ID: 349157
Cookbook: urldownload.jbs
Time: 15:06:24
Date: 05/02/2021
Version: 31.0.0 Emerald

Table of Contents

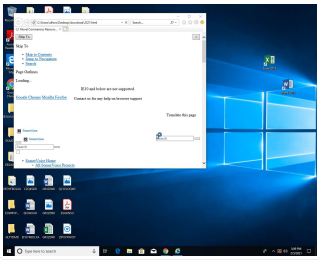
Analysis Report https://somervoice.somervillema.gov/n…

Overview

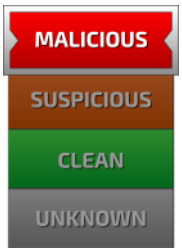
General Information

Sample URL:	http://https://somervoice.somervillema.gov/novel-coronavirus-resources-for-businesses/widgets/16897/videos/2327
Analysis ID:	349157

Most interesting Screenshot:



Detection



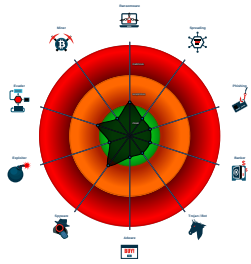
Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Snort IDS alert for network traffic (e….

Queries the volume information (nam…

Classification



Startup

- **System is w10x64**
- cmd.exe (PID: 6080 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' 'https://somervoice.somervillema.gov/novel-coronavirus-resources-for-businesses/widgets/16897/videos/2327' > cmdline.out 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 4580 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - wget.exe (PID: 5924 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' 'https://somervoice.somervillema.gov/novel-coronavirus-resources-for-businesses/widgets/16897/videos/2327' MD5: 3DADB6E2ECE9C4B3E1E322E617658B60)
- iexplore.exe (PID: 5988 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' C:\Users\user\Desktop\download\2327.html MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2092 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5988 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

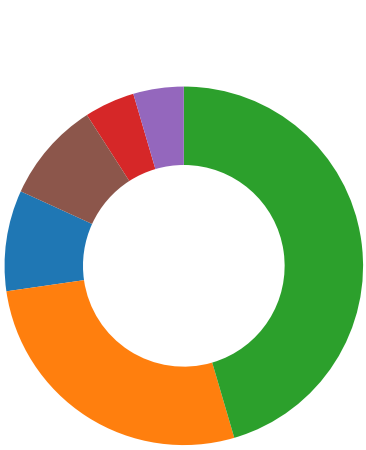
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Compliance:

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

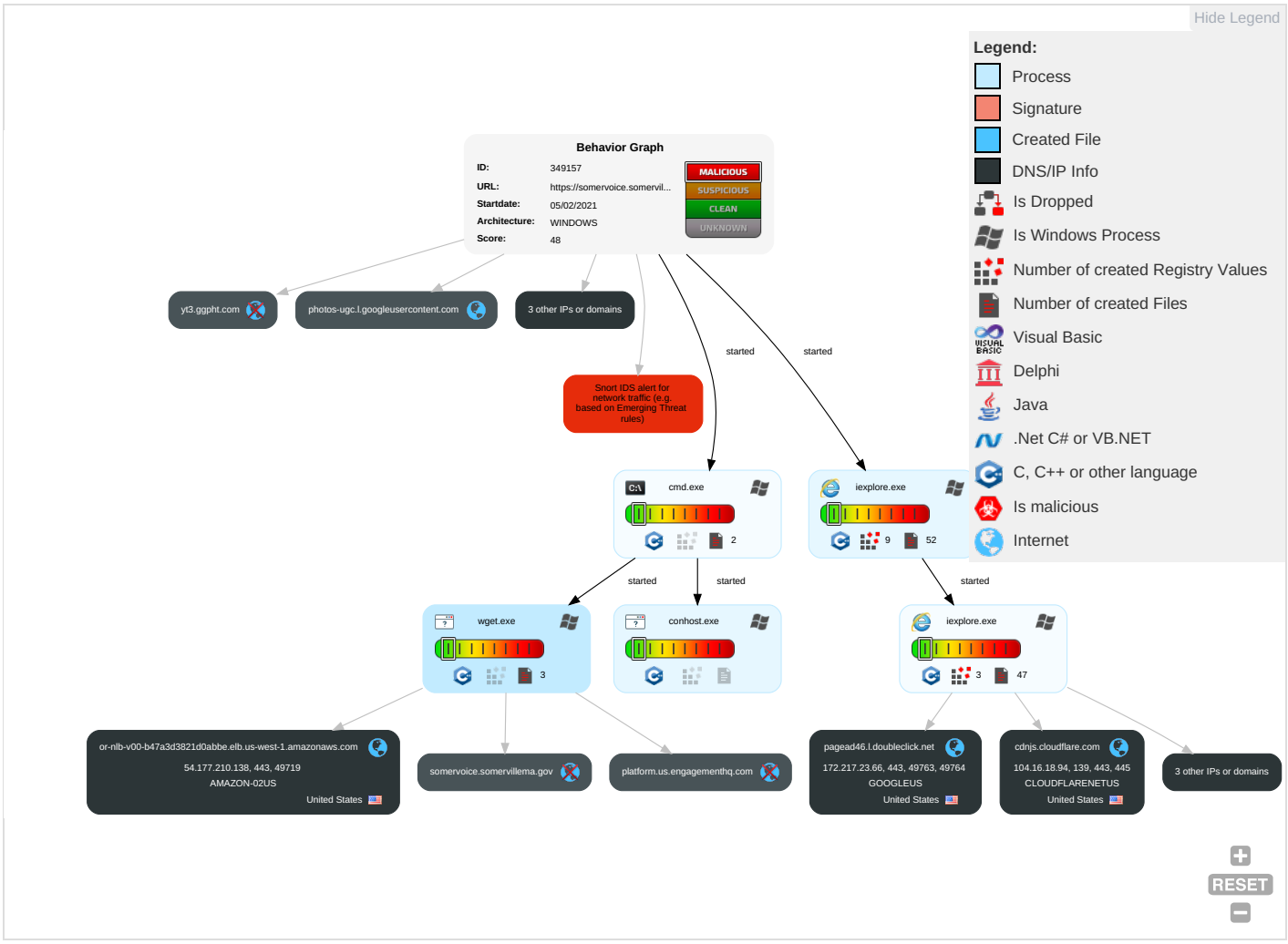
Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

