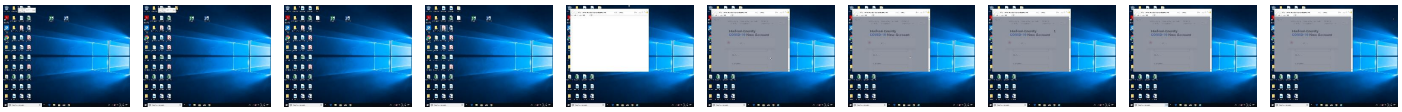
Behavior Graph

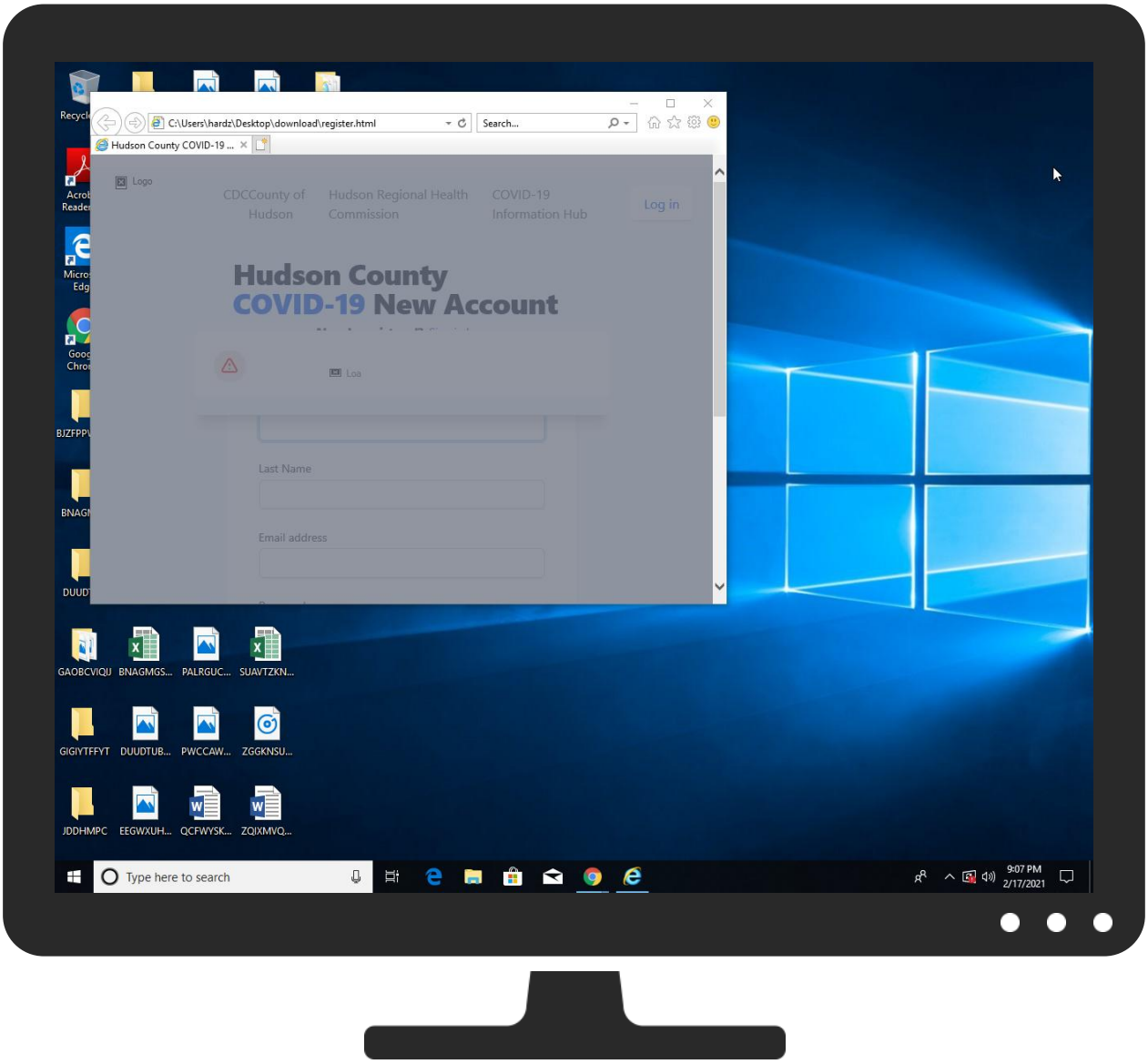


Screenshots

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://hudsoncovidvax.org/register	0%	Virustotal		Browse
http://hudsoncovidvax.org/register	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
hudsoncovidvax.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://praleska.pro/	0%	Virustotal		Browse
http://praleska.pro/	0%	Avira URL Cloud	safe	
http://https://www.hudsonregional.org/	0%	Virustotal		Browse
http://https://www.hudsonregional.org/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hudsoncovidvax.org	52.222.120.45	true	false	• 0%, Virustotal, Browse	unknown
cdn.jsdelivr.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://hudsoncovidvax.org/register	false		unknown