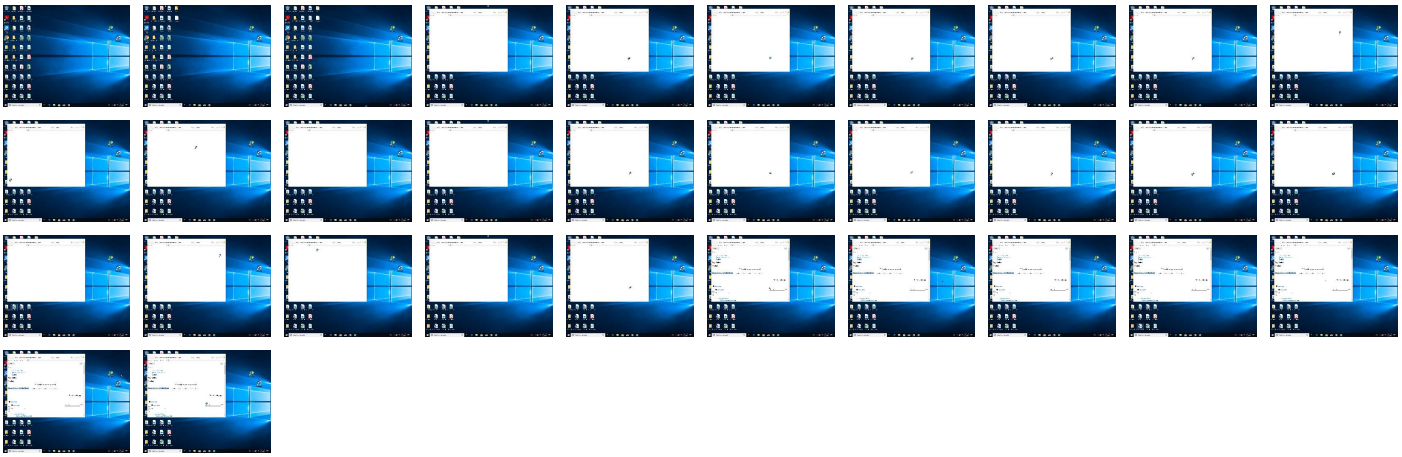
Behavior Graph

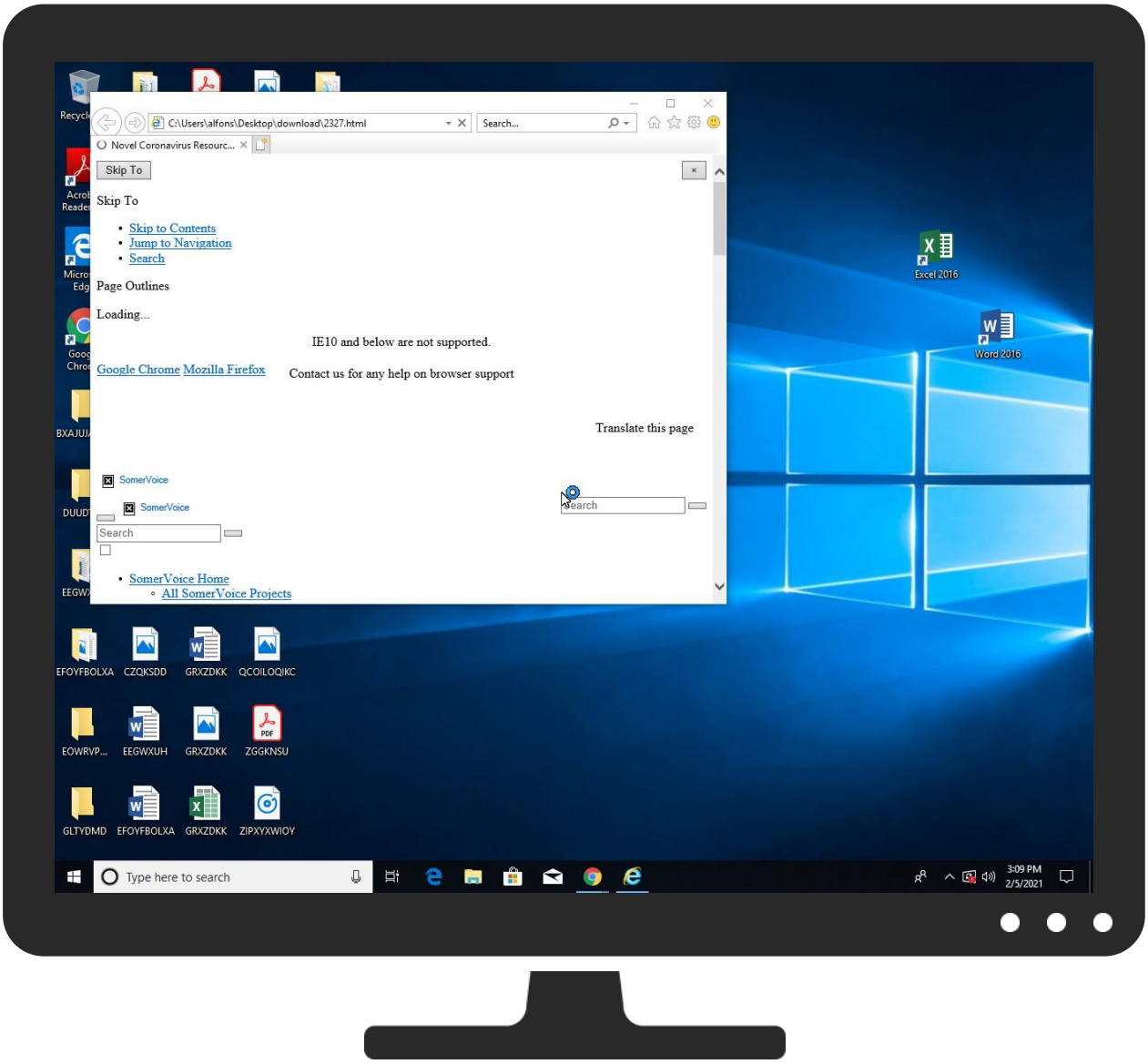


Screenshots

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://https://somervoice.somervillema.gov/novel-coronavirus-resources-for-businesses/widgets/16897/videos/2327	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://r3.i.lencr.org/	0%	Avira URL Cloud	safe	
http://www.somervision2040.com	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0&	0%	Avira URL Cloud	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.org=	0%	Avira URL Cloud	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://s3-us-west-1.amazonaws.co	0%	Avira URL Cloud	safe	
http://www.somervillebydesign.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pagead46.l.doubleclick.net	172.217.23.66	true	false		high
or-nlb-v00-b47a3d3821d0abbe.elb.us-west-1.amazonaws.com	54.177.210.138	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
i.ytimg.com	172.217.22.246	true	false		high
photos-ugc.l.googleusercontent.com	172.217.23.33	true	false		high
d2gu4vothxmtom.cloudfront.net	143.204.15.131	true	false		high
yt3.ggpht.com	unknown	unknown	false		high
googleads.g.doubleclick.net	unknown	unknown	false		high
somervoice.somervillema.gov	unknown	unknown	false		high
www.youtube.com	unknown	unknown	false		high
static.doubleclick.net	unknown	unknown	false		high

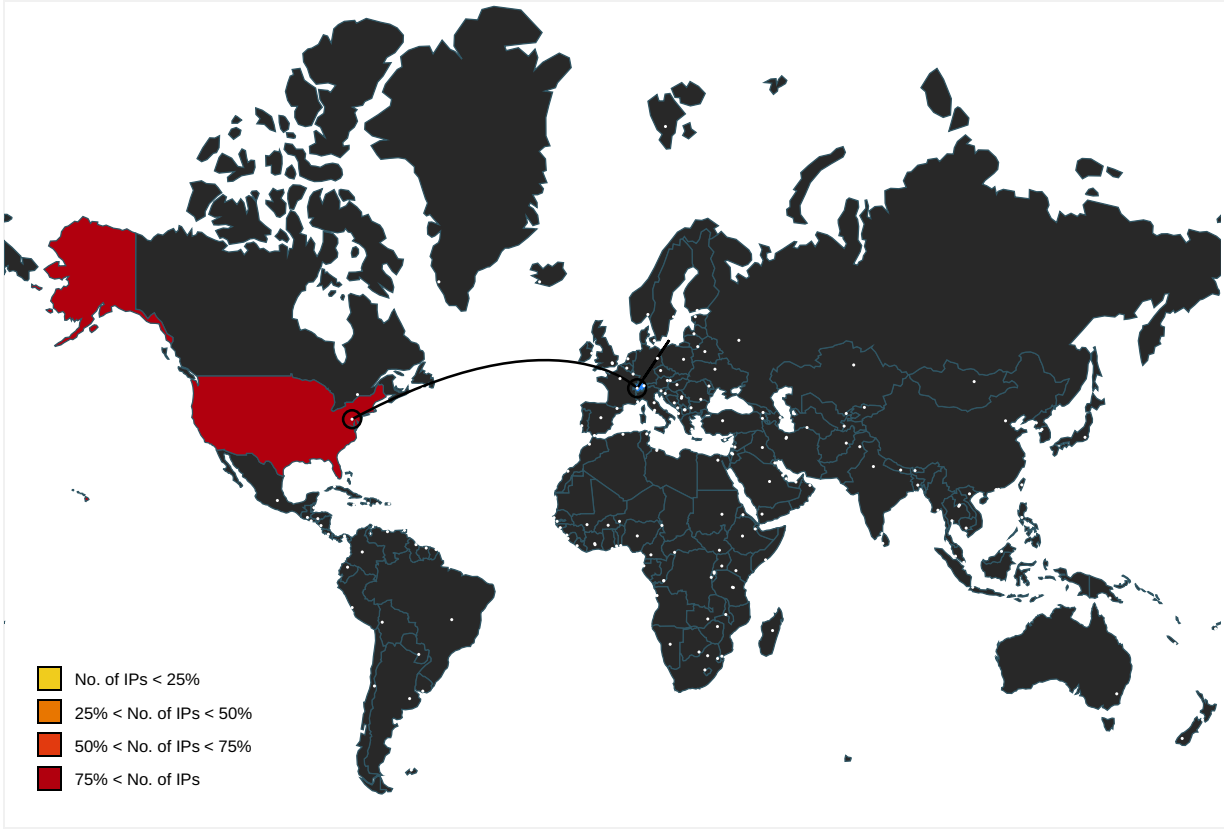
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://youtu.be/Fn7Ou04BHvQ	wget.exe, 00000002.00000002.23 7274437.0000000001048000.00000 004.00000001.sdmp, 2327.2.dr	false		high
http://https://www.youtube.com/watch?v=5GRcO6cLNs8	wget.exe, 00000002.00000003.23 6779922.0000000001040000.00000 004.00000001.sdmp, 2327.2.dr	false		high
http://fontawesome.io	font-awesome.min[1].css.6.dr	false		high
http://https://i.ytimg.com/vi/cuSif0I20vE/hqdefault.jpg	wget.exe, 00000002.00000002.23 7274437.0000000001048000.00000 004.00000001.sdmp, 2327.2.dr	false		high
http://https://youtu.be/wtuxe7VPD3U	wget.exe, 00000002.00000003.23 6829486.0000000001049000.00000 004.00000001.sdmp, wget.exe, 0 0000002.00000003.236786957.000 0000001048000.00000004.0000000 1.sdmp, 2327.2.dr	false		high
http://https://i.ytimg.com/vi/VFxvnJ7wwwU/hqdefault.jpg	wget.exe, 00000002.00000003.23 6779922.0000000001040000.00000 004.00000001.sdmp, 2327.2.dr	false		high
http://https://s3-us-west-1.amazonaws.com/ehq-production-us-california/8cfcc1570c81e97a242433b94052e3e65b3c	2327.2.dr	false		high
http://https://ehq-production-us-california.imgix.net/b811435cc596009e6a357d66f662c1fff094b1f4/image_stores	2327.2.dr	false		high
http://youtube.com/streaming/otf/durations/112015	base[1].js.6.dr	false		high
http://https://somervoice.somervillema.gov/novel-coronavirus-resources-for-businesses/widgets/16897/videos/	2327.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.somervillema.gov/events	wget.exe, 00000002.00000003.23 6779922.0000000001040000.00000 004.00000001.sdmp, 2327.2.dr	false		high
http://cps.letsencrypt.org	wget.exe, 00000002.00000003.23 6829486.0000000001049000.00000 004.00000001.sdmp	false		high
http://youtube.com/streaming/metadata/segment/102015	base[1].js.6.dr	false		high
http://https://youtu.be/	base[1].js.6.dr	false		high
http://r3.i.lencr.org/	wget.exe, 00000002.00000003.23 6829486.0000000001049000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://somervillema.gov	2327.2.dr	false		high
http://https://admin.youtube.com	base[1].js.6.dr	false		high
http://www.somervision2040.com	wget.exe, 00000002.00000003.23 6779922.0000000001040000.00000 004.00000001.sdmp, 2327.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://i.ytimg.com/vi/5GRcO6cLNs8/hqdefault.jpg	wget.exe, 00000002.00000003.23 6779922.0000000001040000.00000 004.00000001.sdmp, 2327.2.dr	false		high
http://r3.o.lencr.org0	wget.exe, 00000002.00000003.23 6829486.0000000001049000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://github.com/krux/postscribe/blob/master/LICENSE.	js[1].js.6.dr	false		high
http://https://www.youtube.com/watch?v=KTb4H2DQcdc	wget.exe, 00000002.00000003.23 6779922.0000000001040000.00000 004.00000001.sdmp, 2327.2.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.6.dr	false		high
http://https://www.youtube.com/watch?v=cuSif0I20vE	wget.exe, 00000002.00000002.23 7274437.0000000001048000.00000 004.00000001.sdmp, 2327.2.dr	false		high
http://https://youtu.be/kaxh4pCyFss	wget.exe, 00000002.00000003.23 6779922.0000000001040000.00000 004.00000001.sdmp, 2327.2.dr	false		high
http://cps.root-x1.letsencrypt.org0	wget.exe, 00000002.00000003.23 6829486.0000000001049000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.i.lencr.org/0&	wget.exe, 00000002.00000003.23 6829486.0000000001049000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i.ytimg.com/vi/kaxh4pCyFss/hqdefault.jpg	wget.exe, 00000002.00000003.23 6779922.0000000001040000.00000 004.00000001.sdmp, 2327.2.dr	false		high
http://https://www.youtube.com/generate_204?cpn=	base[1].js.6.dr	false		high
http://https://youtube.com/api/drm/fps?ek=uninitialized	base[1].js.6.dr	false		high
http://cps.letsencrypt.org0	wget.exe, 00000002.00000003.23 6829486.0000000001049000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://www.googletraveladservices.com/travel/clk/pagead/conversion/	js[1].js.6.dr	false		high
http://www.bangthetable.com/	wget.exe, 00000002.00000003.23 6829486.0000000001049000.00000 004.00000001.sdmp, 2327.2.dr	false		high
http://https://www.youtube.com/embed/wtuxe7VPD3U?feature=oembed	wget.exe, 00000002.00000003.23 6779922.0000000001040000.00000 004.00000001.sdmp, 2327.2.dr, {E57A1C95-6806-11EB-90E5-ECF4BB570DC9}.dat.5.dr	false		high
http://cps.letsencrypt.org=	wget.exe, 00000002.00000003.23 6829486.0000000001049000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://youtube.com/yt/2012/10/10	base[1].js.6.dr	false		high
http://https://cct.google/taggy/agent.js	js[1].js.6.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontawesome.io/license	font-awesome.min[1].css.6.dr	false		high
http://https://i.ytimg.com/vi/KTb4H2DQcdc/hqdefault.jpg	wget.exe, 00000002.00000003.23 6779922.0000000001040000.00000 004.00000001.sdmp, 2327.2.dr	false		high
http://https://i.ytimg.com/vi/wtuxe7VPD3U/hqdefault.jpg	wget.exe, 00000002.00000003.23 6829486.0000000001049000.00000 004.00000001.sdmp, wget.exe, 0 0000002.00000003.236786957.000 0000001048000.00000004.0000000 1.sdmp, 2327.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s3-ap-southeast-2.amazonaws.com/ehq-static-assets/gt-simplified-us.js	wget.exe, 00000002.00000003.23 6829486.0000000001049000.00000 004.00000001.sdmp, 2327.2.dr	false		high
http://https://www.youtube.com/watch?v=wtuxe7VPD3U	wtuxe7VPD3U[1].htm.6.dr	false		high
http://https://www.google.%/ads/ga-audiences	analytics[1].js.6.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://s3-us-west-1.amazonaws.co	wget.exe, 00000002.00000003.23 6829486.0000000001049000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.youtube.com/videoplayback	base[1].js.6.dr	false		high
http://www.somervillebydesign.com	wget.exe, 00000002.00000003.23 6779922.0000000001040000.00000 004.00000001.sdmp, 2327.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.6.1/css/font-awesome.min.css	2327.2.dr	false		high
http://youtube.com/drm/2012/10/10	base[1].js.6.dr	false		high
http://https://i.ytimg.com/vi/Fn7Ou04BHvQ/hqdefault.jpg	wget.exe, 00000002.00000002.23 7274437.0000000001048000.00000 004.00000001.sdmp, 2327.2.dr	false		high
http://cps.root-x1.letsencrypt.org	wget.exe, 00000002.00000003.23 6829486.0000000001049000.00000 004.00000001.sdmp	false		high
http://https://youtu.be/VFxvnJ7wwwU	wget.exe, 00000002.00000003.23 6779922.0000000001040000.00000 004.00000001.sdmp, 2327.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.23.66	unknown	United States		15169	GOOGLEUS	false
54.177.210.138	unknown	United States		16509	AMAZON-02US	false
104.16.18.94	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	349157
Start date:	05.02.2021
Start time:	15:06:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	urldownload.jbs
Sample URL:	http://https://somervoice.somervillema.gov/novel-coronavirus-resources-for-businesses/widgets/16897/videos/2327
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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.win@7/21@13/3
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, 40.88.32.150, 13.88.21.125, 88.221.62.148, 23.210.248.85, 51.104.144.132, 92.122.213.247, 92.122.213.194, 216.58.207.170, 152.199.19.161, 20.54.26.129, 51.103.5.159, 216.58.207.174, 51.104.139.180, 172.217.20.238, 172.217.23.46, 172.217.23.78, 172.217.22.206, 172.217.22.238, 216.58.207.142, 84.53.167.113, 172.217.23.40, 142.250.74.206, 216.58.207.134, 172.217.23.67, 216.58.207.164 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, e15275.g.akamaiedge.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, emea1.wns.notify.trafficmanager.net, wildcard.weather.microsoft.com.edgekey.net, www.googletagmanager.com, www.google.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.google-analytics.com, fonts.googleapis.com, client.wns.windows.com, fs.microsoft.com, www-google-analytics.l.google.com, ie9comview.vo.msecnd.net, fonts.gstatic.com, www-googletagmanager.l.google.com, ris-prod.trafficmanager.net, tile-service.weather.microsoft.com, e1723.g.akamaiedge.net, static-doubleclick-net.l.google.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, youtube-ui.l.google.com, www3.l.google.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, translate.google.com, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net • Execution Graph export aborted for target wget.exe, PID 5924 because there are no executed function • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: https://somervoice.somervillema.gov/novel-coronavirus-resources-for-businesses/widgets/16897/videos/2327

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\DOMStore\DURNCK2N\www.youtube[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	52
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aK1r0aK1r0aK1r0aKb:JFK1rFK1rFK1rFKb
MD5:	770DA68A4DE2539B5002B44767396AF9
SHA1:	E3A118B288CF426DE3027EFCE38AE7241560EC4C
SHA-256:	908FB85A6D01001B303E1030664D87BA5D193B56CA17FB2116D8696196D4DA4A
SHA-512:	B4AA2726B958DDA17F5D1E5A2EB109825D9CDBDBA1E1CFDDBE55BA94D5B6ED5EE7DBB0F15538099C44F0CC80DB2AF445EA4F60D11FE767943FFF99AA495D922
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{E57A1C93-6806-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24152
Entropy (8bit):	1.7558522957006941
Encrypted:	false
SSDEEP:	48:Iw4Gcpr07GwpL2G/ap8rrGIpcKsGvnZpvKqGvHZp9KkGoGVuiqpvK1oGo4qVuRuL:rMZ0VZ02r9WAt6fCu7t6+uRuKWkupu6
MD5:	C938466E82959BF226BE2BA87AAF736E
SHA1:	0CFF088B55A6EC5AFBE25BB6F23B7571D87B3586
SHA-256:	1B0B9FCB81DDBFC9D1E8C9F8D7593A9FD40170A996EB067DE498475A82A683AF
SHA-512:	E2911D724C184AC20D2EE25C2FE6990CD8D5E264ED8F3A8CCBE9BD5374CB19529B229415CF70BD88D48AF01B000C9F95E342CAE1FAFF55FA650300BBFC9245EC
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\{E57A1C95-6806-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28818
Entropy (8bit):	2.132515440757445

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E57A1C95-6806-11EB-90E5-ECF4BB570DC9}.dat	
Encrypted:	false
SSDEEP:	192:rOZ1Qp6H+kHjgjHj2H3NWH0MHu2HDnxyBr:raqEHfHGH6H3kHhHVzx0
MD5:	D97F04B41C604A9740D8C7DEAC570D39
SHA1:	264EA7674BC23FF86A67E45B676B61D4B5A78AD6
SHA-256:	47B5748C2C4252C140F611F91BB3191ACC5FEB5FD936B21C41A4B4C932AD2673
SHA-512:	426ECB1A66FA8B20299D588E46D59F4BD04B2ECD7615ED0E2FEE68997931826E055DD3D51B75125146154608A8D58FB3982EE2FC165D524A9C72DFBC4F38194
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\KFOkCnqEu92Fr1Mu51xIIzQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21528, version 1.1
Category:	downloaded
Size (bytes):	21528
Entropy (8bit):	7.973887568128485
Encrypted:	false
SSDEEP:	384:uy/NCb8EbjU+Fos6gaUFZ3qR474EAqAG3w/Qpt/uxMsucMgwtDw031F:7/4zb7o6XqR4+3QptcuLg0w031F
MD5:	9680D5A0C32D2FD084E07BBC4C8B2923
SHA1:	8020B21E3DB55FF7A02100FAEBD92C2305E7156E
SHA-256:	2CFE69657C55133DAC6EA017B4452EFFF2131422ABD9E90500A072DF7CA5A9C8
SHA-512:	E19A498866F69F3D8136A65A5AB4E92CC047170673ED00B506E325165A84216267B9FEF1E5CFD66458E85ED820C12E9C345CEC9BEE4DE48E1C2E2B1A784F179
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOkCnqEu92Fr1Mu51xIIzQ.woff
Preview:	wOFF.....T.....GDEF.....G...d....GPOS.....hGSUB.....7b..OS/2.....R...`tq#gcmap.....L....cvt .....R...R..-.fpgm.....4....s...gasp...<..... ....glyf...H..@...o..Na.hdmx..M....g.....head..Mp...6...6...ehhea..M....".$...{hmtx..M....k.....1<.loca..P8.....6...maxp..R.... ... .name..R4.....:.post..S..... .a.dprep.. S$.....D..].x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x.....[....#N..m.m.m.mfm....SP..NuM..9]..=.U..!...[.....w...|.....^p....H.....;...).....;..EoDo. ...E.E.D...`.0.GG.aA.H.V.Mx\xA...../..d3.Eb_.J...R.^v.....\^ob.}.z..k.x).v$f$..O)+.2..*....y}6`C6b.6cs...l.....!.....<..|.|..|..|.|....o....l%.4.L.Sl.&C.6..!`...{...c..\.J.(.2.C....V. A..?.M<nG.....v..m.;..R.C..aj.H...=..{.>.:.....}i_Y.....:....o.&k..KY.2..6k....i]..{,.p}../.....VO3.o].fJ....R-TZ..;...RN..&V...C...3.?.....&..z.s&.D....r,.I...t.R..a$k..Mm..Y.U...+b.%kQ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19824, version 1.1
Category:	downloaded
Size (bytes):	19824
Entropy (8bit):	7.970306766642997
Encrypted:	false
SSDEEP:	384:ozNCb8EbW9Wg166uwroOp/taiap3K6MC4fsPPuzt+7NCXzS65XZELt:K4zbWcDVwt230hfs+x+Bb65X2
MD5:	BAFB105BAEB22D965C70FE52BA6B49D9
SHA1:	934014CC9BBE5883542BE756B3146C05844B254F
SHA-256:	1570F866BF6EAE82041E407280894A86AD2B8B275E01908AE156914DC693A4ED
SHA-512:	85A91773B0283E3B2400C7735275422284 78CC1B9E8AD8EA62435D705E98702A40BEDF26CB5B0900DD8FECC79F802B8C1839184E787D9416886DBC73DFF22A64
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxM.woff
Preview:	wOFF.....Mp.....P.....GDEF.....G...d....GPOS.....hGSUB.....7b..OS/2.....R...`tq#.cmap.....L....cvt .....T...T+...fpgm.....5....w.`.gasp...@..... ....glyf...L..:+..j.....hdmx..Fx...g.....head..F....6...6.j.zhhea..G.....$....hmtx..G8...]......Vlloca..I.....?.#.maxp..Kt.. ... .name..K.....t.U9.post..Ld..... .m.dprep..Lx.....I .f..x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x.....[....#N..m.m.m.mfm....SP..NuM..9]..=.U..!...[.....w...|.....^p....H.....;...).....;..EoDo....E.E.D.. .`.0.GG.aA.H.V.Mx\xA...../..d3.Eb_.J...R.^v.....\^ob.}.z..k.x).v$f$..O)+.2..*....y}6`C6b.6cs...l.....!.....<..|.|..|..|.|....o....l%.4.L.Sl.&C.6..!`...{...c..\.J.(.2.C....V.A..?.M<nG. .....v..m.;..R.C..aj.H...=..{.>.:.....}i_Y.....:....o.&k..KY.2..6k....i]..{,.p}../.....VO3.o].fJ....R-TZ..;...RN..&V...C...3.?.....&..z.s&.D....r,.I...t.R..a$k..Mm..Y.U...+b.%kQ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\www-embed-player[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	160750
Entropy (8bit):	5.575543050017186
Encrypted:	false
SSDEEP:	3072:UFSDCrQaZgYk9HLtT0NIvLT4uX2JtRi2/:HSZE9HLtT0N942Jtx/
MD5:	83891D3BDC2580542A5E8EA80319DDF4
SHA1:	8CCC6DCFAA3ED9E50AC1DC4E6F3154AF6F485A23