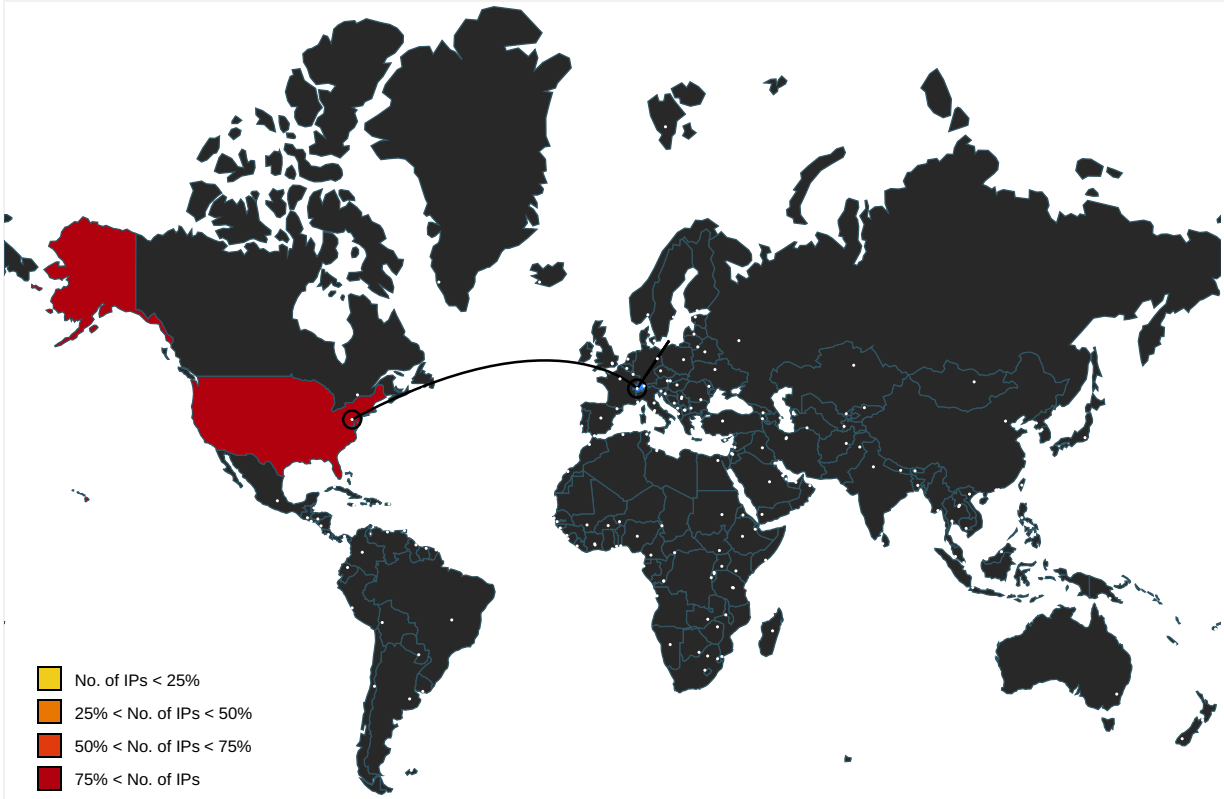
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/svgdotjs/svg.draggable.js	apexcharts[1].js.5.dr	false		high
http://https://dbushell.com/	app[1].css.5.dr	false		high
http://https://github.com/baryon	app[1].js.5.dr	false		high
http://https://github.com/robin0van0der0v	app[1].js.5.dr	false		high
http://https://github.com/xsoh	app[1].js.5.dr	false		high
http://https://github.com/noureddinem	app[1].js.5.dr	false		high
http://https://github.com/TalAter	app[1].js.5.dr	false		high
http://https://github.com/sirn	app[1].js.5.dr	false		high
http://https://github.com/socketpair	app[1].js.5.dr	false		high
http://https://github.com/chrisrodz	app[1].js.5.dr	false		high
http://https://github.com/ebraminio	app[1].js.5.dr	false		high
http://https://github.com/jonashdown	app[1].js.5.dr	false		high
http://https://github.com/kyungw00k	app[1].js.5.dr	false		high
http://https://github.com/joshbrooks	app[1].js.5.dr	false		high
http://https://github.com/marobo	app[1].js.5.dr	false		high
http://https://github.com/ryanhart2	app[1].js.5.dr	false		high
http://https://github.com/kcthota	app[1].js.5.dr	false		high
http://new.gramota.ru/spravka/buro/search-answer?s=242637	app[1].js.5.dr	false		high
http://https://github.com/demidov91	app[1].js.5.dr	false		high
http://https://github.com/kalehv	app[1].js.5.dr	false		high
http://https://github.com/flakerimi	app[1].js.5.dr	false		high
http://https://github.com/kwisatz	app[1].js.5.dr	false		high
http://https://github.com/aliem	app[1].js.5.dr	false		high
http://https://github.com/Manfre98	app[1].js.5.dr	false		high
http://https://github.com/evoL	app[1].js.5.dr	false		high
http://https://github.com/vnathalye	app[1].js.5.dr	false		high
http://https://github.com/suupic	app[1].js.5.dr	false		high
http://https://github.com/bustta	app[1].js.5.dr	false		high
http://https://github.com/le0tan	app[1].js.5.dr	false		high
http://https://github.com/mehiel	app[1].js.5.dr	false		high
http://https://github.com/narainsagar	app[1].js.5.dr	false		high
http://https://hudson-county-coronavirus-resources-hudsoncogis.hub.arcgis.com/	register.3.dr	false		high
http://https://github.com/ryangreaves	app[1].js.5.dr	false		high
http://https://github.com/DevelopmentIL	app[1].js.5.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/ragulka	app[1].js.5.dr	false		high
http://https://github.com/ElFadiliY	app[1].js.5.dr	false		high
http://https://github.com/ibnesayeed	app[1].js.5.dr	false		high
http://https://github.com/jbleduigou	app[1].js.5.dr	false		high
http://https://github.com/skfd	app[1].js.5.dr	false		high
http://https://github.com/muminoff	app[1].js.5.dr	false		high
http://www.reddit.com/	msapplication.xml4.4.dr	false		high
http://https://github.com/JanisE	app[1].js.5.dr	false		high
http://https://github.com/abdelsaid	app[1].js.5.dr	false		high
http://https://github.com/chyngyz	app[1].js.5.dr	false		high
http://cps.root-x1.letsencrypt.org0	wget.exe, 00000003.00000003.19 9978132.0000000002E89000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/tailwindcss/tailwindcss/issues/362	app[1].css.5.dr	false		high
http://https://github.com/hehachris	app[1].js.5.dr	false		high
http://https://github.com/zemlanin	app[1].js.5.dr	false		high
http://https://github.com/mayanksinghal	app[1].js.5.dr	false		high
http://cps.letsencrypt.org0	wget.exe, 00000003.00000003.19 9978132.0000000002E89000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/andela-batolagbe	app[1].js.5.dr	false		high
http://https://github.com/forabi	app[1].js.5.dr	false		high
http://https://github.com/stephenramthun	app[1].js.5.dr	false		high
http://https://github.com/bleadof	app[1].js.5.dr	false		high
http://https://github.com/mozdevs/cssremedy/issues/4	app[1].css.5.dr	false		high
http://praleska.pro/	app[1].js.5.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://github.com/Kaushik1987	app[1].js.5.dr	false		high
http://https://github.com/bangnk	app[1].js.5.dr	false		high
http://https://github.com/mirontoli	app[1].js.5.dr	false		high
http://https://github.com/petrbela	app[1].js.5.dr	false		high
http://https://github.com/boyaq	app[1].js.5.dr	false		high
http://https://github.com/mrbase	app[1].js.5.dr	false		high
http://https://github.com/naderio	app[1].js.5.dr	false		high
http://https://github.com/kaushikgandhi	app[1].js.5.dr	false		high
http://https://github.com/B0k0	app[1].js.5.dr	false		high
http://https://github.com/middagj	app[1].js.5.dr	false		high
http://https://github.com/javkhaanj7	app[1].js.5.dr	false		high
http://https://github.com/mweimerskirch	app[1].js.5.dr	false		high
http://https://github.com/kruyvanna	app[1].js.5.dr	false		high
http://https://github.com/suvash	app[1].js.5.dr	false		high
http://https://github.com/floydpink	app[1].js.5.dr	false		high
http://https://github.com/julionc	app[1].js.5.dr	false		high
http://https://github.com/andrewhood125	app[1].js.5.dr	false		high
http://https://github.com/suitcss/base	app[1].css.5.dr	false		high
http://new.gramota.ru/spravka/rules/139-prop	app[1].js.5.dr	false		high
http://www.youtube.com/	msapplication.xml7.4.dr	false		high
http://https://github.com/rajeevnaikte	app[1].js.5.dr	false		high
http://https://github.com/ShahramMebashar	app[1].js.5.dr	false		high
http://https://github.com/soniasimoes	app[1].js.5.dr	false		high
http://https://github.com/BYK	app[1].js.5.dr	false		high
http://https://github.com/mozdevs/cssremedy/issues/14	app[1].css.5.dr	false		high
http://nicolasgallagher.com/micro-clearfix-hack/	app[1].css.5.dr	false		high
http://https://github.com/skakri	app[1].js.5.dr	false		high
http://https://github.com/jalex79	app[1].js.5.dr	false		high
http://https://github.com/vajradog	app[1].js.5.dr	false		high
http://https://github.com/wernerm	app[1].js.5.dr	false		high
http://https://github.com/kraz	app[1].js.5.dr	false		high
http://https://github.com/nurlan	app[1].js.5.dr	false		high
http://https://github.com/nusretparlak	app[1].js.5.dr	false		high
http://https://github.com/sigurdga	app[1].js.5.dr	false		high
http://https://github.com/tailwindcss/tailwindcss/pull/116	app[1].css.5.dr	false		high
http://https://github.com/anthonylau	app[1].js.5.dr	false		high
http://https://github.com/nostalgiaz	app[1].js.5.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/sampathsris	app[1].js.5.dr	false		high
http://https://www.hudsonregional.org/	register.3.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://github.com/Viktorminator	app[1].js.5.dr	false		high
http://https://github.com/milan-j	app[1].js.5.dr	false		high
http://https://github.com/ulmus	app[1].js.5.dr	false		high
http://https://github.com/gurdiga	app[1].js.5.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.222.120.45	unknown	United States		8987	AMAZONEXPANSIONGB	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	354427
Start date:	17.02.2021
Start time:	21:04:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	urldownload.jbs
Sample URL:	http://hudsoncovidvax.org/register
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:	28
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:	clean1.win@7/19@3/1
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): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.193.48, 104.42.151.234, 52.147.198.201, 88.221.62.148, 151.101.2.109, 151.101.66.109, 151.101.130.109, 151.101.194.109, 216.58.206.42, 52.255.188.83, 51.11.168.160, 184.30.24.56, 152.199.19.161, 92.122.213.247, 92.122.213.194, 20.54.26.129, 93.184.221.240, 51.104.139.180 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, dualstack.f3.shared.global.fastly.net, fonts.googleapis.com, fs.microsoft.com, ie9comview.vo.msecnd.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Execution Graph export aborted for target wget.exe, PID 5320 because there are no executed function • Report size getting too big, too many NtQueryValueKey calls found.