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\www-embed-player[1].js	
SHA-256:	9E7C514CB8307B6155F4172E355ECC822B8B41484C4B4F227B066CE2A0375580
SHA-512:	E8B944C7F077D7CA7CD4A8653450099A8EBED700661E3341160AF2587981DBEEF752BC0FA111D36E5015AB0640083267B647868837FAD6BC19ADDF5F64B90F7(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/s/player/4bc55fd6/www-embed-player.vflset/www-embed-player.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var m;function aa(a){var b=0;return function(){return b<a.length?{done:!1, value:a[b++]}:{done:!0}}}.var ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b] =c.value;return a};.function ca(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof glo bal&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}.var ea=ca(this);function t(a,b){if(b)a:{for(var c=ea,d=a.split("."),e=0;e<d.length-1;e++){var f=d[e];if(!(f in c))break a;c=c[f]}d=d[d.length-1];e=c[d];f=b(e);f!=e&&null!=f&&ba(c,d,{configurable:!0,writable:!0,value:f})}}.t("Sy mbol",function(a){function b(e){if(this instanceof b)throw new TypeError("Symbol is not a constructor");return new c("jscomp_symbol_"+(e||"")+"_"+d++,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\www-player[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	347347
Entropy (8bit):	5.242800843137371
Encrypted:	false
SSDEEP:	1536:gzu9IdYR9WDQI0irpHrp3/fn8MZv8M5q4ay95G0VXkMAXOP5kRrDJciM/By2N+CQ:gzu99F3zTg2yV1uD
MD5:	9CBA01AF120AA5B7997C053E42C6B53B
SHA1:	95688132A444ADA064A1544649A98AB69DE44ACF
SHA-256:	23D321BC61FB66783A98FA49AC1D6E18CA4E1CCBF4177D7983DB1DAFBC57BE22
SHA-512:	FD3CF5B2CD7CF3A37118087504DDF12C9AAF6611AD8742C3AD987E537C1F3BD8C9FCA4690570EF0DBBB0F5530C3EE00AD78F40517F3411D18A0FB1991D67E3 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/s/player/4bc55fd6/www-player.css
Preview:	.html5-video-player{position:relative;width:100%;height:100%;overflow:hidden;z-index:0;outline:0;font-family:"YouTube Noto",Roboto,Arial,Helvetica,sans-serif;color:#eee;t ext-align:left;direction:ltr;font-size:11px;line-height:1.3;-webkit-font-smoothing:antialiased;-webkit-tap-highlight-color:rgba(0,0,0,0);touch-action:manipulation;-ms-high-contrast-adjust:none}.html5-video-player:not(.ytp-transparent),.html5-video-player.unstarted-mode,.html5-video-player.ad-showing,.html5-video-player.ended-mode,.html5-video-player.ytp-fullscreen{background-color:#000}.ytp-big-mode{font-size:17px}.ytp-autohide{cursor:none}.html5-video-player a{color:inherit;text-decoration:none;-moz-transition:color .1s cubic-bezier(0.0,0.0,0.2,1);-webkit-transition:color .1s cubic-bezier(0.0,0.0,0.2,1);transition:color .1s cubic-bezier(0.0,0.0,0.2,1);outline:0}.html5-video-player a:hover{color:#fff;-moz-transition:color .1s cubic-bezier(0.4,0.0,1,1);-webkit-transition:color .1s cubic-bezier(0.4,0.0,1,1);transition:co

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ad_status[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	29
Entropy (8bit):	4.142295219190901
Encrypted:	false
SSDEEP:	3:lZOwFQvn:lQw6n
MD5:	1FA71744DB23D0F8DF9CCE6719DEFCB7
SHA1:	E4BE9B7136697942A036F97CF26EBAF703AD2067
SHA-256:	EED0DC1FDB5D97ED188AE16FD5E1024A5BB744AF47340346BE2146300A6C54B9
SHA-512:	17FA262901B608368EB4B70910DA67E1F11B9CFB2C9DC81844F55BEE1DB3EC11F704D81AB20F2DDA973378F9C0DF56EAAD8111F34B92E4161A4D194BA902F82 F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.doubleclick.net/instream/ad_status.js
Preview:	window.google_ad_status = 1;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\font-awesome.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	28759
Entropy (8bit):	4.756560965670852
Encrypted:	false
SSDEEP:	384:2u5yWeTUKW+KlkJ5de2UYmydfwYUas8l8yQ/8dw3G:Zlr+Klk3YlKfwYUf8l8yQ/e5
MD5:	89916FA773CE96569604016EF25CAB50
SHA1:	6F794D3B074C0275E3213AF5611A67817979E207
SHA-256:	B5D7707EA8FC00AAE40BF500AC7498D7F32F6B1BBFF7B4FDE976A40345EB5F9D
SHA-512:	4C40813D30F90DBF7B9E5B09FE018106FF492D7835EF661C1ADAE5FC71CCE31F56FBE3CF284A47B3AD68815778C76A264E0493D5D207A32D87798599CDC6731
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\font-awesome.min[1].css	
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.6.1/css/font-awesome.min.css
Preview:	/*!. * Font Awesome 4.6.1 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */@font-face{font-family:'FontAwesome';src:url('../fonts/fontawesome-webfont.eot?v=4.6.1');src:url('../fonts/fontawesome-webfont.eot?#iefix&v=4.6.1') format('embedded-opentype'),url('../fonts/fontawesome-webfont.woff2?v=4.6.1') format('woff2'),url('../fonts/fontawesome-webfont.woff?v=4.6.1') format('woff'),url('../fonts/fontawesome-webfont.ttf?v=4.6.1') format('truetype'),url('../fonts/fontawesome-webfont.svg?v=4.6.1#fontawesomeregular') format('svg');font-weight:normal;font-style:normal}.fa{display:inline-block;font:normal normal normal 14px/1 FontAwesome;font-size:inherit;text-rendering:auto;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.fa-lg{font-size:1.33333333em;line-height:.75em;vertical-align:-15%}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-fw{width:1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\js[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	99052
Entropy (8bit):	5.524436666588082
Encrypted:	false
SSDEEP:	1536:JOpsXGpm9O700z6fcJYo/+dEiWizqOUQoz+cxlEmvmh+AwAjL1z9ggKPe3PwMAfs:JOpsXQsO70qYg+siUiKenFjkj+
MD5:	266F19351DBEDB764BCCE628C5C3D106
SHA1:	03DF2213F3E09241C85F8B1B283586454AEB2CC3
SHA-256:	EE072DAD39A9FB932711DB264D8EE3A15B8FB8B04CCCE7293BA35EF89A1337CA
SHA-512:	05D111645D21E91241DA26B2264D3D82BBBFE0EAAB3A84E01C5DAAB6D4A8AAD2368B44D8E0E3D30BE67E514FA48555C10BFBA1CC530C29AEEE6B5DE02EDBDE1C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagmanager.com/gtag/js?id=UA-13225056-7
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"1",. . "macros":[{. "function":"__e". },{. "function":"__cid". }],."tags":[{. "function":"__rep",. "once_per_event":true,. "vtp_containerId":["macro",1],. "tag_id":1. }],. "predicates":[{. "function":"_eq",. "arg0":["macro",0],. "arg1":"gtm.js". }],. "rules":[. [["if",0],["add",0]]].},."runtime":[].....};./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var aa,ba=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},ca=function(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:ba(a)}},ha="function"==typeof Object.create?Object.create:function(a){var b=function(){};b.prototype=a;return new b},ja;.if("function"==typeof Object.setPrototypeOf)ja=Object.setPrototypeOf;else{var ka;a:{var la={a:!0},ma={};t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\base[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1569985
Entropy (8bit):	5.585596091283248
Encrypted:	false
SSDEEP:	12288:NhwjbmeWGR10wMSB0joXCadTa+hJNMdvzk6P:NmjbmeWGR1//B0joyadTaUwbx
MD5:	51F9BFFE25EA3744AD0C1DA159EBACC3
SHA1:	4976DEFC0111939E42341CFCEA9FAFAA3CCADAAA
SHA-256:	2E2F083236148C0530C60F772060FA6E3BE4200D1968AD9038CD51DCD48E8A5E
SHA-512:	81B9C7198AC0CC0BA0C83FAE51C640F07107AA5E4C545C499877EF17A884B185A10DC6C4C290F28316D5EE33A2B132CA7D3D42810658E681A211C02C7B38768
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/s/player/4bc55fd6/player_ias.vflset/en_US/base.js
Preview:	var _yt_player={};(function(g){var window=this;/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var ba,da,maa,ha,ia,la,pa,qa,ra,w,sa,ta,naa,taa,ua,va,uaa,wa,xa,ya,Aa,Ba,Ca,Ga,Ea,Ja,Ka,xaa,yaa,Ta,Ua,Va,zaa,Aaa,Wa,Baa,Ya,Za,Caa,Daa,ab,ib,Eaa,pb,qb,Faa,wb,sb,Gaa,tb,Haa,Iaa,Jaa,Eb,Gb,Ib,Lb,Nb,Ob,Rb,Xb,Zb,bc,cc,gc,ic,jc,Maa,kc,lc,mc,vc,wc,yc,Dc,Jc,Kc,Oc,Mc,Qaa,Taa,Uaa,Vaa,Uc,Vc,Xc,Wc,Zc,bd,Waa,Xaa,ad,Yaa,hd,id,jd,kd,nd,pd,qd,$aa,rd,sd,wd,xd,Cd,Dd,Ed,Fd,Gd,Hd,Jd,Ld,Od,Qd,Rd,Sd,bba,Td,Ud,Vd,Wd,Zd,$d,ge,ie,le,pe,qe,ve,we,ze,xe,Be,Ee,De,Ce,gba,ne,Se,Qe,Re,Ue,Te,me,Ve,We,iba,$e,bf,Ze,df,ef,hf,jf,kf,lf,.mf,nf,jba,uf,qf,Gf,kba,Kf,Mf,Rf,Sf,Tf,Uf,Vf,Xf,Wf,Yf,Zf,nba,pba,qba,sba,dg,eg,fg,hg,ig,jg,lg,kg,uba,tba,ng,og,vba,pg,wba,qg,xba,rg,tg,vg,Cg,Dg,Gg,yba,Jg,lg,Kg,zba,Sg,Aba,Tg,Vg,Wg,Xg,Yg,Zg,Bba,$g,ah,bh,ch,dh,eh,fh,Cba,gh,hh,ih,Dba,Eba,jh,lh,kh,nh,oh,rh,ph,Gba,qh,sh,Iba,Hba,Jba,yh,Kba,Ah,Bh,Ch,zh,Dh,Lba,Eh,Mba,Nba,Hh,Pba,Ih,Jh,Kh,Qba,Mh,Oh,Rh,Uh,Wh,Th,Sh,Xh,Rba,Yh,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\fetch-polyfill[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Pascal source, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8543
Entropy (8bit):	5.238064281324506
Encrypted:	false
SSDEEP:	192:oQHdiEslZc0rsNYNU5mSJHqI03aej6tZoaMLQO/x5/P80+HcW:ocHslLsP5muHqI0Jj6tZcUO/x5+V
MD5:	04E3CC8A9641B3F9F9C9370F4E9B5BDD
SHA1:	9602A891F583094BB04FD407B253ABCAFFB8C8D0
SHA-256:	DE6C4FFA2BD9FD283610E28D0DB2EC48607AAB39D213A51AEF248673A0A7E980
SHA-512:	58942BCC0F39D620A475B65C1AEB4F18872F68F22C89DEC076906A0DB8BC2B7CCA9357710A7824A0FA7404FF73F41013AECA34609CAACD2187414F7BD0D490D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\fetch-polyfill[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/yts/jsbin/fetch-polyfill-vfl6MZH8P/fetch-polyfill.js
Preview:	/*.. Copyright (c) 2014-2016 GitHub, Inc... Permission is hereby granted, free of charge, to any person obtaining. a copy of this software and associated documentation fi les (the. "Software"), to deal in the Software without restriction, including. without limitation the rights to use, copy, modify, merge, publish,. distribute, sublicense, and/or s ell copies of the Software, and to. permit persons to whom the Software is furnished to do so, subject to. the following conditions:.. The above copyright notice and this permission notice shall be. included in all copies or substantial portions of the Software... THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,. EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF. MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND. NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE. LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETH ER IN AN ACTION. OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\KFOjCnqEu92Fr1Mu51S7ACc6CsI[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21564, version 1.1
Category:	downloaded
Size (bytes):	21564
Entropy (8bit):	7.9688026243536
Encrypted:	false
SSDEEP:	384:bc6bX9TFqgFUvxQi0W1jHYHwnSthN/yiJsMw52R5oBAvhPFx466gfwu5:bcCV4aUlxHSw8ZyixnFP3N6U5
MD5:	FFCC050B2D92D4B14A4FCB527EE0BCC8
SHA1:	DE3033F27DB6BBDA89A0E6F16EC51E8C877739AB
SHA-256:	C8912EBD82B4DF2EB87E37B1F66432FA2186182E08BB8A533BA4C2DF6CE67FBA
SHA-512:	7D517BB33DE3D088B8EE4EC9250AB1645CF76B35B25F57C004BF82B5A9A30C15252C865765EFFD4679A68ACDF6EFB89E4B0319283914880935D8D1AC823FE65
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOjCnqEu92Fr1Mu51S7ACc6CsI.woff
Preview:	wOFF.....T<.....GDEF.....G...d....GPOS.....GSUB.....7b..OS/2.....Q...`t.#ycmap...4.....L....cvt .....\...\1..Mfpgm...@...2.....$.gasp...t..... ....glyf.....@...p.N..Hhdmx..M(...f.....head..M....6...6...vhhea..M....'...$....hmtx..M....k.....3.loca..PX.....G.*"maxp..R4... ... .name..RT.....!.>gpost..S0..... .a.dprep.. SH.....X9..x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x...pfK.G...1.c>..`9..m<+;..m.x...bg.M.T...O.....l...XU.../{.[_..W....c._..72.. ." z.+..F.....&.& ...`e..T].....K=..K2S....q..d...xf.$~i..$?.d..dU.....@R-/LMO-J6...[]..Z..O.C_."lf..d....fS....$d.G>eL`....Tf1.....9.c>..`1.TR..x./d-.....q.....7....{...v.....!.....1.QG=.4.D3-..F;=. .1'.'q.rw...9..e!.....Q....f.....qV.n.h.V.Z]..B..C.[B...V.....v...o.w.{...w..zRO.i=..._.....-.m....].=...[...(1.(.#.....O0/.0?..04rL.G.9.....i6..l..|.(o.....\|$,..{|&|....YJ...x.e8B.#..t;R8.{+....\=.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\KFOlCnqEu92Fr1MmEU9fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20012, version 1.1
Category:	downloaded
Size (bytes):	20012
Entropy (8bit):	7.966842359681559
Encrypted:	false
SSDEEP:	384:Yc6bX9TagDCXKqs4+W5XVgaflKHjsGdZtlh3K/qzWz/scZpuB:YcCVaeCaF4ea9KHYQZtlh3Kgy4B
MD5:	DE8B7431B74642E830AF4D4F4B513EC9
SHA1:	F549F1FE8A0B86EF3FBDCB8D508440AFF84C385C
SHA-256:	3BFE46BB1CA35B205306C5EC664E99E4A816F48A417B6B42E77A1F43F0BC4E7A
SHA-512:	57D3D4DE3816307ED954B796C13BFA34AF22A46A2FEA310DF90E966301350AE8ADAC62BCD2ABF7D7768E6BDCBB3DFC5069378A728436173D07ABFA483C1025 AC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc-.woff
Preview:	wOFF.....N,.....GDEF.....G...d....GPOS.....GSUB.....7b..OS/2.....R...`t.#.cmap...4.....L....cvt .....\...\1..Kfpgm...@...2.....$.gasp...t.....glyf.. ....:..j.'..hdmx..G,...f.....head..G....6...6...rhhea..G.....$....hmtx..G....a.....MOloca..JP.....\v@zmaxp..L,... ... .name..LL.....:.post..M(..... .m.dprep..M<.....S...)x...1.. P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x...pfK.G...1.c>..`9..m<+;..m.x...bg.M.T...O.....l...XU.../{.[_..W....c._..72.. ." z.+..F.....&.&...`e..T].....K=..K2 S....q..d...xf.$~i..$?.d..dU.....@R-/LMO-J6...[]..Z..O.C_."lf..d....fS....$d.G>eL`....Tf1.....9.c>..`1.TR..x./d-.....q.....7....{...v.....!.....1.QG=.4.D3-..F;=..1'.'q.rw...9..e!.....Q....f.. ....qV.n.h.V.Z]..B..C.[B...V.....v...o.w.{...w..zRO.i=..._.....-.m....].=...[...(1.(.#.....O0/.0?..04rL.G.9.....i6..l..|.(o.....\|$,..{|&|....YJ...x.e8B.#..t;R8.{+....\=.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	47051
Entropy (8bit):	5.516264124030958
Encrypted:	false
SSDEEP:	768:ryOveCSBZfsnt5XqY/yPndFTkoWY3SoavqVy2rlebYUDTJC6g0stZm:ryJNDfs5hYdFTwY3SorSg0su
MD5:	53EE95B384D866E8692BB1AEF923B763
SHA1:	A82812B87B667D32A8E51514C578A5175EDD94B4
SHA-256:	E441C3E2771625BA05630AB464275136A82C99650EE2145CA5AA9853BEDEB01B
SHA-512:	C1F98A09A102BB1E87BFDF825A725B0E2CC1DBEDB613D1BD9E8FD9D8FD8B145104D5F4CACA44D96DB14AC20F2F51B4C653278BFC87556E7F00E48A5FA6231 AD