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\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{E6DD9952-71A6-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24152
Entropy (8bit):	1.758465408321881
Encrypted:	false
SSDEEP:	48:IwRGcprUGwpLZG/ap8hGIpc3pGvnZpv3uGvHZp93zGomTqpv3GGo4aiXpcbGWmvY:rnZsZ92jWGt7fBtxrWB
MD5:	B2A847F2F0B0CA3DE28AF0C17A753998
SHA1:	D3B2C9524E9744EF388AE362CDB02A7CE716A16B
SHA-256:	2C53088C853A99696002DD1E59ED2C011FFC200F60267321A25B6386EA763FB3
SHA-512:	35B5A6B9BD926401B5DFA4A096F167595DAFE1AA55F2CC68CF4863C7FDBCFDB6236F3C0DB6F6DD40224E50C31F07B5B45F396AE65F02F9003A48C4913744774
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E6DD9954-71A6-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28088
Entropy (8bit):	2.050747898518416
Encrypted:	false
SSDEEP:	192:rlZuQyuzrkzQ/zrGzSmz33zzj6DFPM1MUMQmQXhWr:rrr5UC+tr7UFPM1MUMQK
MD5:	88E09E8B9941CA8135187C66306B0BB0
SHA1:	1446EDA69550BD274FE7A49EC90521F404459B6A
SHA-256:	555214D13E89757A64D5E2BB5F2853A3997981232D28F03D97158CDC537381B8
SHA-512:	E4FCC70A62F9F623D4538092715D545387A13336F287C07AF12A9027ABF6CEAE314A7FED445B06B064B33470560F07C994D83B5A8D315070E3C9854C5E4F02D4
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.060023711385613
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEde6eAnWimI002EtM3MHdNMNxOEde6eAnWimI00ObVbkEtMb:2d6NxO+SZHKd6NxO+SZ76b
MD5:	545A422666A858565D0355CF4C7D307C
SHA1:	1083795D57535B39325C75CF511593438FAC2007
SHA-256:	B1CF587EDEC66B601B26A2CBB4E1607A98D17A7ADA0DC11DCF9F6508CCFBDF73
SHA-512:	EC8CA3A4261F951C22FA07E24BC32F0C17A0B2B3F6369718DB31AEFADD4534B514F8FC835FDABD7054CE860640746CD3A36E4A3841497FD0D543C75A48EC42 3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xbdd20301,0x01d705b3</date> accdate>0xbdd20301,0x01d705b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xbdd20301,0x01d705b3</date><accdate>0 xbdd20301,0x01d705b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile ></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.074732533413301
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kJUeEUeAnWimI002EtM3MHdNMNxe2kJUeEFTeAnWimI00Obkak6Ety:2d6NxruCiSZHKd6NxruCF/SZ7Aa7b
MD5:	1CA9CC2C6DEEFA05783DB6225A74167A
SHA1:	FBDE72F26C57189495B6401837F1F9B886E08777
SHA-256:	2DFF976433E5702837BE3557013BF65BA244AAF5779B129F12EEB0BD92B6D039
SHA-512:	7C78C1ACABF17519535A9C3A1E753FDB7EFC35567BAED6FADD7837BFE023CD9F43B740086DB473BB720031F603CF2E683D65E0BBCCA47DA55D810BCA716A5 00
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xbdcadbf3,0x01d705b3</date><a ccdate>0xbdcadbf3,0x01d705b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xbdcadbf3,0x01d705b3</date><a ccdate>0xbdcd3e61,0x01d705b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.128325762739983
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLXuHeCuHeAnWimI002EtM3MHdNMNxvLXuHeCuHeAnWimI00ObmZEtMb:2d6Nxvz+8SZHKd6Nxvz+8SZ7mb
MD5:	AE1AF21CE690A5BB9A26A70EF871525F
SHA1:	FAF4BECDCDF7371050120D8F7C3A543DBD804B9D
SHA-256:	9F419DA893F494F5D6C649CC6E4EB7510EA1F5D619C6111F416836BFAA116914
SHA-512:	1CF56639A11DD2DD2647C6551FB58E6D17DCDB487DC0A574AFA9606DCCED738CD2CFA4209E1ECEB07F527D1AC1DA68AAA850ACA2E10B090DC8B51AF76107 622
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xbdd46566,0x01d705b3</date> <accdate>0xbdd46566,0x01d705b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>.. <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xbdd46566,0x01d705b3</date><accda te>0xbdd46566,0x01d705b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe dia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.045388841076145