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\analytics[1].js</th></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://www.google-analytics.com/analytics.js</td></tr>
<tr><td>Preview:</td><td>(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var l=this||self,m=function(a,b){a=a.split(".");var c=l;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},r=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var t=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var u=window,v=document,w=function(a,b){v.addEventListener?v.addEventListener(a,b,!1):v.attachEvent&&v.attachEvent("on"+a,b)};var x={},y=function(){x.TAGGING=x.TAGGING||[];x.TAGGING[1]=!0};var z=/:[0-9]+$/,A=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponent(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},D=function(a,b){b&&(b=String(b).toLowerCase());if("p</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\wtuxe7VPD3U[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	50374
Entropy (8bit):	5.898870077721632
Encrypted:	false
SSDEEP:	768:d7aCaR6oVfOmN4D6p1NIKoH0v+my3KPuvs15E/dnUVJVY6iyrrmo:eNVc6z1tRbr1
MD5:	5438C2496A7A9ADCA89808E501CD652E
SHA1:	A3C75F818415D36365E9E27F567C0DAD700E5F52
SHA-256:	7965B07B1D625D8AFE62781C68691D08FA1678474279C951D00CF8DF998652EA
SHA-512:	839F90D83DD80FA78FB5CC5D89815CB3EB0562713E558E22AC7E825E533FF3884DCF6D8F5291A212620DD9DBB0A040DD1DC204D6E16CDA0EABCDDD3A21909 46
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/embed/wtuxe7VPD3U?feature=oembed
Preview:	<!DOCTYPE html> <html lang="en" dir="ltr" data-cast-api-enabled="true">.<head><meta name="viewport" content="width=device-width, initial-scale=1"><style name="www-roboto" >@font-face{font-family:'Roboto';font-style:italic;font-weight:500;src:url(//fonts.gstatic.com/s/roboto/v18/KFOjCnqEu92Fr1Mu51S7ACc6CsI.woff)format('woff');}@font-face{font-family:'Roboto';font-style:italic;font-weight:400;src:url(//fonts.gstatic.com/s/roboto/v18/KFOkCnqEu92Fr1Mu51xIIzQ.woff)format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxM.woff)format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:500;src:url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc-.woff)format('woff');}</style><script name="www-roboto" >if (document.fonts && document.fonts.load) {document.fonts.load("400 10pt Roboto", "");document.fonts.load("500 10pt Roboto", "");}</script> <link rel="stylesheet" href="/s/player/4

C:\Users\user\AppData\Local\Temp\~DF945E8E7F0625E9E8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12965
Entropy (8bit):	0.41873979718625315
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRVi9l8fRVS9lTqVv5jWn1AWn/z5ujWU+T:c9lLh9lLh9lIn9lIn9lo09loE9lWN8b1
MD5:	71A74E90E309C91710F49A6F4582862F
SHA1:	43EC38C98AE7F1A852EEEEB094771D48D2617215
SHA-256:	F3950D2F81BA7D91C7B6D43B98F1BD7E96228CBE73AC79125917B78D2D1EFECF
SHA-512:	81B24A57DC6A0CCBC860B7134027FE20F1D312C7E50467EA817C23CD47CB920F915283FF16B1DDD37EDE3CF869A6A97CDD6E11A18B7E900994A2BCFDC9370 18
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFA17A083F6A4A7026.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	37471
Entropy (8bit):	0.811720869166821
Encrypted:	false
SSDEEP:	96:kBqoxKAHzHySHRSHzHoHuHkH1HeHJuiJPPTQ:kBqoxKAHzH3HUHzHoHuHkH1HeHJh
MD5:	E31D22F64BAA17C9D73309218BCE29ED
SHA1:	23774B9B6F9DD1E10E05A9B5A1DEEF80BAD19658
SHA-256:	85DF6C80DA28B185B256C887329A48D8B063537F26CC348DB1E803B91AD0B244
SHA-512:	C08B62EA27699DFB8A08D402AF8936B2660BBC22412498A88B0048CDB1CE65EA39A0500FB27FECC70B2A8C1841CD8F62753E8DACFAC411E1400AE7602316D8 3

C:\Users\user\AppData\Local\Temp\~DFA17A083F6A4A7026.TMP	
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):	629
Entropy (8bit):	5.060514363988684
Encrypted:	false
SSDEEP:	12:HVuMUeHrCVSKYJfblfCglT1De5RhKkk1DbV3JRbKsSD0AiV3JRbKsSOa:1ZUmb9JfhfCYxePgJ1NPbVAQPbVS
MD5:	AD92A78AE4A2A6D637654650CD756167
SHA1:	978EBE2B58DFA3551A1C963D701B44154092EA93
SHA-256:	9358FDAC43E8017A809573536E44CBC26CAB4B848E5AADD6EC6227E31904457D
SHA-512:	64336607057312FF83ADB3DE813EEB9ED432BBF0D2C07D65AD4CF468E0CE7E4E6703B88EBC9507FC4733FB930B657628B62FB4CCAD5760B5C24B178E455B11D 5
Malicious:	false
Reputation:	low
Preview:	--2021-02-05 15:07:16-- https://somervoice.somervillema.gov/novel-coronavirus-resources-for-businesses/widgets/16897/videos/2327..Resolving somervoice.somervil lema.gov (somervoice.somervillema.gov)... 54.177.210.138..Connecting to somervoice.somervillema.gov (somervoice.somervillema.gov)|54.177.210.138|:443... connect ed...HTTP request sent, awaiting response... 200 OK..Length: unspecified [text/html]..Saving to: 'C:/Users/user/Desktop/download/2327'.... 0K .... 1.78M=0.02s....2021-02-05 15:07:18 (1.78 MB/s) - 'C:/Users/user/Desktop/download/2327' saved [30490]....

C:\Users\user\Desktop\download\.wget-hsts	
Process:	C:\Windows\SysWOW64\wget.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	186
Entropy (8bit):	5.145345546398632
Encrypted:	false
SSDEEP:	3:SY2FyFARLlbwFAM9CxnOLVFzDwIVhyyJxWQ5RdkA8dyTWlx1YonBov:SYeRLlbA0noH9VhyyJQQ5oA8UaiCBy
MD5:	F1F9F3AEFB2A41A2179A6D15844A6B72
SHA1:	7E24449947EA6826EF6F5FBB8E8C95E99A86CA5B
SHA-256:	FBF6A88139E77DCA14227B7B38C85E45B8374CF777BB3B8E7AA7A941F23FA3C4
SHA-512:	257033A9CADAAAF6700D012D737869F6CE2641D768A0D38897B841F1B4E201E595526A843C7B5AD6770413A9C9B2C28CEC03B35E492567F683C1858157D6E130
Malicious:	false
Reputation:	low
Preview:	# HSTS 1.0 Known Hosts database for GNU Wget...# Edit at your own risk...# <hostname>.<port>.<incl. subdomains>.<created>.<max-age>..somervoice.somerv illema.gov.0.1.1612566438.31536000..

C:\Users\user\Desktop\download\2327	
Process:	C:\Windows\SysWOW64\wget.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	30490
Entropy (8bit):	5.332276673228413
Encrypted:	false
SSDEEP:	768:nN/HvB0lKJmjbMMVelA69pqLQkgoHNo95OWrb:nlOlKJmjbMte8sLQkgONo95OWrb
MD5:	F2F1E74AAAFA78664323227DADD94089
SHA1:	E5973248182FE41A2F7DA9E01DCCDB4DE546F014
SHA-256:	A8D20DAE71CAA41D107710D49150ACFD636633A64FAF1F38BF41EACD2136A540
SHA-512:	FDC9041518C841F6DA80169DB2F851427F641C9096F8B348D7BECE343C1A92ED04B93C72068E9BDFCD5214BEB5163A63904A0E5658550E73D4C8D712C928788
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html lang='en-US' xml:lang='en-US'>.<head>.<meta content='IE=edge' http-equiv='X-UA-Compatible'>.<meta content='text/html; charset=utf-8' http- equiv='Content-type'>.<meta content='width=device-width' name='viewport'>.<link href='https://s3-us-west-1.amazonaws.com/ehq-production-us-california/8cfcc1570c 81e97a242433b94052e3e65b3cb2c7/image_stores/favicons/000/002/489/original/SomerVoice_Favicon.png?1568919813' rel='icon' type='image/ico'>..<meta name="csrf- param" content="authenticity_token" />.<meta name="csrf-token" content="rt1Jznfq0uCCm+nf5MsfZ3MQ/aC2xV1TIkl7Ffzd4U8sTRx3lPTB5e146UjBVuAkpxdGtyWp gi0wVdaVkd42eA==" />...<title>.Novel Coronavirus Resources for Businesses. | SomerVoice.</title>.<span data-reporting-params='{"authenticity_token":&q uot;cMq9flDYpHpTwfnU+EJvX3Qol0Qp6z/4oRpm4+xTFnfyWujHs8a3fzwi+UPd35AcoC8sU7qH4IazBstjgVDBQA==","referrer":null,"type&quot ;:"InformedVisit","logger":{"page_id":"5265&q

Static File Info

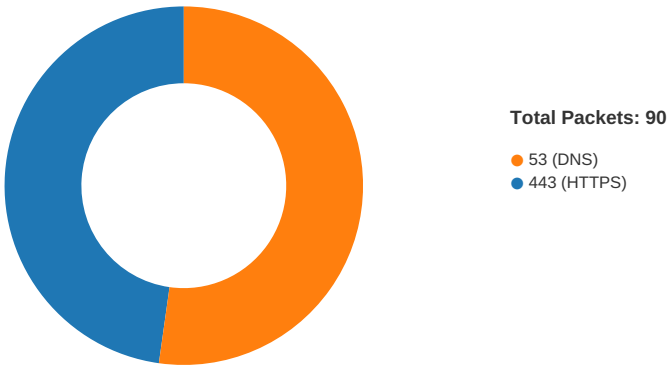
No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/05/21-15:07:26.634075	ICMP	466	ICMP L3retriever Ping			192.168.2.5	143.204.15.131
02/05/21-15:07:26.634075	ICMP	384	ICMP PING			192.168.2.5	143.204.15.131
02/05/21-15:07:26.679233	ICMP	408	ICMP Echo Reply			143.204.15.131	192.168.2.5
02/05/21-15:07:49.094460	ICMP	466	ICMP L3retriever Ping			192.168.2.5	216.58.207.170
02/05/21-15:07:49.094460	ICMP	384	ICMP PING			192.168.2.5	216.58.207.170
02/05/21-15:07:49.136350	ICMP	408	ICMP Echo Reply			216.58.207.170	192.168.2.5
02/05/21-15:08:11.527840	ICMP	466	ICMP L3retriever Ping			192.168.2.5	216.58.207.174
02/05/21-15:08:11.527840	ICMP	384	ICMP PING			192.168.2.5	216.58.207.174
02/05/21-15:08:11.569121	ICMP	408	ICMP Echo Reply			216.58.207.174	192.168.2.5
02/05/21-15:08:33.833431	ICMP	466	ICMP L3retriever Ping			192.168.2.5	143.204.15.81
02/05/21-15:08:33.833431	ICMP	384	ICMP PING			192.168.2.5	143.204.15.81
02/05/21-15:08:33.877435	ICMP	408	ICMP Echo Reply			143.204.15.81	192.168.2.5
02/05/21-15:08:56.206196	ICMP	466	ICMP L3retriever Ping			192.168.2.5	104.16.18.94
02/05/21-15:08:56.206196	ICMP	384	ICMP PING			192.168.2.5	104.16.18.94
02/05/21-15:08:56.250712	ICMP	408	ICMP Echo Reply			104.16.18.94	192.168.2.5