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNxiJRieERieAnWimI002EtM3MHdNMNxiJRieERieAnWimI00Obd5EtMb:2d6NxQR4R8SZHKd6NxQR4R8SZ7Jjb
MD5:	11AD8014611C5DEA145FAA7EA996DE0E
SHA1:	5019BF2D5342C5E0268FBB5F6CC110D4C13D61EB
SHA-256:	0FB4A5FA690B26AB4A16CC3D0679ECD3A6D07100DD6D727186C50D96A9E71545
SHA-512:	7629F8F55B4F4324630DE26FA0FF78404AAC056043BCB5FEBB9F64F3FCF493A27936661A225B5DE00C4A01E8719589B57220E0C095FBE9118C21156928E3A1D4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xbdcfa0fe,0x01d705b3</date><acc date>0xbdcfa0fe,0x01d705b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xbdcfa0fe,0x01d705b3</date><accdate>0xbdcfa 0fe,0x01d705b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.139591862833914
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwXuHeCuHeAnWimI002EtM3MHdNMNxhGwXuHeCuHeAnWimI00Ob8K0z:2d6NxQ4+8SZHKd6NxQ4+8SZ7YKajb
MD5:	C1C82D02596A7E05417CBE7FB714BA79
SHA1:	75381AE393A4646E4B27B75C2DF636B129389A9B
SHA-256:	153F86741C8F132AD8CD58CEBDEC8B0A45AF0DC4B3CC5D220B5CDEDF94F76225
SHA-512:	0ACA997D844CCC983AE3CC05524A7A1CF3EA2275B5848E7552E6EABAE097F96943B1BE010A9952824AA62EE9C4E65B0C9CEAE2EB95E466DF23AA56B9C9E399 2E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xbdd46566,0x01d705b3</date>< accdate>0xbdd46566,0x01d705b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xbdd46566,0x01d705b3</date><accdate>0 xbdd46566,0x01d705b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.058551984238958
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nde6eAnWimI002EtM3MHdNMNx0nde6eAnWimI00ObxEtMb:2d6Nx0HSZHKd6Nx0HSZ7nb
MD5:	AEFFC4593B81D71D877B1796A3DFD9FF
SHA1:	D2398E89EF4D68CF958FB2551FCA75A2C4514887
SHA-256:	D1560551425AAFA392FF92AA593A6E184EACC9F3669E4B1A263BE9131F8945A8
SHA-512:	2F118E421E7854429A0154F53EC1D78B572EBEAFA25F4E6084F801A0E93B69701DDD94AC7472C6EA8A99A812C3580B692FCDCB81DD6B5A32579756FEA9E04D9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xbdd20301,0x01d705b3</date><a ccdate>0xbdd20301,0x01d705b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xbdd20301,0x01d705b3</date><accdate>0xb dd20301,0x01d705b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin202591677780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.100447412656309
Encrypted:	false
SSDEEP:	12:TMHdNMNxxde6eAnWimI002EtM3MHdNMNxxde6eAnWimI00Ob6Kq5EtMb:2d6Nx5SZHKd6Nx5SZ7ob
MD5:	E2FAEA6F542DF1D6473F07F9A73F514A
SHA1:	C0AAF572B61914551778084A0CA58FC3947B8A85
SHA-256:	D7E01E635DBD86053A04C66259314BA315B474EC4F87FFD6AF767B0231F60F35

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
SHA-512:	01D16F4496116B66A27ED3B99358F39995A11FEA3FB6EFB559B1B5109DBEBAAB589D5B7192A04F2BB7B20DCE490F92F30F3E9F7624565268A6A82F4A41D9E9B3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xbdd20301,0x01d705b3</date><accdate>0xbdd20301,0x01d705b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xbdd20301,0x01d705b3</date><accdate>0xbdd20301,0x01d705b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.042502884674027
Encrypted:	false
SSDEEP:	12:TMHdNMNxcJRieERieAnWimI002EtM3MHdNMNxcJRieERieAnWimI00ObVEtMb:2d6NxmR4R8SZHKd6NxmR4R8SZ7Db
MD5:	7A91E9401D5C4E99A6D326B8F3B3BEF3
SHA1:	AC46A98158C5D4DDAE94A85424647401C83D3912
SHA-256:	A500B5D393CA2BA3D771E9645E29D53763F96DF92337C8D302B03DB55A69FC61
SHA-512:	8B1FC04863BDD63F7F8D83327C555ABCE78739933A43904ED5A73C7B90AA677DB13EC0A35E11CA1EC5C3989823ABCAEB37CF6340B46E04A042201C532C1ECC F1
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xbdcfa0fe,0x01d705b3</date><accdate>0xbdcfa0fe,0x01d705b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xbdcfa0fe,0x01d705b3</date><accdate>0xbdcfa0fe,0x01d705b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.031656402659191
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnJRieERieAnWimI002EtM3MHdNMNxfnJRieERieAnWimI00Obe5EtMb:2d6NxBR4R8SZHKd6NxBR4R8SZ7ijb
MD5:	7EB8E30B2FFC0E177C92ADEB0E4E2E36
SHA1:	83E65B6BDFFC390BCF624449FB16389696FEAA8A
SHA-256:	E361EADE6D09986D6D87D357D0D0DEA239584947ECD29C635AEB52869839BD61
SHA-512:	12003DD18CEA433D514639F700BE05346A893AE94B2957ED1CF6CF11E62515254F457F5EAD0C02FFECB746707D880AED1EB64A88258F452D4C6C0702088B6EF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xbdcfa0fe,0x01d705b3</date><accdate>0xbdcfa0fe,0x01d705b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xbdcfa0fe,0x01d705b3</date><accdate>0xbdcfa0fe,0x01d705b3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\app[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	4630213
Entropy (8bit):	4.9944667875013975
Encrypted:	false
SSDEEP:	12288:ml9yaxYSqmHJ7USZIk1KOj0i5WqH4g0fBG2G67Fr6Sh6g50ufCq9cirKmU9ttuap:O0PUeUkUdUm
MD5:	BC64EACDD97BBDE1DA476E901A4D06BE
SHA1:	0C5107B57E4DF5FB7FAD099CC3325EF4CB0140C7
SHA-256:	BA6EED30B0DDBD317500FD2CFC37524F08B3668C12D3C1A6F21F566B19DED085
SHA-512:	78944EBE73E72C774EDAB7A24DC45CEE2A2152338235AC5D1B6345868FDACE4F3DE395655E04AAF8636D0E0C7FE396523D5BBA0D8FCD7E044E7AE97729EEAI 42
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hudsoncovidvax.org/css/app.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\app[1].css	
Preview:	@charset "UTF-8";...flatpickr-calendar {. background: transparent;. opacity: 0;. display: none;. text-align: center;. visibility: hidden;. padding: 0;. -webkit-animation: none;. animation: none;. direction: ltr;. border: 0;. font-size: 14px;. line-height: 24px;. border-radius: 5px;. position: absolute;. width: 307.875px;. box-sizing: border-box;. touch-action: manipulation;. background: #fff;. box-shadow: 1px 0 0 #e6e6e6, -1px 0 0 #e6e6e6, 0 1px 0 #e6e6e6, 0 -1px 0 #e6e6e6, 0 3px 13px rgba(0, 0, 0, 0.08);. }...flatpickr-calendar.open, .flatpickr-calendar.inline {. opacity: 1;. max-height: 640px;. visibility: visible;.}...flatpickr-calendar.open {. display: inline-block;. z-index: 99999;.}...flatpickr-calendar.animate.open {. -webkit-animation: fpFadeInDown 300ms cubic-bezier(0.23, 1, 0.32, 1);. animation: fpFadeInDown 300ms cubic-bezier(0.23, 1, 0.32, 1);.}...flatpickr-calendar.inline {. display: block;. position: relative;. top: 2px;.}...flatpickr-calendar.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\app[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	5426110
Entropy (8bit):	5.927068717787939
Encrypted:	false
SSDEEP:	49152:K5eruGw4R2EVY0tRnc9rQF6JWLZxQbhbRcLMGUxjcZpRZyoOnCE4AfzvB+l8uWwt:jRXFKqUxgr4h4AfzJJbig0oL6n/gC
MD5:	DED864A07035113076D308061A1F8665
SHA1:	1421FF05787A093A5AC84DCD83DEFE3F04F166EA
SHA-256:	649B9080E93A4084019748DBD39068B106DD44F1F16923F1D462AC58D339CF2F
SHA-512:	53F2EC9607DA1C005F5AE78DF6838807089C70B21CA96B66F8819D46EA3C78C53F536982C4C35B17CA64B33EFB3B1BC0841CC0BEEC6854FB4044658F6A5C5A1C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://hudsoncovidvax.org/js/app.js
Preview:	/******/ (function(modules) { // webpackBootstrap./******/ .// The module cache./******/ .var installedModules = {};./******/./******/ .// The require function./******/ .function _ _webpack_require__(moduleId) {./******/./******/ ..// Check if module is in cache./******/ ..if(installedModules[moduleId]) {./******/ ...return installedModules[moduleId].exports;./******/ ..}./******/ ..// Create a new module (and put it into the cache)./******/ ..var module = installedModules[moduleId] = {./******/ ...i: moduleId,./******/ ...l: false,./******/ ...exports: {}./******/ ..};./******/./******/ ..// Execute the module function./******/ ..modules[moduleId].call(module.exports, module, module.exports, __webpack _require__);./******/./******/ ..// Flag the module as loaded./******/ ..module.l = true;./******/./******/ ..// Return the exports of the module./******/ ..return module.exports;. /******/ .}./******/./******/./******/ .// expose the modules object (__webpack_modules__)./******/ .__webpack

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\apexcharts[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	474593
Entropy (8bit):	5.277544382560772
Encrypted:	false
SSDEEP:	6144:DVZhLJwmpDrClAOIILrUHWJZIK/NnKjZl4Uv3eecTyXlkP9zdrbUq0CNPudvDJBS:ZxwC8dSCNPOBjhqz
MD5:	BD2E4AA6DF4150607333FC01C11A4504
SHA1:	7D8326E51CBEA2DC825402A79E2D375811A84CB1
SHA-256:	59BBD4147A7264206B218C4EBC96EBACEE81A9265B009B48EBF62BE8850DA8E8
SHA-512:	52441634A1F53D379ADEB0991ED6CAE6084F6DD6D20902B82ED805353995096F90288DE35CED689246F006902E6C050D85BE024BCA2B7298C143DE1DDA75B69
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.jsdelivr.net/npm/apexcharts
Preview:	/*!. * ApexCharts v3.25.0. * (c) 2018-2021 Juned Chhipa. * Released under the MIT License.. */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module? module.exports=e():"function"==typeof define&&define.amd?define(e):(t="undefined"!=typeof globalThis?globalThis:t||self).ApexCharts=e()}(this,(function(){"use strict"; function t(e){return(t="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){return typeof t}:function(t){return t&&"function"==typeof Symbol&&t.constructor===Symbol&&t!==Symbol.prototype?"symbol":typeof t})(e)}function e(t,e){if(!(t instanceof e))throw new TypeError("Cannot call a class as a function")}function i(t,e){for(var i=0;i<e.length;i++){var a=e[i];a.enumerable=a.enumerable||!1,a.configurable=!0,"value"in a&&(a.writable=!0),Object.defineProperty(t,a.key,a)}}function a(t,e,a){return e&&i(t.prototype,e),a&&i(t,a),t}function s(t,e,i){return e in t?Object.defineProperty(t,e,{value:i,enumerable:!0,configurable:!0,writable:!0}):t[e]=i,t}func