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 15:07:17.234325886 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:17.433872938 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:17.434001923 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:17.437586069 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:17.636428118 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:17.643752098 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:17.643841028 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:17.643906116 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:17.644006014 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:17.651972055 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:17.852556944 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:17.855004072 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:18.095331907 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.779860973 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.779933929 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.779982090 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.780024052 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.780023098 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:18.780066013 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.780090094 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:18.780108929 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.780148029 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.780170918 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:18.780328989 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.780375004 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.780399084 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:18.780417919 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.780463934 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:18.980484962 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.980554104 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.980590105 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.980623007 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.980654001 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.980664015 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:18.980685949 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.980699062 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:18.980716944 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.980747938 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.980752945 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:18.980781078 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.980812073 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:18.980818033 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.980850935 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.980866909 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:18.980880022 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.980911970 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.980927944 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:18.980946064 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.980971098 CET	443	49719	54.177.210.138	192.168.2.5
Feb 5, 2021 15:07:18.981021881 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:19.052896023 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:19.511015892 CET	49719	443	192.168.2.5	54.177.210.138
Feb 5, 2021 15:07:47.969913960 CET	49732	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:47.970504999 CET	49733	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.015928984 CET	443	49732	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.015958071 CET	443	49733	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.016436100 CET	49733	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.017091990 CET	49732	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.025310993 CET	49733	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.028707027 CET	49732	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.069597006 CET	443	49733	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.075431108 CET	443	49732	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.075465918 CET	443	49732	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.075481892 CET	443	49732	104.16.18.94	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 15:07:48.075500011 CET	443	49733	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.075515985 CET	443	49733	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.075551033 CET	49732	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.075584888 CET	49733	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.078671932 CET	49732	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.118846893 CET	49732	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.118983984 CET	49733	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.125889063 CET	49733	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.127099037 CET	49733	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.127728939 CET	49732	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.163048983 CET	443	49732	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.163070917 CET	443	49733	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.163397074 CET	443	49733	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.163758039 CET	49733	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.163779974 CET	443	49733	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.163921118 CET	49733	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.164876938 CET	443	49732	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.164891005 CET	443	49732	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.165201902 CET	49732	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.166642904 CET	49733	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.168697119 CET	49732	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.170252085 CET	443	49733	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.171236038 CET	443	49733	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.171724081 CET	443	49732	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.171741962 CET	443	49732	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.171878099 CET	49732	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.172256947 CET	443	49733	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.173785925 CET	49733	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.253895044 CET	443	49732	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.257519007 CET	443	49733	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.296605110 CET	443	49733	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.296655893 CET	443	49733	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.296701908 CET	49733	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.296726942 CET	49733	443	192.168.2.5	104.16.18.94
Feb 5, 2021 15:07:48.296744108 CET	443	49733	104.16.18.94	192.168.2.5
Feb 5, 2021 15:07:48.296782017 CET	443	49733	104.16.18.94	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 15:07:11.764857054 CET	63183	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:11.811811924 CET	53	63183	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:12.898927927 CET	60151	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:12.950552940 CET	53	60151	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:13.766228914 CET	56969	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:13.821501970 CET	53	56969	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:15.069468975 CET	55161	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:15.124907970 CET	53	55161	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:15.927023888 CET	54757	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:15.973674059 CET	53	54757	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:17.141604900 CET	49992	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:17.226108074 CET	53	49992	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:21.032305002 CET	60075	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:21.091984987 CET	53	60075	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:22.374574900 CET	55016	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:22.446049929 CET	53	55016	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:26.574177980 CET	64345	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:26.632848978 CET	53	64345	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:31.823400021 CET	57128	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:31.885289907 CET	53	57128	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:40.430713892 CET	54791	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:40.477413893 CET	53	54791	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:43.970624924 CET	50463	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:44.030214071 CET	53	50463	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 15:07:47.870496988 CET	50394	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:47.898520947 CET	58530	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:47.936458111 CET	53	50394	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:47.950846910 CET	53	58530	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:49.026160002 CET	53813	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:49.084217072 CET	53	53813	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:51.063024998 CET	63732	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:51.120110989 CET	53	63732	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:52.040589094 CET	57344	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:52.073610067 CET	63732	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:52.089591980 CET	53	57344	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:52.122888088 CET	53	63732	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:53.055794001 CET	57344	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:53.073965073 CET	63732	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:53.102307081 CET	53	57344	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:53.125210047 CET	53	63732	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:54.056523085 CET	57344	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:54.104392052 CET	53	57344	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:55.072053909 CET	63732	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:55.120407104 CET	53	63732	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:56.072550058 CET	57344	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:56.123999119 CET	53	57344	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:57.659216881 CET	54450	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:57.722939968 CET	53	54450	8.8.8.8	192.168.2.5
Feb 5, 2021 15:07:59.087770939 CET	63732	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:07:59.143445969 CET	53	63732	8.8.8.8	192.168.2.5
Feb 5, 2021 15:08:00.072258949 CET	57344	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:08:00.129827023 CET	53	57344	8.8.8.8	192.168.2.5
Feb 5, 2021 15:08:01.758694887 CET	59261	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:08:01.808022976 CET	53	59261	8.8.8.8	192.168.2.5
Feb 5, 2021 15:08:03.219429016 CET	57151	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:08:03.266285896 CET	53	57151	8.8.8.8	192.168.2.5
Feb 5, 2021 15:08:07.014214039 CET	59413	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:08:07.080498934 CET	53	59413	8.8.8.8	192.168.2.5
Feb 5, 2021 15:08:07.742432117 CET	60516	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:08:07.801554918 CET	53	60516	8.8.8.8	192.168.2.5
Feb 5, 2021 15:08:10.302572966 CET	51649	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:08:10.369622946 CET	53	51649	8.8.8.8	192.168.2.5
Feb 5, 2021 15:08:11.465857983 CET	65086	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:08:11.525525093 CET	53	65086	8.8.8.8	192.168.2.5
Feb 5, 2021 15:08:32.599138975 CET	56432	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:08:32.661825895 CET	53	56432	8.8.8.8	192.168.2.5
Feb 5, 2021 15:08:33.773889065 CET	52929	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:08:33.831979990 CET	53	52929	8.8.8.8	192.168.2.5
Feb 5, 2021 15:08:42.363190889 CET	64317	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:08:42.414575100 CET	53	64317	8.8.8.8	192.168.2.5
Feb 5, 2021 15:08:54.905102015 CET	61004	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:08:54.951648951 CET	53	61004	8.8.8.8	192.168.2.5
Feb 5, 2021 15:08:54.961630106 CET	56895	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:08:55.031986952 CET	53	56895	8.8.8.8	192.168.2.5
Feb 5, 2021 15:08:56.079540014 CET	62372	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:08:56.128251076 CET	53	62372	8.8.8.8	192.168.2.5
Feb 5, 2021 15:09:04.572551012 CET	61515	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:09:04.633744001 CET	53	61515	8.8.8.8	192.168.2.5
Feb 5, 2021 15:09:17.297841072 CET	56675	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:09:17.367232084 CET	53	56675	8.8.8.8	192.168.2.5
Feb 5, 2021 15:09:17.704849958 CET	57172	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:09:17.751698017 CET	53	57172	8.8.8.8	192.168.2.5
Feb 5, 2021 15:09:19.678814888 CET	55267	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:09:19.725985050 CET	53	55267	8.8.8.8	192.168.2.5
Feb 5, 2021 15:09:19.806108952 CET	50969	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:09:19.818259954 CET	64362	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:09:19.872160912 CET	53	50969	8.8.8.8	192.168.2.5
Feb 5, 2021 15:09:19.876028061 CET	53	64362	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2021 15:09:21.981621027 CET	54766	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:09:22.033730984 CET	53	54766	8.8.8.8	192.168.2.5
Feb 5, 2021 15:09:22.591409922 CET	61446	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:09:22.596565962 CET	57515	53	192.168.2.5	8.8.8.8
Feb 5, 2021 15:09:22.657424927 CET	53	61446	8.8.8.8	192.168.2.5
Feb 5, 2021 15:09:22.664328098 CET	53	57515	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Feb 5, 2021 15:08:56.206196070 CET	192.168.2.5	104.16.18.94	4f58		Echo
Feb 5, 2021 15:08:56.250711918 CET	104.16.18.94	192.168.2.5	5758		Echo Reply