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	175
Entropy (8bit):	5.031069620363828
Encrypted:	false
SSDEEP:	3:0SYWFFWlIYCN7tFSRI5XwDKLRIHDfFRWdFTfqzrZqcd+4sIbhWiseoYARNin:0IFFJtFS+56ZRWHTizlpd+7IbrsPNin
MD5:	95CF7B42351AE6BCCC4FA6B6E8C5F91F
SHA1:	3A152A19923551E52B87D7BA3C69A82C66D8E0F6
SHA-256:	94BF9A6D7D7A02901D180435970107C58D1CAECE2E0A9D964470BD7AB662554E
SHA-512:	48232A8EA8A9D0F2FC6494D8F035362C3B5787D5F1BF84BDF086963A08800B292C710806F9DE6D7E8A617659F69641AC73020951C49E48ED220376160A553C52
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Nunito

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\css[1].css	
Preview:	@font-face {. font-family: 'Nunito';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/nunito/v16/XRXV3I6Li01BKofINeaH.woff) format('woff');.}.

C:\Users\user\AppData\Local\Temp\~DF0BFD6412979B4C12.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12965
Entropy (8bit):	0.4182714077317336
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loZDF9loZJ9lWZm0fDff0N00C:kBqoII2X7v
MD5:	92235C1523CB2CB51A1D00A0A6CC18F3
SHA1:	301C4F11CCD80642F28F55318759F802F8E176D7
SHA-256:	6F7B238B3903CAE88CB9CFD18352D3920BC20425053AC8AA1542927D5F8E6B61
SHA-512:	9318342C06452B28972E606A879C4B9F670882316650211014231A0B234834F9FFF78F026CC3ABEDB2B3460BDA77516A81249114BCBADC445069896B7F7165F0
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFB4B5035858316FB9.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	36765
Entropy (8bit):	0.7423220751161954
Encrypted:	false
SSDEEP:	192:kBqoxK0zfzvzszHzazwzqzozDz3FPM1MUMQmQ:kBqoxK0DTQ7GMWMnzFPM1MUMQ
MD5:	8CEE520B91DA001BF12BCCB60DD9091C
SHA1:	10F7CBCE32A886BD86626B12926FEE4561CEB3F6
SHA-256:	EC46BED710E37CB4D67D181038881EACCD436F93461FDB0D6BC7F6F94879F3E3
SHA-512:	ECE6F9B5A078E2E5FBEE87859BEB0F5B389DE12039DD7D9EA14679844726B06C244F94B910DDA83D971DB2C8774E3A88FF4F94B1DA7A4D51D5A6C5C0467DC4 43
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\Desktop\cmdline.out	
Process:	C:\Windows\SysWOW64\wget.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	797
Entropy (8bit):	5.100920939114529
Encrypted:	false
SSDEEP:	24:YYw4U7C5oCIxeP6j4UMovY54Uu8CjxePgJ1p77pYE7u:y7TouFH1p772E7u
MD5:	48CB8CA9266C5E568A19A739E65689FC
SHA1:	89FEF91FAA951807303E192B9B545AF8F5E81235
SHA-256:	A8C9FAC4FEE25B51A9444BF78E448358D761F920B186B9925E9DCDB1556F883D
SHA-512:	33571EB715686D5D9558B5D3E7134CE79C27C9F8E5F73EFE92ED2F866AD6FC1C500ACF815B0FA9306C5579089730673EC2AA8E383586D9AA0A9B442A6B13001
Malicious:	false
Reputation:	low
Preview:	--2021-02-17 21:05:18-- http://hudsoncovidvax.org/register..Resolving hudsoncovidvax.org (hudsoncovidvax.org)... 52.222.120.45..Connecting to hudsoncovidvax.org (hudsoncovidvax.org)|52.222.120.45|:80... connected...HTTP request sent, awaiting response... 301 Moved Permanently..Location: https://hudsoncovidvax.org/register [following]..--2021-02-17 21:05:19-- https://hudsoncovidvax.org/register..Connecting to hudsoncovidvax.org (hudsoncovidvax.org)|52.222.120.45|:443... connected...HTTP request sent, awaiting response... 200 OK..Length: unspecified [text/html]..Saving to: 'C:/Users/user/Desktop/download/register'.... 0K .... 93.6K=0.2s....2021-02-17 21:05:20 (93.6 KB/s) - 'C:/Users/user/Desktop/download/register' saved [18260]....

C:\Users\user\Desktop\download\register	
Process:	C:\Windows\SysWOW64\wget.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped

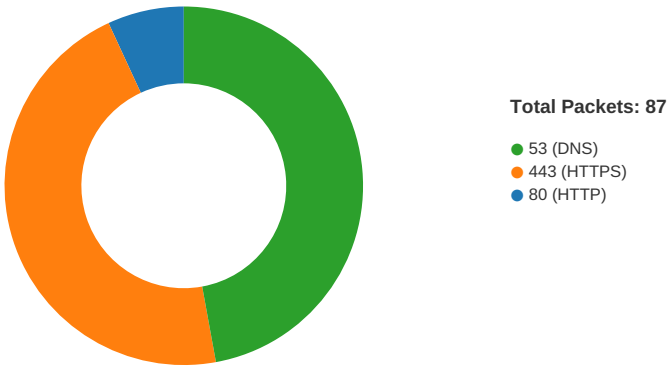
C:\Users\user\Desktop\download\register	
Size (bytes):	18260
Entropy (8bit):	4.683492835703746
Encrypted:	false
SSDEEP:	384:ESCcujLMV3AtKlHnVFw0j4vIpd19CowConCogCoUo4fB/2:PDXrQOBYpq
MD5:	EB83FE75FFFD659106A3A7FA33A01676
SHA1:	FAB1BF7CBBA1CA5287FAA58EFE576C49295AFC4A
SHA-256:	2683BE5CB77D65ACEBD54DEBAB34C3FA54EB3920EEEB62B518B014F5656BEA87
SHA-512:	EFE958CADCFFE4C4008E8789B20F5EDF0268F5295C161270D19DF3349BEFABD6FC395F70F3BBDB1CDA2B8FBD18C0AE93D5705133B3C131D1909C7E215EAD831
Malicious:	false
Reputation:	low
Preview:	<!doctype html>.<html lang="en">.<head>. <meta charset="utf-8">. <meta name="viewport" content="width=device-width, initial-scale=1">.. CSRF Token -->. <meta name="csrf-token" content="6x8pRtyFDyzw4RYb4cZP0nHl2k8dRIF8PcekFKX0">.. <title>Hudson County COVID-19 Vaccination</title>.. Scripts -->. <script src="https://hudsoncovidvax.org/js/app.js" defer></script>. <script src="https://cdn.jsdelivr.net/npm/apexcharts"></script>. . Fonts -->. <link rel="dns-prefetch" href="//fonts.gstatic.com">. <link href="https://fonts.googleapis.com/css?family=Nunito" rel="stylesheet">.. Styles -->. <link href="https://hudsoncovidvax.org/css/app.css" rel="stylesheet">. <style>[wire\:loading], [wire\:loading\.delay] {display: none;}[wire\:offline] {display: none;}[wire\:dirty]:not(textarea):not(input):not(select) {display: none;}input:-webkit-autofill, select:-webkit-autofill, textarea:-webkit-autofill {animation-duration: 50000s;animation-na

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 17, 2021 21:05:18.974270105 CET	49712	80	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:19.172930002 CET	80	49712	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:19.173093081 CET	49712	80	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:19.176599026 CET	49712	80	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:19.375197887 CET	80	49712	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:19.606251955 CET	80	49712	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:19.647639990 CET	49712	80	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:19.728673935 CET	49714	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:19.927510977 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:19.927710056 CET	49714	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:19.935168982 CET	49714	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:20.133862019 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.135318995 CET	443	49714	52.222.120.45	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 17, 2021 21:05:20.135360956 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.135390043 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.135452986 CET	49714	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:20.138803005 CET	49714	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:20.337990046 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.338043928 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.341557026 CET	49714	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:20.540307045 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.551088095 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.551115990 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.551127911 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.551143885 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.551156044 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.551172018 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.551215887 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.551230907 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.551249027 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.551278114 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.551295042 CET	49714	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:20.551350117 CET	49714	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:20.551409006 CET	49714	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:20.566274881 CET	49712	80	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:20.753047943 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.753077984 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.753089905 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.753106117 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.753169060 CET	49714	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:20.753204107 CET	49714	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:20.753317118 CET	443	49714	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.768656969 CET	80	49712	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:20.768719912 CET	49712	80	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:20.803900957 CET	49714	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:21.300215006 CET	49714	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:24.812627077 CET	49720	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:24.813610077 CET	49719	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.011863947 CET	443	49720	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.012075901 CET	49720	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.012438059 CET	443	49719	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.013607025 CET	49719	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.016398907 CET	49720	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.016634941 CET	49719	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.215306997 CET	443	49720	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.215500116 CET	443	49719	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.234394073 CET	443	49720	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.234447956 CET	443	49720	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.234479904 CET	49720	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.234491110 CET	443	49720	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.234518051 CET	49720	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.234539032 CET	49720	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.243519068 CET	49720	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.243784904 CET	49720	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.323847055 CET	443	49719	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.323903084 CET	443	49719	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.323931932 CET	49719	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.323935986 CET	443	49719	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.323961973 CET	49719	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.323977947 CET	49719	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.327349901 CET	49719	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.327673912 CET	49719	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.442413092 CET	443	49720	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.442560911 CET	443	49720	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.442668915 CET	443	49720	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.442739964 CET	49720	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.456207991 CET	443	49720	52.222.120.45	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 17, 2021 21:05:25.456281900 CET	443	49720	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.456322908 CET	49720	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.456331968 CET	443	49720	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.456348896 CET	49720	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.456392050 CET	443	49720	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.456394911 CET	49720	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.456439972 CET	443	49720	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.456454039 CET	49720	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.456485033 CET	443	49720	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.456506968 CET	49720	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.456530094 CET	443	49720	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.456546068 CET	49720	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.456577063 CET	443	49720	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.456593990 CET	49720	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.456640005 CET	443	49720	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.456641912 CET	49720	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.456707001 CET	49720	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.526251078 CET	443	49719	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.526375055 CET	443	49719	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.526531935 CET	49719	443	192.168.2.3	52.222.120.45
Feb 17, 2021 21:05:25.526585102 CET	443	49719	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.546988964 CET	443	49719	52.222.120.45	192.168.2.3
Feb 17, 2021 21:05:25.547030926 CET	443	49719	52.222.120.45	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 17, 2021 21:05:11.820369959 CET	50620	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:11.869339943 CET	53	50620	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:12.790611029 CET	64938	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:12.842093945 CET	53	64938	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:13.927182913 CET	60152	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:13.978940010 CET	53	60152	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:15.233908892 CET	57544	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:15.282566071 CET	53	57544	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:16.300792933 CET	55984	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:16.352303982 CET	53	55984	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:17.286109924 CET	64185	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:17.334796906 CET	53	64185	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:18.551748991 CET	65110	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:18.611712933 CET	53	65110	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:18.812103033 CET	58361	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:18.956094980 CET	53	58361	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:19.521755934 CET	63492	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:19.570513010 CET	53	63492	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:20.463742018 CET	60831	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:20.521064997 CET	53	60831	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:21.648906946 CET	60100	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:21.697779894 CET	53	60100	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:22.734466076 CET	53195	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:22.783009052 CET	53	53195	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:23.384277105 CET	50141	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:23.441494942 CET	53	50141	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:23.804049969 CET	53023	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:23.853477955 CET	53	53023	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:24.740765095 CET	49563	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:24.762803078 CET	51352	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:24.795275927 CET	53	49563	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:24.817352057 CET	53	51352	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:24.817501068 CET	59349	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:24.874429941 CET	53	59349	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:25.293214083 CET	57084	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:25.350281954 CET	53	57084	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:26.480789900 CET	58823	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 17, 2021 21:05:26.529411077 CET	53	58823	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:27.526828051 CET	57568	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:27.575864077 CET	53	57568	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:28.321137905 CET	50540	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:28.370996952 CET	53	50540	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:29.268687010 CET	54366	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:29.332087994 CET	53	54366	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:44.269737005 CET	53034	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:44.318440914 CET	53	53034	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:50.898164988 CET	57762	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:50.959816933 CET	53	57762	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:53.423474073 CET	55435	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:53.472541094 CET	53	55435	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:54.327207088 CET	50713	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:54.378972054 CET	53	50713	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:54.433231115 CET	55435	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:54.482008934 CET	53	55435	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:55.339205980 CET	50713	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:55.390935898 CET	53	50713	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:55.447901964 CET	55435	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:55.496808052 CET	53	55435	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:55.864023924 CET	56132	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:55.925307989 CET	53	56132	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:56.353960991 CET	50713	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:56.405556917 CET	53	50713	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:57.463565111 CET	55435	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:57.512748957 CET	53	55435	8.8.8.8	192.168.2.3
Feb 17, 2021 21:05:58.370842934 CET	50713	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:05:58.422413111 CET	53	50713	8.8.8.8	192.168.2.3
Feb 17, 2021 21:06:01.479777098 CET	55435	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:06:01.528678894 CET	53	55435	8.8.8.8	192.168.2.3
Feb 17, 2021 21:06:02.385940075 CET	50713	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:06:02.437490940 CET	53	50713	8.8.8.8	192.168.2.3
Feb 17, 2021 21:06:05.454668045 CET	58987	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:06:05.522586107 CET	53	58987	8.8.8.8	192.168.2.3
Feb 17, 2021 21:06:05.541332006 CET	56579	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:06:05.593039989 CET	53	56579	8.8.8.8	192.168.2.3
Feb 17, 2021 21:06:19.164448023 CET	60633	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:06:19.216002941 CET	53	60633	8.8.8.8	192.168.2.3
Feb 17, 2021 21:06:22.301582098 CET	61292	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:06:22.365835905 CET	53	61292	8.8.8.8	192.168.2.3
Feb 17, 2021 21:06:54.104264021 CET	63619	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:06:54.153578043 CET	53	63619	8.8.8.8	192.168.2.3
Feb 17, 2021 21:06:55.776607037 CET	64938	53	192.168.2.3	8.8.8.8
Feb 17, 2021 21:06:55.847626925 CET	53	64938	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 17, 2021 21:05:18.812103033 CET	192.168.2.3	8.8.8.8	0x76bb	Standard query (0)	hudsoncovidvax.org	A (IP address)	IN (0x0001)
Feb 17, 2021 21:05:24.740765095 CET	192.168.2.3	8.8.8.8	0x9884	Standard query (0)	hudsoncovidvax.org	A (IP address)	IN (0x0001)
Feb 17, 2021 21:05:24.762803078 CET	192.168.2.3	8.8.8.8	0xa851	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 17, 2021 21:05:18.956094980 CET	8.8.8.8	192.168.2.3	0x76bb	No error (0)	hudsoncovidvax.org		52.222.120.45	A (IP address)	IN (0x0001)
Feb 17, 2021 21:05:24.795275927 CET	8.8.8.8	192.168.2.3	0x9884	No error (0)	hudsoncovidvax.org		52.222.120.45	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 17, 2021 21:05:24.817352057 CET	8.8.8.8	192.168.2.3	0xa851	No error (0)	cdn.jsdelivr.net	dualstack.f3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- hudsoncovidvax.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49712	52.222.120.45	80	C:\Windows\SysWOW64\wget.exe