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 5, 2021 15:07:17.141604900 CET	192.168.2.5	8.8.8.8	0x8369	Standard query (0)	somervoice.somervillema.gov	A (IP address)	IN (0x0001)
Feb 5, 2021 15:07:22.374574900 CET	192.168.2.5	8.8.8.8	0x5423	Standard query (0)	d2gu4vothxmtom.cloudfront.net	A (IP address)	IN (0x0001)
Feb 5, 2021 15:07:26.574177980 CET	192.168.2.5	8.8.8.8	0x3af7	Standard query (0)	d2gu4vothxmtom.cloudfront.net	A (IP address)	IN (0x0001)
Feb 5, 2021 15:07:47.898520947 CET	192.168.2.5	8.8.8.8	0x8443	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Feb 5, 2021 15:08:32.599138975 CET	192.168.2.5	8.8.8.8	0xb0f6	Standard query (0)	d2gu4vothxmtom.cloudfront.net	A (IP address)	IN (0x0001)
Feb 5, 2021 15:08:33.773889065 CET	192.168.2.5	8.8.8.8	0x4fdb	Standard query (0)	d2gu4vothxmtom.cloudfront.net	A (IP address)	IN (0x0001)
Feb 5, 2021 15:08:54.905102015 CET	192.168.2.5	8.8.8.8	0xf486	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Feb 5, 2021 15:08:54.961630106 CET	192.168.2.5	8.8.8.8	0x2789	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)
Feb 5, 2021 15:08:56.079540014 CET	192.168.2.5	8.8.8.8	0xd144	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Feb 5, 2021 15:09:19.678814888 CET	192.168.2.5	8.8.8.8	0x9e16	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Feb 5, 2021 15:09:19.806108952 CET	192.168.2.5	8.8.8.8	0x29c2	Standard query (0)	static.doubleclick.net	A (IP address)	IN (0x0001)
Feb 5, 2021 15:09:22.591409922 CET	192.168.2.5	8.8.8.8	0x5ac	Standard query (0)	i.ytimg.com	A (IP address)	IN (0x0001)
Feb 5, 2021 15:09:22.596565962 CET	192.168.2.5	8.8.8.8	0x141	Standard query (0)	yt3.ggpht.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 5, 2021 15:07:17.226108074 CET	8.8.8.8	192.168.2.5	0x8369	No error (0)	somervoice.somervillema.gov	platform.us.engagementhq.com		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 15:07:17.226108074 CET	8.8.8.8	192.168.2.5	0x8369	No error (0)	platform.us.engagementhq.com	or-nlb-v00-b47a3d3821d0abbe.elb.us-west-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 15:07:17.226108074 CET	8.8.8.8	192.168.2.5	0x8369	No error (0)	or-nlb-v00-b47a3d3821d0abbe.elb.us-west-1.amazonaws.com		54.177.210.138	A (IP address)	IN (0x0001)
Feb 5, 2021 15:07:22.446049929 CET	8.8.8.8	192.168.2.5	0x5423	No error (0)	d2gu4vothxmtom.cloudfront.net		143.204.15.131	A (IP address)	IN (0x0001)
Feb 5, 2021 15:07:22.446049929 CET	8.8.8.8	192.168.2.5	0x5423	No error (0)	d2gu4vothxmtom.cloudfront.net		143.204.15.81	A (IP address)	IN (0x0001)
Feb 5, 2021 15:07:22.446049929 CET	8.8.8.8	192.168.2.5	0x5423	No error (0)	d2gu4vothxmtom.cloudfront.net		143.204.15.197	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 5, 2021 15:07:22.446049929 CET	8.8.8.8	192.168.2.5	0x5423	No error (0)	d2gu4vothx mtom.cloud front.net		143.204.15.206	A (IP address)	IN (0x0001)
Feb 5, 2021 15:07:26.632848978 CET	8.8.8.8	192.168.2.5	0x3af7	No error (0)	d2gu4vothx mtom.cloud front.net		143.204.15.131	A (IP address)	IN (0x0001)
Feb 5, 2021 15:07:26.632848978 CET	8.8.8.8	192.168.2.5	0x3af7	No error (0)	d2gu4vothx mtom.cloud front.net		143.204.15.81	A (IP address)	IN (0x0001)
Feb 5, 2021 15:07:26.632848978 CET	8.8.8.8	192.168.2.5	0x3af7	No error (0)	d2gu4vothx mtom.cloud front.net		143.204.15.197	A (IP address)	IN (0x0001)
Feb 5, 2021 15:07:26.632848978 CET	8.8.8.8	192.168.2.5	0x3af7	No error (0)	d2gu4vothx mtom.cloud front.net		143.204.15.206	A (IP address)	IN (0x0001)
Feb 5, 2021 15:07:47.950846910 CET	8.8.8.8	192.168.2.5	0x8443	No error (0)	cdnjs.clou dflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Feb 5, 2021 15:07:47.950846910 CET	8.8.8.8	192.168.2.5	0x8443	No error (0)	cdnjs.clou dflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Feb 5, 2021 15:08:32.661825895 CET	8.8.8.8	192.168.2.5	0xb0f6	No error (0)	d2gu4vothx mtom.cloud front.net		143.204.15.81	A (IP address)	IN (0x0001)
Feb 5, 2021 15:08:32.661825895 CET	8.8.8.8	192.168.2.5	0xb0f6	No error (0)	d2gu4vothx mtom.cloud front.net		143.204.15.206	A (IP address)	IN (0x0001)
Feb 5, 2021 15:08:32.661825895 CET	8.8.8.8	192.168.2.5	0xb0f6	No error (0)	d2gu4vothx mtom.cloud front.net		143.204.15.131	A (IP address)	IN (0x0001)
Feb 5, 2021 15:08:32.661825895 CET	8.8.8.8	192.168.2.5	0xb0f6	No error (0)	d2gu4vothx mtom.cloud front.net		143.204.15.197	A (IP address)	IN (0x0001)
Feb 5, 2021 15:08:33.831979990 CET	8.8.8.8	192.168.2.5	0x4fdb	No error (0)	d2gu4vothx mtom.cloud front.net		143.204.15.81	A (IP address)	IN (0x0001)
Feb 5, 2021 15:08:33.831979990 CET	8.8.8.8	192.168.2.5	0x4fdb	No error (0)	d2gu4vothx mtom.cloud front.net		143.204.15.206	A (IP address)	IN (0x0001)
Feb 5, 2021 15:08:33.831979990 CET	8.8.8.8	192.168.2.5	0x4fdb	No error (0)	d2gu4vothx mtom.cloud front.net		143.204.15.131	A (IP address)	IN (0x0001)
Feb 5, 2021 15:08:33.831979990 CET	8.8.8.8	192.168.2.5	0x4fdb	No error (0)	d2gu4vothx mtom.cloud front.net		143.204.15.197	A (IP address)	IN (0x0001)
Feb 5, 2021 15:08:54.951648951 CET	8.8.8.8	192.168.2.5	0xf486	No error (0)	cdnjs.clou dflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Feb 5, 2021 15:08:54.951648951 CET	8.8.8.8	192.168.2.5	0xf486	No error (0)	cdnjs.clou dflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Feb 5, 2021 15:08:55.031986952 CET	8.8.8.8	192.168.2.5	0x2789	No error (0)	www.youtub e.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 15:08:56.128251076 CET	8.8.8.8	192.168.2.5	0xd144	No error (0)	cdnjs.clou dflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Feb 5, 2021 15:08:56.128251076 CET	8.8.8.8	192.168.2.5	0xd144	No error (0)	cdnjs.clou dflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Feb 5, 2021 15:09:19.725985050 CET	8.8.8.8	192.168.2.5	0x9e16	No error (0)	googleads. g.doubleclick.net	pagead46.l.doubleclick.ne t		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 15:09:19.725985050 CET	8.8.8.8	192.168.2.5	0x9e16	No error (0)	pagead46.l .doubleclick.net		172.217.23.66	A (IP address)	IN (0x0001)
Feb 5, 2021 15:09:19.872160912 CET	8.8.8.8	192.168.2.5	0x29c2	No error (0)	static.dou bleclick.net	static-doubleclick-net.l.google.com		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 15:09:22.657424927 CET	8.8.8.8	192.168.2.5	0x5ac	No error (0)	i.ytimg.com		172.217.22.246	A (IP address)	IN (0x0001)
Feb 5, 2021 15:09:22.664328098 CET	8.8.8.8	192.168.2.5	0x141	No error (0)	yt3.ggpht.com	photos-ugc.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Feb 5, 2021 15:09:22.664328098 CET	8.8.8.8	192.168.2.5	0x141	No error (0)	photos-ugc .l.googleu sercontent.com		172.217.23.33	A (IP address)	IN (0x0001)

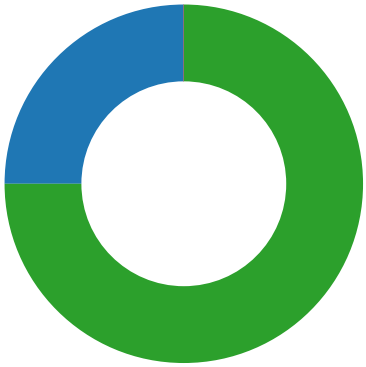
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 5, 2021 15:07:17.643906116 CET	54.177.210.138	443	192.168.2.5	49719	CN=somervoice.somervillema.gov 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.	Wed Jan 20 04:15:50 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Apr 20 05:15:50 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 5, 2021 15:07:48.075481892 CET	104.16.18.94	443	192.168.2.5	49732	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Feb 5, 2021 15:07:48.075515985 CET	104.16.18.94	443	192.168.2.5	49733	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Feb 5, 2021 15:09:19.830374002 CET	172.217.23.66	443	192.168.2.5	49764	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 05 13:07:00 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 30 14:06:59 CEST 2021 Wed Dec 15 01:00:42 CET 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 5, 2021 15:09:19.831161022 CET	172.217.23.66	443	192.168.2.5	49763	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 05 13:07:00 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 30 14:06:59 CEST 2021 Wed Dec 15 01:00:42 CET 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: 6080 Parent PID: 768

General

Start time:	15:07:14
Start date:	05/02/2021
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' 'https://somervoice.somervillema.gov/novel-coronavirus-resources-for-businesses/widgets/16897/videos/2327' > cmdline.out 2>&1
Imagebase:	0x150000
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	15D194	CreateFileW

Analysis Process: conhost.exe PID: 4580 Parent PID: 6080

General

Start time:	15:07:15
Start date:	05/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 5924 Parent PID: 6080

General

Start time:	15:07:16
Start date:	05/02/2021
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' 'https://somervoice.somervillema.gov/novel-coronavirus-resources-for-businesses/widgets/16897/videos/2327'
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\2327	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	46596C	fopen
C:\Users\user\Desktop\download\.wget-hsts	read attributes | synchronize | generic read | 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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\download\2327	unknown	8192	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 27 65 6e 2d 55 53 27 20 78 6d 6c 3a 6c 61 6e 67 3d 27 65 6e 2d 55 53 27 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 27 49 45 3d 65 64 67 65 27 20 68 74 74 70 2d 65 71 75 69 76 3d 27 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 27 3e 0a 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 27 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 27 20 68 74 74 70 2d 65 71 75 69 76 3d 27 43 6f 6e 74 65 6e 74 2d 74 79 70 65 27 3e 0a 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 27 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 27 20 6e 61 6d 65 3d 27 76 69 65 77 70 6f 72 74 27 3e 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 27 68 74 74 70 73 3a 2f 2f 73	<!DOCTYPE html>.<html lang='en-US' xml:lang='en-US'>. <head>.<meta content='IE=edge' http-equiv='X-UA-Compatible'>. <meta content='text/html; charset=utf-8' http-equiv='Content-type'>. <meta content='width=device-width' name='viewport'>. <link href='https://s	success or wait	4	47F21C	fwrite

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5988 Parent PID: 5704

General

Start time:	15:07:20
Start date:	05/02/2021
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\2327.html
Imagebase:	0x7ff7319a0000
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: 2092 Parent PID: 5988

General

Start time:	15:07:20
Start date:	05/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5988 CREDAT:17410 /prefetch:2
Imagebase:	0xdb0000
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

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

Disassembly

Code Analysis