Timestamp	kBytes transferred	Direction	Data
Feb 17, 2021 21:05:19.176599026 CET	986	OUT	GET /register 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: hudsoncovidvax.org Connection: Keep-Alive
Feb 17, 2021 21:05:19.606251955 CET	992	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 17 Feb 2021 20:05:19 GMT Server: Apache/2.4.41 (Ubuntu) Location: https://hudsoncovidvax.org/register Content-Length: 327 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 68 75 64 73 6f 6e 63 6f 76 69 64 76 61 78 2e 6f 72 67 2f 72 65 67 69 73 74 65 72 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 31 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 75 64 73 6f 6e 63 6f 76 69 64 76 61 78 2e 6f 72 67 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.41 (Ubuntu) Server at hudsoncovidvax.org Port 80</address></body></html>

HTTPS Packets

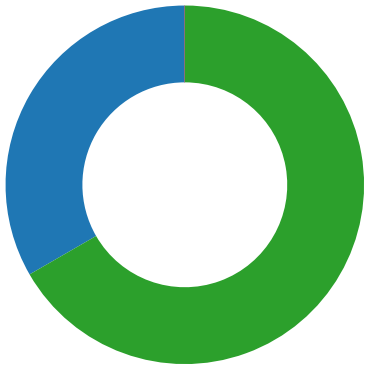
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 17, 2021 21:05:20.135360956 CET	52.222.120.45	443	192.168.2.3	49714	CN=hudsoncovidvax.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Jan 28 03:17:27 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Apr 28 04:17:27 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49200-159-52393-52392-52394-49195-49199-158-49188-49192-107-49187-49191-103-49162-49172-57-49161-49171-51-157-156-61-60-53-47-255,0-11-10-35-22-23-13,29-23-25-24,0-1-2	807fca46d9d0cf63adf4e5e80e414bbe
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 17, 2021 21:05:25.234447956 CET	52.222.120.45	443	192.168.2.3	49720	CN=hudsoncovidvax.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Jan 28 03:17:27 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Apr 28 04:17:27 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 17, 2021 21:05:25.323903084 CET	52.222.120.45	443	192.168.2.3	49719	CN=hudsoncovidvax.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Jan 28 03:17:27 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Apr 28 04:17:27 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



cmd.exe
conhost.exe
wget.exe
iexplore.exe
iexplore.exe

Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: 5944 Parent PID: 2592

General

Start time:	21:05:16
Start date:	17/02/2021
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://hudsoncovidvax.org/register' > 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: 6076 Parent PID: 5944

General

Start time:	21:05:16
Start date:	17/02/2021
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: 5320 Parent PID: 5944

General

Start time:	21:05:17
Start date:	17/02/2021
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://hudsoncovidvax.org/register'
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\register	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\register	unknown	8192	3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 0a 20 20 20 20 3c 21 2d 2d 20 43 53 52 46 20 54 6f 6b 65 6e 20 2d 2d 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 63 73 72 66 2d 74 6f 6b 65 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 36 78 38 70 52 74 79 46 44 79 7a 77 34 52 59 62 34 63 5a 50 30 6e 48 6c 32 6b 38 64 52 49 46 38 50 63 65 6b 46 4b 58 30 22 3e 0a 0a 20 20 20 20 3c 74 69 74 6c	<!doctype html>.<html lang="en">.<head>. <meta charset="utf-8">. <meta name="viewport" content="width=device-width, initial-scale=1">.. CSRF Token -->. <meta name="csrf-token" content="6x8pRtyFDy zw4RYb4cZP0nHl2k8dRIF 8PcekFKX0">.. <titl	success or wait	2	47F21C	fwrite

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 752 Parent PID: 5584

General

Start time:	21:05:22
Start date:	17/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' C:\Users\user\Desktop\download\register.html
Imagebase:	0x7ff6292d0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 4904 Parent PID: 752

General

Start time:	21:05:23
Start date:	17/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:752 CREDAT:17410 /prefetch:2
Imagebase:	0x1210000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis