ID: 409519
Cookbook: browseurl.jbs
Time: 10:09:19
Date: 10/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

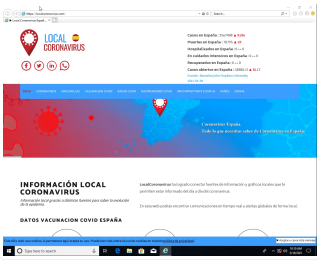
Analysis Report http://localcoronavirus.com

Overview

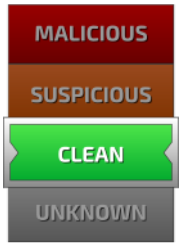
General Information

Sample URL:	http://localcoronavirus.com
Analysis ID:	409519
Infos:	

Most interesting Screenshot:



Detection

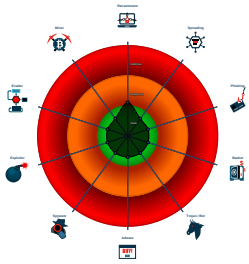


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5660 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5656 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5660 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- OpenWith.exe (PID: 6460 cmdline: C:\Windows\system32\OpenWith.exe -Embedding MD5: D179D03728E95E040A889F760C1FC402)
- **cleanup**

Malware Configuration

No configs have been found

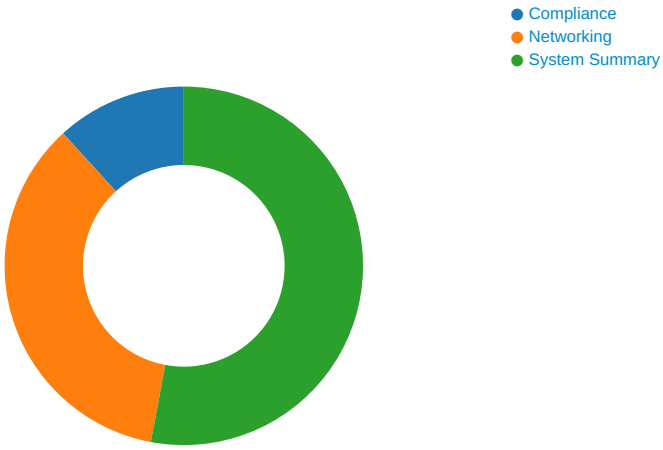
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



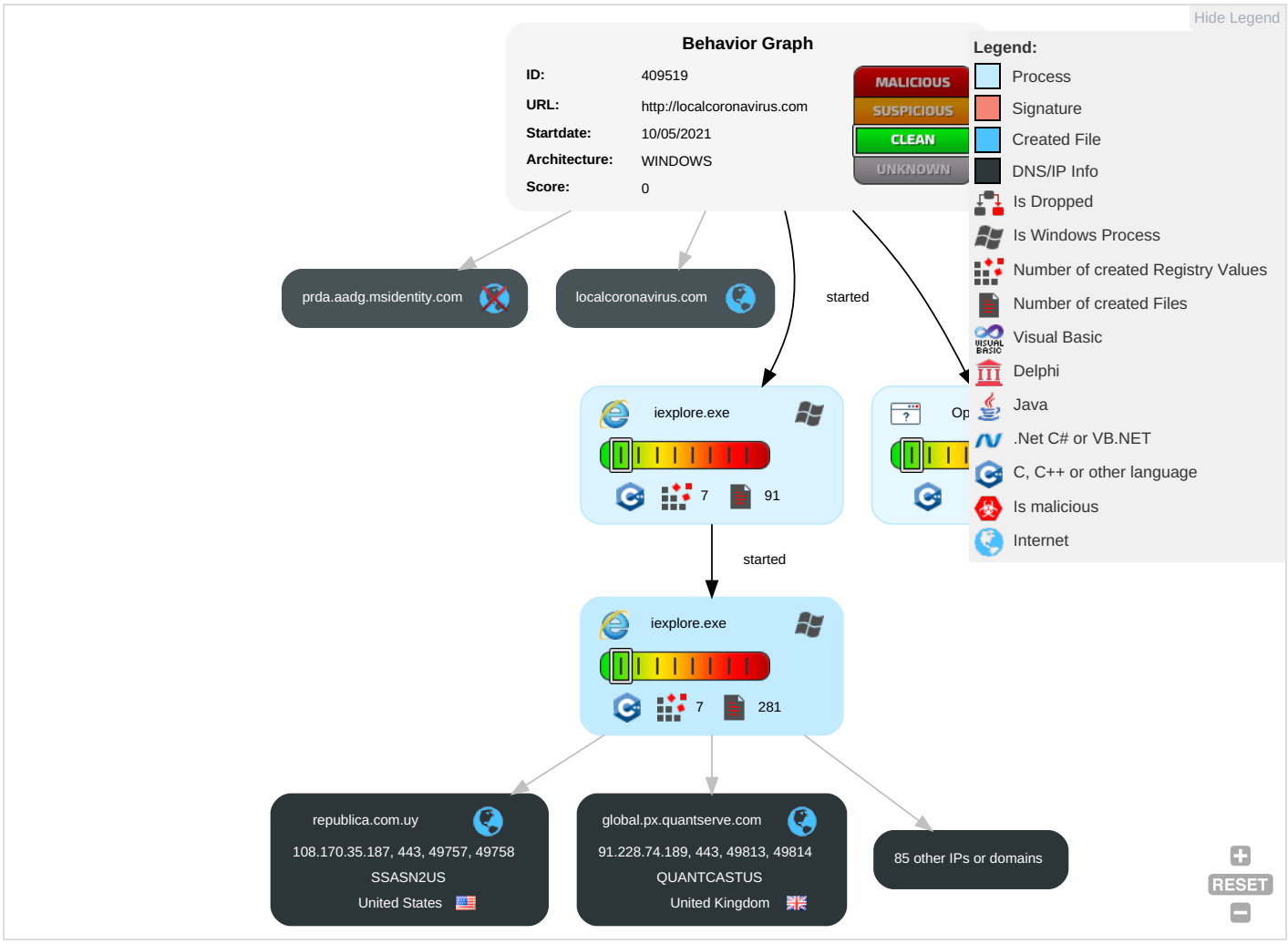
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory 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	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	System Information Discovery 1	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	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	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	Delet Devic Data
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		Carri Billin Fraud

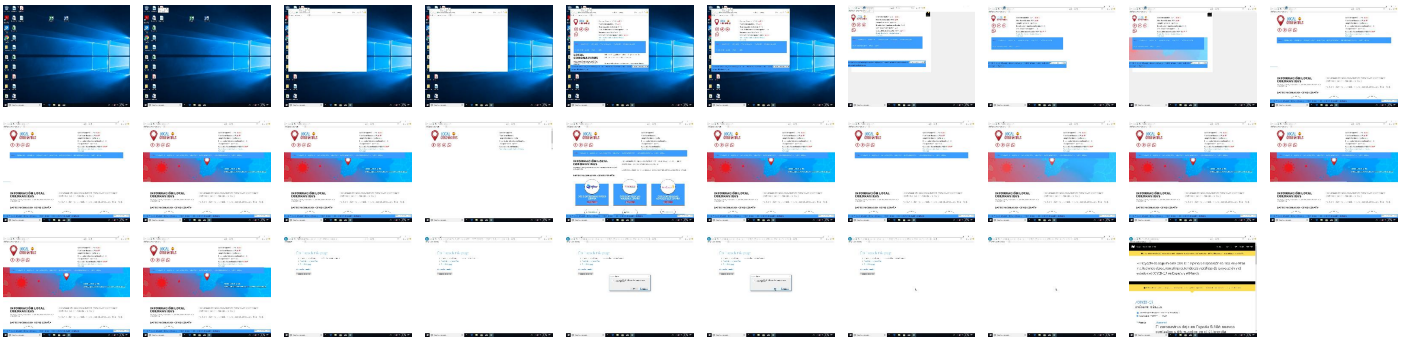
Behavior Graph

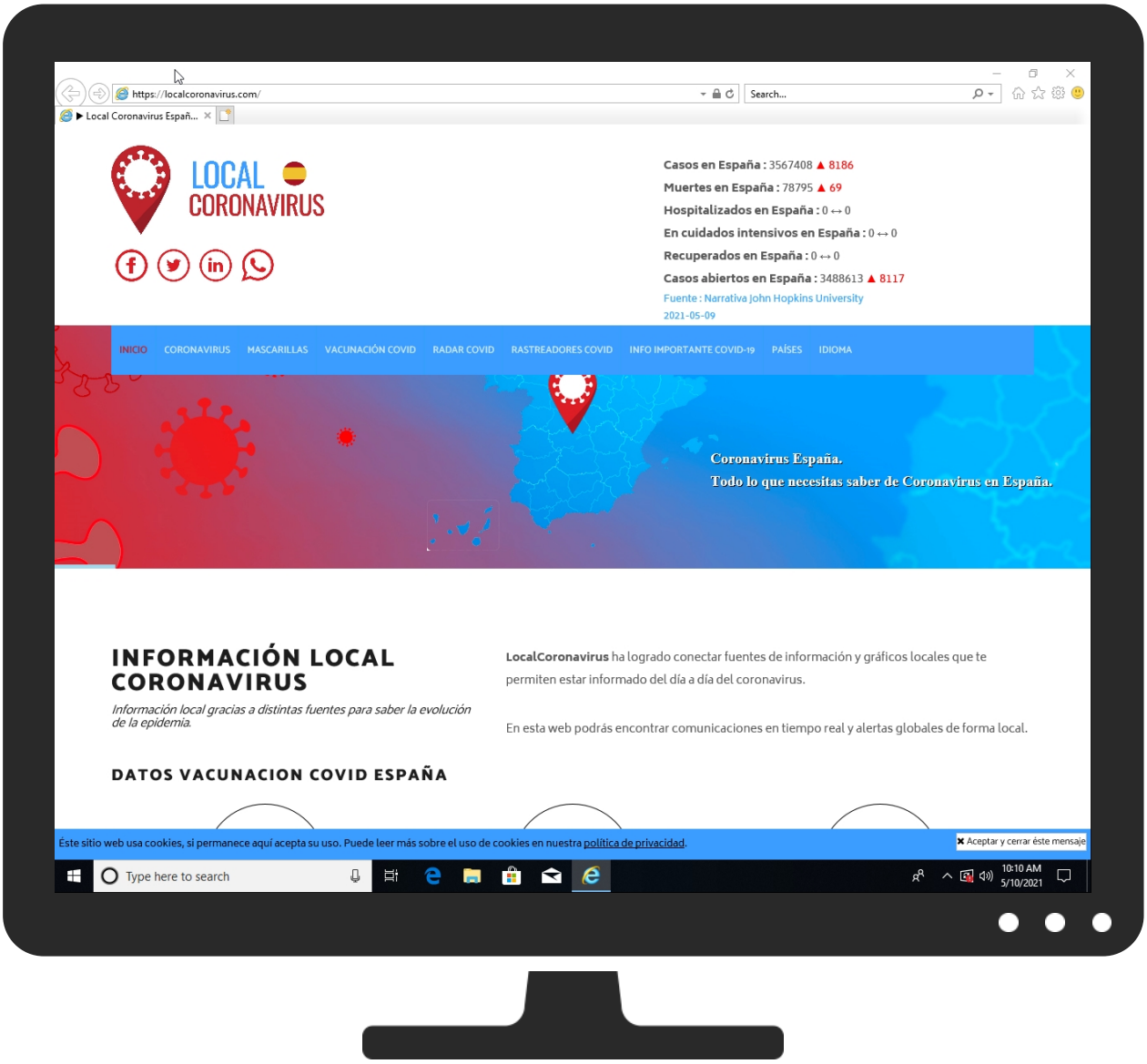


Screenshots

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://localcoronavirus.com	5%	Virustotal		Browse
http://localcoronavirus.com	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://https://covid19tracking.narrativa.com/img/Logo_RTVE.png	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/sv.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/sv.html	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.hotjarconsent.com/sv.html	0%	URL Reputation	safe	
http://https://help.narrativa.com/	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/pt.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/pt.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/pt.html	0%	URL Reputation	safe	
http://https://fontawesome.comhttps://fontawesome.comFont	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/de.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/de.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/de.html	0%	URL Reputation	safe	
http://https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://www.mscbs.gob.es/profesionales/saludPublica/ccayes/alertasActual/nCov/vacunaCovid19.htm	0%	Avira URL Cloud	safe	
http://https://covid19tracking.narrativa.com/img/infobae.png	0%	Avira URL Cloud	safe	
http://https://www.nwc10.com/politica-privacidad	0%	Avira URL Cloud	safe	
http://https://covid19tracking.narrativa.com/img/carto.png	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/pl.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/pl.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/pl.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fr.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fr.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fr.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/ru.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/ru.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/ru.html	0%	URL Reputation	safe	
http://https://www.narrativa.com	0%	Avira URL Cloud	safe	
http://labs.skinkers.com/touchSwipe/	0%	URL Reputation	safe	
http://labs.skinkers.com/touchSwipe/	0%	URL Reputation	safe	
http://labs.skinkers.com/touchSwipe/	0%	URL Reputation	safe	
http://https://www.appliedxl.com/	0%	Avira URL Cloud	safe	
http://https://covid19tracking.narrativa.com/v2/bootstrap-4.4.1-dist/css/custom.css	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://twitter.cRoot	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/el.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/el.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/el.html	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://proteccion10.net/compras.html	0%	Avira URL Cloud	safe	
http://https://www.mscbs.gob.es/profesionales/saludPublica/ccayes/alertasActual/nCov-China/situacionActual.	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/zh.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/zh.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/zh.html	0%	URL Reputation	safe	
http://www.nwc10.com/condiciones-del-servicio	0%	Avira URL Cloud	safe	
http://www.nwc10.com/politica-privacidad	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/fi.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fi.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fi.html	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.googletagservices.com	216.58.214.226	true	false		high
puntodebreak.com	185.125.78.79	true	false		high
global.px.quantserve.com	91.228.74.189	true	false		high
di7juyclzlgyp.cloudfront.net	13.32.25.93	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dbpabf0off7y1.cloudfront.net	65.9.66.65	true	false		high
cc.adingo.jp	54.64.53.220	true	false		unknown
republica.com.uy	108.170.35.187	true	false		unknown
rtb.openx.net	35.186.253.211	true	false		high
scontent.xx.fbcdn.net	31.13.92.14	true	false		high
aec01.esg.rtve.edgetcdn.io	51.210.220.45	true	false		unknown
script.hotjar.com	13.32.25.86	true	false		high
tagr-gcp-odr-euw4.mookie1.com	34.98.67.61	true	false		high
d1j70itqjm2icu.cloudfront.net	13.32.25.35	true	false		high
cm.g.doubleclick.net	172.217.16.98	true	false		high
localcoronavirus.com	172.67.183.244	true	false		unknown
id.rlcdn.com	35.244.174.68	true	false		high
a7cb1ba23276f4b358d8fca4e8cdf9ab-1165437553.us-east-1.elb.amazonaws.com	184.73.211.96	true	false		high
d3cra5ec8gdi8w.cloudfront.net	13.35.253.104	true	false		high
static-cdn.hotjar.com	13.32.25.105	true	false		high
www.google.de	172.217.16.99	true	false		high
pagead46.l.doubleclick.net	172.217.19.98	true	false		high
pugm22000nf.pubmatic.com	185.64.189.115	true	false		high
cs491300.wpc.mucdn.net	192.229.220.196	true	false		unknown
us-u.openx.net	35.244.159.8	true	false		high
d2jcax5o6gwtn6.cloudfront.net	13.32.25.3	true	false		high
stats.l.doubleclick.net	74.125.140.154	true	false		high
d37ub18b7ivraq.cloudfront.net	99.86.2.109	true	false		high
www.elconfidencialdigital.com	104.25.56.34	true	false		high
tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com	52.29.48.214	true	false		high
akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com	54.194.190.147	true	false		high
cs491.wac.edgecastcdn.net	192.229.233.25	true	false		high
4i2g925ohj.execute-api.eu-west-3.amazonaws.com	65.9.66.121	true	false		high
proteccion10.net	193.32.242.105	true	false		unknown
vars.hotjar.com	99.86.2.129	true	false		high
cec01.eug.edgetcdn.io	51.68.35.185	true	false		unknown
partnerad.l.doubleclick.net	216.58.214.226	true	false		high
googleads.g.doubleclick.net	216.58.214.194	true	false		high
prisa-us-eu.map.fastly.net	199.232.194.133	true	false		unknown
www.google.ch	172.217.19.99	true	false		high
aragornapp-v2-prod-uk-lbj.inbake.com	18.135.148.201	true	false		unknown
ag.innovid.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
www.republica.com.uy	unknown	unknown	false		unknown
as01.epimg.net	unknown	unknown	false		high
pixel.everesttech.net	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
static.hotjar.com	unknown	unknown	false		high
www.lavozdegalicia.es	unknown	unknown	false		high
i.blogs.es	unknown	unknown	false		high
platform.twitter.com	unknown	unknown	false		high
static2.abc.es	unknown	unknown	false		high
static4.abc.es	unknown	unknown	false		high
covid19tracking.narrativa.com	unknown	unknown	false		unknown
odr.mookie1.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
pixel.rubiconproject.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
imagenes.20minutos.es	unknown	unknown	false		high
ssum-sec.casalemedia.com	unknown	unknown	false		high
cronicaglobal.elespanol.com	unknown	unknown	false		high
phantom-elmundo.unidadeditorial.es	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high
www.puntodebreak.com	unknown	unknown	false		high
image6.pubmatic.com	unknown	unknown	false		high
s1.eestatic.com	unknown	unknown	false		high
cdn2.excelsior.com.mx	unknown	unknown	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d.agkn.com	unknown	unknown	false		high
ep00.epimg.net	unknown	unknown	false		high
e.dlx.addthis.com	unknown	unknown	false		high
phantom-expansion.unidadeditorial.es	unknown	unknown	false		high
beacon.walmart.com	unknown	unknown	false		high
adservice.google.ch	unknown	unknown	false		high
img.huffingtonpost.com	unknown	unknown	false		high
img2.rtve.es	unknown	unknown	false		high
cms.quantserve.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.puntodebreak.com/files/alexander-zverev-conclusiones-mutua-madrid-open-2021.png	false		high

URLs from Memory and Binaries

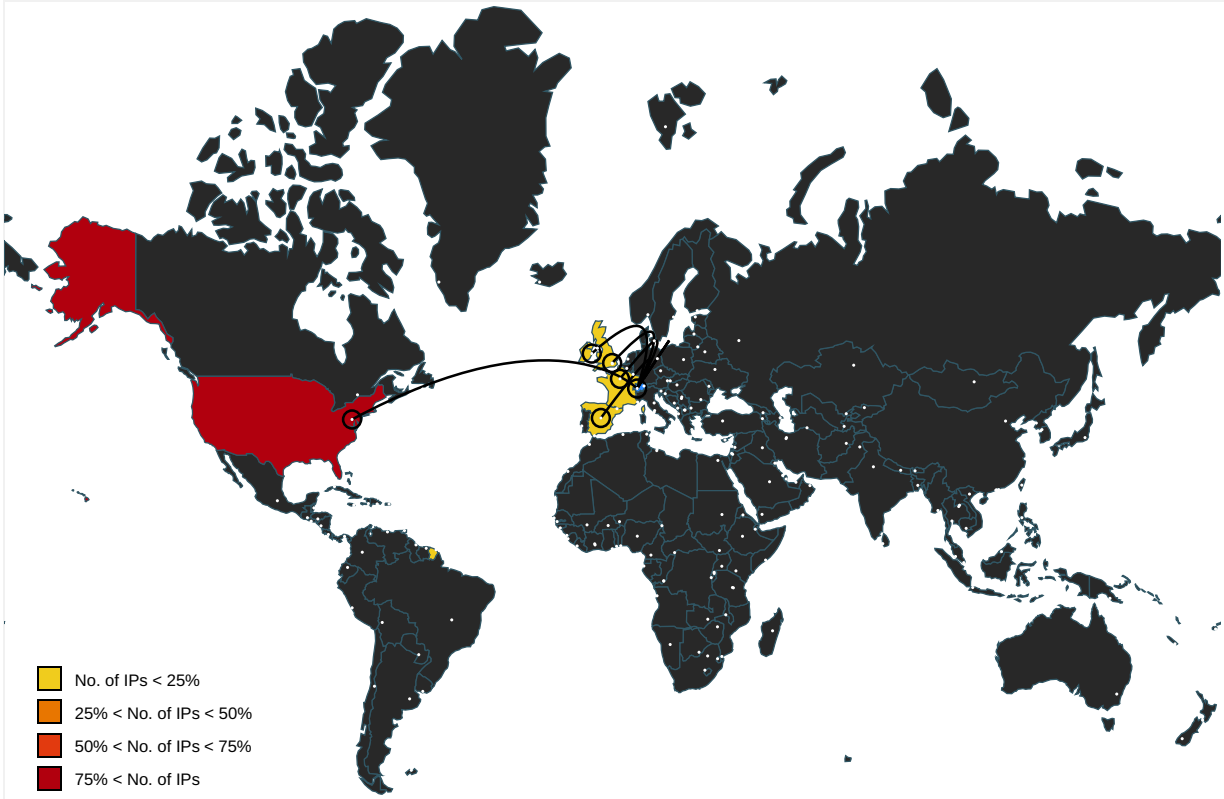
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://covid19tracking.narrativa.com/img/Logo_RTVE.png	ZLRC4GGW.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.lavozdegalicia.es/default/2021/05/09/00121620573842504277471/Foto/O29Y8020.jpg	VUUSS9Y4.htm.3.dr	false		high
http://fontawesome.io	font-awesome.min[1].css.3.dr	false		high
http://https://www.santepubliquefrance.fr/maladies-et-traumatismes/maladies-et-infections-respiratoires/inf	ZLRC4GGW.htm.3.dr	false		high
http://https://stats.g.doubleclick.net/g/collect	js[2].js.3.dr	false		high
http://https://www.hotjarconsent.com/sv.html	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.lavozdegalicia.es/noticia/educacion/2021/05/09/alumnos-espanoles-saben-detectar-mensajes	VUUSS9Y4.htm.3.dr	false		high
http://https://googleads.g.doubleclick.net/aclk?sa=l&ai=ClKdQb-qYYMr1LqKKiM0P1PegsAOSlLyrYPOgk4PxDJ64iL	ads[3].htm.3.dr	false		high
http://https://www.rtve.es/noticias/20210510/ritmo-vacunacion-comunidades/2083665.shtml	VUUSS9Y4.htm.3.dr	false		high
http://https://www.elblogsalmon.com/mundo-laboral/todo-trabajo-que-se-ha-perdido-mundo-pandemia-puede-supon	VUUSS9Y4.htm.3.dr	false		high
http://https://help.narrativa.com/	ZLRC4GGW.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.abc.es/espana/castilla-leon/abci-igea-si-tiene-volver-estado-alarma-gobierno-debe-dimiti	VUUSS9Y4.htm.3.dr	false		high
http://https://www.hotjarconsent.com/pt.html	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://fontawesome.comhttps://fontawesome.comFont	free-fa-brands-400[1].eot.3.dr, free-fa-regular-400[1].eot.3.dr, free-fa-solid-900[1].eot.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/html/r20210505/r20190131/zrt_lookup.html	{93606B04-B1B2-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://img.huffingtonpost.com/asset/6098cbc1260000e269b4296a.jpg?ops=1200_630	VUUSS9Y4.htm.3.dr	false		high
http://https://fontawesome.com	free-fa-brands-400[1].eot.3.dr, free-v4-font-face.min[1].css.3.dr	false		high
http://https://www.youtube.com/iframe_api	js[2].js.3.dr	false		high
http://https://www.hotjarconsent.com/de.html	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://4i2g925ohj.execute-api.eu-west-3.amazonaws.com/pro/coronavirus?confirmed_num=158.339.218&act	ZLRC4GGW.htm.3.dr	false		high
http://https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	widgets[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://phantom-elmundo.unidadeditorial.es/de450e428f4bd13b9bd4d4d7d5445edc/resize/1200/f/jpg/assets	VUUSS9Y4.htm.3.dr	false		high
http://https://www.puntodebreak.com/files/alexander-zverev-conclusiones-mutua-madrid-open-2021.png	VUUSS9Y4.htm.3.dr	false		high
http://https://connect.facebook.net/en_US/fbevents.js	VUUSS9Y4.htm.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://getbootstrap.com)	bootstrap[1].css.3.dr, bootstrap[1].js.3.dr	false	• Avira URL Cloud: safe	low
http://https://googleads.g.doubleclick.net/pagead/html/r20210505/r20190131/zrt_lookup.html#RS-0-&adk=181227	{93606B04-B1B2-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/interaction/%3Fai%3DCLqxzh-qYYLfXGqyAmAe5rpSAA9ib8aZi_uTt	ads[2].htm0.3.dr, {93606B04-B1B2-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://script.hotjar.com/	hotjar-2075733[1].js.3.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.3.dr	false		high
http://https://cdn.ampproject.org/amp4ads-host-v0.js	f[1].txt0.3.dr	false		high
http://https://www.mscbs.gob.es/profesionales/saludPublica/ccayes/alertasActual/nCov/vacunaCovid19.htm	VUUSS9Y4.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://greensock.com	jquery.themepunch.tools.min[1].js.3.dr	false		high
http://https://covid19tracking.narrativa.com/img/infobae.png	ZLRC4GGW.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://https://covid19tracking.narrativa.com/	VUUSS9Y4.htm.3.dr	false		unknown
http://https://www.elmundo.es/ciencia-y-salud/salud/2021/05/10/6098bf1a21efa0e9398b45d6.html	VUUSS9Y4.htm.3.dr	false		high
http://https://www.abc.es/gastronomia/abci-diez-restaurantes-donde-comer-buen-rabo-toro-madrid-202105100904	VUUSS9Y4.htm.3.dr	false		high
http://https://insights-staging.hotjar.com	box-5e3cec51ed8e99df6977c199d27812d7[1].htm.3.dr	false		high
http://https://www.nwc10.com/politica-privacidad	VUUSS9Y4.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://vars.hotjar.com/box-5e3cec51ed8e99df6977c199d27812d7.html	{93606B04-B1B2-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://covid19tracking.narrativa.com/img/carto.png	ZLRC4GGW.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.rtve.es/	ZLRC4GGW.htm.3.dr	false		high
http://https://cdn.jsdelivr.net/npm/chart.js	VUUSS9Y4.htm.3.dr	false		high
http://https://www.hotjarconsent.com/pl.html	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/images/mtad/back_blue.png	ads[1].htm0.3.dr, ads[2].htm0.3.dr	false		high
http://https://www.hotjarconsent.com/fr.html	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.hotjarconsent.com/ru.html	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.narrativa.com	ZLRC4GGW.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/images/mtad/x_blue.png	{93606B04-B1B2-11EB-90E4-ECF4BB862DED}.dat.1.dr, ads[1].htm1.3.dr, ads[1].htm.3.dr, ads[3].htm0.3.dr, ads[2].htm.3.dr	false		high
http://labs.skinkers.com/touchSwipe/	jquery.themepunch.tools.min[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ep00.epimg.net/elcomidista/imagenes/2021/05/03/articulo/1620035561_444557_1620041680_rrss_no	VUUSS9Y4.htm.3.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/images/adchoices/iconx2-000000.png	{93606B04-B1B2-11EB-90E4-ECF4BB862DED}.dat.1.dr, ads[1].htm1.3.dr, ads[1].htm.3.dr	false		high
http://https://twitter.com/NarrativaAI	ZLRC4GGW.htm.3.dr	false		high
http://https://systems.jhu.edu/research/public-health/ncov/	ZLRC4GGW.htm.3.dr	false		high
http://https://www.appliedxl.com/	ZLRC4GGW.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://imagenes.20minutos.es/files/og_thumbnail/uploads/imagenes/2021/05/10/primera-noche-en-barcel	VUUSS9Y4.htm.3.dr	false		high
http://https://imagenes.20minutos.es/files/og_thumbnail/uploads/imagenes/2021/05/09/madrid.jpeg	VUUSS9Y4.htm.3.dr	false		high
http://https://cronicaglobal.elespanol.com/primeras-planas/quinta-ola-tambores-electorales-en-cataluna_4807	VUUSS9Y4.htm.3.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&h=280&adk=	{93606B04-B1B2-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://covid19tracking.narrativa.com/v2/bootstrap-4.4.1-dist/css/custom.css	ZLRC4GGW.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.googletagservices.com/activeview/js/current/osd.js	f[1].txt0.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cct.google/taggy/agent.js	js[2].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/pcm-dpc/COVID-19	ZLRC4GGW.htm.3.dr	false		high
http://https://twitter.cRoot	{93606B04-B1B2-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/drt/si	{93606B04-B1B2-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://www.hotjarconsent.com/el.html	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.google.%/ads/ga-audiences	analytics[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.youtube.com/	msapplication.xml7.1.dr	false		high
http://https://proteccion10.net/compras.html	VUUSS9Y4.htm.3.dr, {93606B04-B1B2-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap[1].css0.3.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/interaction/%3Fai%3DCf7H6b-qYYPjdOZ3cYLKXnPAMkpS8q2DzoJOD	ads[1].htm0.3.dr	false		high
http://https://stats.g.doubleclick.net/g/collect?v=2&	js[2].js.3.dr	false		high
http://https://s1.eestatic.com/2021/05/07/ciencia/salud/579456311_184747324_600x315.jpg	VUUSS9Y4.htm.3.dr	false		high
http://googleads.g.doubleclick.net	f[1].txt0.3.dr, f[2].txt0.3.dr	false		high
http://carto.com/	ZLRC4GGW.htm.3.dr	false		high
http://https://www.mscbs.gob.es/profesionales/saludPublica/ccayes/alertasActual/nCov-China/situacionActual.	ZLRC4GGW.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://d3cra5ec8gdi8w.cloudfront.net/uploads/imagenes/social/2021/05/10/_europapress2721462cremafal	VUUSS9Y4.htm.3.dr	false		high
http://https://img2.rtve.es/imagenes/asi-avanza-vacunacion-cada-comunidad-autonoma/1617127710560.jpg	VUUSS9Y4.htm.3.dr	false		high
http://https://twitter.com/in	{93606B04-B1B2-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://www.hotjarconsent.com/zh.html	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nwc10.com/condiciones-del-servicio	VUUSS9Y4.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.nwc10.com/politica-privacidad	VUUSS9Y4.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://static2.abc.es/media/espana/2021/05/10/1436723653-kos--1024x512	VUUSS9Y4.htm.3.dr	false		high
http://https://twitter.com/SaludPublicaEs	VUUSS9Y4.htm.3.dr	false		high
http://https://stats.uptimerobot.com/Q6NlpspLQ	ZLRC4GGW.htm.3.dr	false		high
http://https://www.hotjar.com	box-5e3cec51ed8e99df6977c199d27812d7[1].htm.3.dr	false		high
http://https://static4.abc.es/media/gastronomia/2021/05/10/casa-pedro-rabo-toro-madrid-kh8--1024x512	VUUSS9Y4.htm.3.dr	false		high
http://https://www.hotjarconsent.com/fi.html	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://static4.abc.es/media/espana/2021/05/10/igea2-k0NH--1024x512	VUUSS9Y4.htm.3.dr	false		high
http://https://ka-f.fontawesome.com	b745858f50[1].js.3.dr	false		high
http://plugins.jquery.com/project/touchSwipe	jquery.themepunch.tools.min[1].js.3.dr	false		high
http://www.puntodebreak.com/2021/05/10/10-conclusiones-deja-mutua-madrid-open-2021	VUUSS9Y4.htm.3.dr	false		high
http://https://elcomidista.elpais.com/elcomidista/2021/05/03/articulo/1620035561_444557.html	VUUSS9Y4.htm.3.dr	false		high
http://www.greensock.com/club/	jquery.themepunch.tools.min[1].js.3.dr	false		high
http://https://github.com/mattbryson/TouchSwipe-Jquery-Plugin	jquery.themepunch.tools.min[1].js.3.dr	false		high
http://https://googleads.g.doubleclick.net/aclk?sa=l&ai=CfWPacOqYYMOHBJCEYLbTvrAOkpS8q2DzoJOD8QzX5dLmlQ	ads[2].htm.3.dr	false		high
http://greensock.com/standard-license	jquery.themepunch.tools.min[1].js.3.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/images/mtad/ad_choices_blue.png	{93606B04-B1B2-11EB-90E4-ECF4BB862DED}.dat.1.dr, ads[1].htm1.3.dr, ads[1].htm.3.dr, ads[3].htm0.3.dr, ads[2].htm.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.abc.es/espana/noticias-ultima-hora/abci-seis-noticias-debes-conocer-lunes-10-mayo-202105	VUUSS9Y4.htm.3.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.16.98	cm.g.doubleclick.net	United States		15169	GOOGLEUS	false
13.35.253.104	d3cra5ec8gdi8w.cloudfront.net	United States		16509	AMAZON-02US	false
52.29.48.214	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
185.125.78.79	puntodebreak.com	Spain		60458	ASN-XTUDIONETES	false
54.64.53.220	cc.adingo.jp	United States		16509	AMAZON-02US	false
99.86.2.129	vars.hotjar.com	United States		16509	AMAZON-02US	false
216.58.214.226	www.googletagservices.com	United States		15169	GOOGLEUS	false
192.229.220.196	cs491300.wpc.mucdn.net	United States		15133	EDGECASTUS	false
74.125.140.154	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
13.32.25.35	d1j70itqjm2icu.cloudfront.net	United States		7018	ATT-INTERNET4US	false
172.217.19.99	www.google.ch	United States		15169	GOOGLEUS	false
35.244.174.68	id.rlcdn.com	United States		15169	GOOGLEUS	false
34.98.67.61	tagr-gcp-odr-euw4.mookie1.com	United States		15169	GOOGLEUS	false
216.58.214.194	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
192.229.233.25	cs491.wac.edgecastcdn.net	United States		15133	EDGECASTUS	false
91.228.74.189	global.px.quantserve.com	United Kingdom		27281	QUANTCASTUS	false
31.13.92.14	scontent.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false
108.170.35.187	republica.com.uy	United States		20454	SSASN2US	false
35.244.159.8	us-u.openx.net	United States		15169	GOOGLEUS	false
18.135.148.201	aragornapp-v2-prod-uk-lbj.inbake.com	United States		16509	AMAZON-02US	false
65.9.66.121	4i2g925ohj.execute-api.eu-west-3.amazonaws.com	United States		16509	AMAZON-02US	false
199.232.194.133	prisa-us-eu.map.fastly.net	United States		54113	FASTLYUS	false
13.32.25.86	script.hotjar.com	United States		7018	ATT-INTERNET4US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.64.189.115	pugm22000nf.pubmatic.com	United Kingdom		62713	AS-PUBMATICUS	false
54.194.190.147	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
13.32.25.3	d2jcax5o6gwtn6.cloudfront.net	United States		7018	ATT-INTERNET4US	false
51.210.220.45	aec01.esg.rtve.edgetcdn.io	France		16276	OVHFR	false
99.86.2.109	d37ub18b7ivraq.cloudfront.net	United States		16509	AMAZON-02US	false
51.68.35.185	cec01.eug.edgetcdn.io	France		16276	OVHFR	false
184.73.211.96	a7cb1ba23276f4b358d8fca4e8cdf9ab-1165437553.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
35.186.253.211	rtb.openx.net	United States		15169	GOOGLEUS	false
172.67.183.244	localcoronavirus.com	United States		13335	CLOUDFLARENETUS	false
193.32.242.105	proteccion10.net	Spain		41705	GRUPOBALADIGES	false
65.9.66.65	dbpabf0off7y1.cloudfront.net	United States		16509	AMAZON-02US	false
13.32.25.93	di7juyclzlgyp.cloudfront.net	United States		7018	ATT-INTERNET4US	false
104.25.56.34	www.elconfidencialdigital.com	United States		13335	CLOUDFLARENETUS	false
13.32.25.105	static-cdn.hotjar.com	United States		7018	ATT-INTERNET4US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	409519
Start date:	10.05.2021
Start time:	10:09:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://localcoronavirus.com
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:	18
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@4/219@52/37
EGA 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 • Browsing link: https://localcoronavirus.com/ • Browsing link: https://faceboo k.com/sharer/sharer.php?u=http s%3A%2F%2Flocalcoronavirus.com • Browsing link: https://twitter.com/intent/tweet/? text=Local%20information%20from%20COVID%2 019&url=https%3A%2F%2Floca lcoronavirus.com • Browsing link: https://www.lin kedin.com/shareArticle?mini=tr ue&url=https%3A%2F%2Flocal coronavirus.com&title=Loca l%20information%20from%20COVID %2019&summary=Local%20info rmation%20from%20COVID%2019&am p;source=https%3A%2F%2Flocalcoronavirus.com • Browsing link: whatsapp://send/? text=Local%20information%20f rom%20COVID%2019%20https%3A%2F %2Flocalcoronavirus.com • Browsing link: https://covid19 tracking.narrativa.com/

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.43.193.48, 168.61.161.212, 88.221.62.148, 172.217.20.10, 172.217.18.104, 142.250.186.142, 172.217.19.98, 92.122.213.154, 92.122.213.162, 151.101.2.109, 151.101.66.109, 151.101.130.109, 151.101.194.109, 172.217.16.99, 172.217.20.14, 104.42.151.234, 172.217.19.100, 172.217.19.97, 172.217.20.3, 92.122.147.230, 69.173.144.138, 69.173.144.165, 69.173.144.139, 34.246.227.69, 52.18.11.109, 99.80.199.35, 92.122.144.200, 152.199.19.161, 52.247.32.180, 2.20.143.16, 2.20.142.209, 52.255.188.83, 40.126.31.6, 20.190.159.134, 40.126.31.137, 40.126.31.143, 20.190.159.132, 20.190.159.136, 40.126.31.135, 40.126.31.4, 20.49.157.6, 104.18.22.52, 104.18.23.52, 172.67.198.134, 104.21.44.98 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, ka-f.fontawesome.com.cdn.cloudflare.net, partner.googleadservices.com, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, e11290.dspg.akamaiedge.net, beacon-cdn-custom.walmart.com.akadns.net, login.live.com, audownload.windowsupdate.nsatc.net, www.google.com, tp00.everesttech.net.akadns.net, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, www.google-analytics.com, fonts.googleapis.com, fs.microsoft.com, ag-5-split.ag.innovid.com.akadns.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, www.tm.a.prd.aadg.akadns.net, pagead2.googlesyndication.com, skypedataprdcolcus15.cloudapp.net, www3.l.google.com, blobcollector.events.data.trafficmanager.net, wac.apr-8315.edgecastdns.net, cs9.wpc.v0cdn.net, beacon-cdn.walmart.com.akadns.net, a1972.g2.akamai.net, au.download.windowsupdate.com.edgesuite.net, pixel.rubiconproject.net.akadns.net, adservice.google.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, iecvlist.microsoft.com, go.microsoft.com, e8037.g.akamaiedge.net, www.googletagmanager.com, arc.trafficmanager.net, prod.fs.microsoft.com.akadns.net, dualstack.f3.shared.global.fastly.net, kit.fontawesome.com.cdn.cloudflare.net, static-abc.akamaized.net, www-google-analytics.l.google.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, login.msa.msidentity.com, skypedataprdcoleus17.cloudapp.net, tpc.googlesyndication.com, go.microsoft.com.edgekey.net, iris-de-ppe-azsc-uks.uksouth.cloudapp.azure.com, analytics.google.com, ssum-sec.casalemedia.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, aws-uk-neb-virg-oh-oreg.ag.innovid.com.akadns.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:11:26	API Interceptor	1x Sleep call for process: OpenWith.exe modified

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\6RHT5YPW\googleads.g.doubleclick[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\VXDGRK8V\localcoronavirus[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	419167
Entropy (8bit):	5.227480035603258
Encrypted:	false
SSDEEP:	12288:KY2YaY2YEY9Y9Y5YNYtYlYyYyYyYy646o6T6T6J6A:KY2YaY2YEY9Y9Y5YNYtYlYyYyYyYy64U
MD5:	5AFE6D39B29F6FA2B8888A74BE591E4A
SHA1:	97617D22A44105CE74F7F1967777AC26A6FE6C51
SHA-256:	2A31D952133171BC62B77A9B320200625084A84D7AB68AB69B7B16588AD904CD
SHA-512:	F5B36E24107AAA2F6829E811194AF9DBCB98938FB47B49B03F1612209C855358947B06F24BE35E9C91DB9493D8F614E0CD9E4C0616AB53B5BE571492496A26AE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\VXDGRK8V\localcoronavirus[1].xml	
Preview:	<root></root><root><item name="goog_pem_mod" value="88" ltime="1486130944" htime="30885311" /></root><root><item name="goog_pem_mod" value="88" ltime="1486130944" htime="30885311" /><item name="google_experiment_mod34" value="512" ltime="1486440944" htime="30885311" /><item name="google_experiment_mod53" value="829" ltime="1486440944" htime="30885311" /></root><root><item name="goog_pem_mod" value="88" ltime="1486130944" htime="30885311" /><item name="google_experiment_mod34" value="512" ltime="1486440944" htime="30885311" /><item name="google_experiment_mod53" value="829" ltime="1486440944" htime="30885311" /><item name="google_experiment_mod36" value="397" ltime="1486600944" htime="30885311" /><item name="google_experiment_mod37" value="200" ltime="1486600944" htime="30885311" /></root><root><item name="goog_pem_mod" value="88" ltime="1486130944" htime="30885311" /><item name="google_experiment_mod34" value="512" ltime="1486440944" htime="30885311" /><item name="google_experiment_mod

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{93606B02-B1B2-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.8779373116385074
Encrypted:	false
SSDEEP:	48:IwCGcprfGwpLaG/ap8WGIpcCuGvnZpvCtGoRqp9CZGo4xpmC3GWzp9CyGWppvCJ1:r2ZpZA22WCrtCCfC6xMClCYCSfCXsrCJ
MD5:	78462BF49BF19296B6F80A4A580BC8E9
SHA1:	4BB808FCC86692A9EC233F4D51EBE38836E02D66
SHA-256:	0872F6E0BA6D2A33590447879C4708C8E7F9B8EC8BBBCFD7DBE03B245A6B7C3B
SHA-512:	D055F37CFAE8BA5E1E602A07125EC3993600962AFE79A6CF359B3808F77A848341D38615F4702E7BCFC608C66206C09F31630D2B6F9C96818270F29797991D91
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\{93606B04-B1B2-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	1184436
Entropy (8bit):	4.083972720931286
Encrypted:	false
SSDEEP:	12288:PGw07pz+Gw4RM1OfMa48qC+OREOR4RM1OfMa48qC0:eL51fMa4B1fMa4v
MD5:	87AC7C4A822F0C7E245ABC8D6B6AC39C
SHA1:	C3E17C4BA70DEDF118B7720CCE952D933D9CB392
SHA-256:	91A44F1024E4E83C199B8D6688493BE52A58251F4195FB6A76596A9BCA8D440C
SHA-512:	C5A149DD3467D4CB550F38DC10C80226A681E0065ACB7178E5245CB861269A41BB049CC359997432517562E184D97AD7368205F1C8250979BCEDCC507E033FC
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\{9E41A913-B1B2-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5654629678591514
Encrypted:	false
SSDEEP:	48:IwSGcprbGwpaqG4pQeGrapbSvGQpKxEG7HpRrTGIpG:rmZ1QK6QBS5AxPTBA
MD5:	2E9F7694ADEAAA5637A6A42F4B4045DB
SHA1:	E99572D902A885872377C7CBF2DC0E2700120959
SHA-256:	4516CD4002CE72DC60AA5368CADC0E6A301CB8AB4954D5377F817D293ED54BE4
SHA-512:	9E003D5B8DC226FAF4EE03B9210C5A7116288AD77846B31B19A0AD597C1994F8EFD5B2A051E16B50BBECDA991950954B0F6412009830E94A4AF14AC715624669
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
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.089150424949241
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEw4nWimI002EtM3MHdNMNxOEs44nWimI00ObVbkEtMb:2d6NxOb4SZHKd6NxOy4SZ76b
MD5:	7F8E3E29D74561EE0AA9D200A7493B3A
SHA1:	D11AB568FF338D78BAC7E66ADECA313C15781D5F
SHA-256:	620736B5447FDC7B8C4FF2818E410176E1D79B26BBA0B9387BE334A5C3D607A4
SHA-512:	BAC747D7E594305C1096915A23B098CB18F78AEFD9E8B22298979C0B0EA875277F4049CA3093629DE49C7B744FB6D58B12542A41A43F71B0B8B6F44595D9E479
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x6ddb0c4e,0x01d745bf</date><accdate>0x6ddb0c4e,0x01d745bf</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>0x6ddb0c4e,0x01d745bf</date><accdate>0x6ddba87e,0x01d745bf</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):	5.132413726892852
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2ky4nWimI002EtM3MHdNMNxe2kV4nWimI00Obkak6EtMb:2d6NxrR4SZHKd6Nxru4SZ7Aa7b
MD5:	7FDA66E9FC368EB0FD5D61A68862F187
SHA1:	1584B3E5B9D40838F7331D43A6B674E7D698A2E0
SHA-256:	51527A6C009CCD843818671822C0FA075094CB91BFB8F99986FDCC49884C115A
SHA-512:	856F3671636C1FE5B4F98A23752AA385DF0B501D60D8BAB75C2AACD7ECA2748B4CA85AE1FF9E623B3A0FC06AAD1381F391FB9B03EEF49545F44FBA1C5FB2926A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x6dd280ab,0x01d745bf</date><accdate>0x6dd280ab,0x01d745bf</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>0x6dd280ab,0x01d745bf</date><accdate>0x6dd31d00,0x01d745bf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.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):	5.117858112135717
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL+rt4nWimI002EtM3MHdNMNxvL+CYt4nWimI00ObmZEtMb:2d6NxvC4SZHKd6Nxvw4SZ7mb
MD5:	B8450DFD7197060E7D64947D6C3319E1
SHA1:	D8DD717BFE3252AF21D56440B0D6828BCD5D6C1F
SHA-256:	19FD75A96BC17CD3EC76158F2EF5242C36A2C2466D68869D42321BC0B1573329
SHA-512:	5C24598F4F999349A8496B497BB1CC1AB59EBE46FEF45CE53F5C171C503FDF49234578B48E5A7D69403961AEE483CB3D51930B325A044D30EEA97AB965DCE65
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x6ddc44b6,0x01d745bf</date><accdate>0x6ddc44b6,0x01d745bf</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>0x6ddc44b6,0x01d745bf</date><accdate>0x6ddce0ef,0x01d745bf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.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):	5.121300567366668

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNxiG4nWimI002EtM3MHdNMNxiNWcS4nWimI00Obd5EtMb:2d6Nxr4SZHKd6Nx8Wt4SZ7Jjb
MD5:	1AA7E68C64883B12D2AAEFEA85142664
SHA1:	9C1064782C1451E70748537098B5FACD7F581177
SHA-256:	B8A0EBA99BB56306E91FA0FE51B585AC610A385A343F2410FD8E031A76FF5742
SHA-512:	FA8AE342D52A0A244CEFC47F5EB36DCC2FE33E4194D93E4F008AC359CF5281461E708E4658F8994D7B591DD3BDED3079FDC0181CFD93B210D68C554D2C7954 9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x6dd7fed7,0x01d745bf</date><acc date>0x6dd7fed7,0x01d745bf</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>0x6dd7fed7,0x01d745bf</date><accdate>0x6dd89 b39,0x01d745bf</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):	5.14858430390065
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwPkr4nWimI002EtM3MHdNMNxhGwPME4nWimI00Ob8K075EtMb:2d6NxQD4SZHKd6NxQo4SZ7YKajb
MD5:	A14006DF641D1AEC00EA912670577918
SHA1:	42973850F2C6208DC113F1E14D56893EC9B19276
SHA-256:	EB3527673673502D9EC7E9610CE03E56053F791DA39714BBA6FEE73EA9852501
SHA-512:	E8A3BD0B5E7E35107A4E544982DE23B9B07665A662A03F512019A5CF6E4C9AC084F37114347332D12E60D50A3DF20149423132E33DC41BFE81B4DD8D3844A5C(
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x6ddd7d27,0x01d745bf</date>< accdate>0x6ddd7d27,0x01d745bf</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>0x6ddd7d27,0x01d745bf</date><accdate>0 x6dde1993,0x01d745bf</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):	5.101530570588366
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nXgEDEigEDEt4nWimI002EtM3MHdNMNx0nXgEDE6K4nWimI00ObxEty:2d6Nx0XxY4SZHKd6Nx0XpK4SZ7nb
MD5:	6E236887FEB8BB3BDC0090DAA4832576
SHA1:	0C0F3AA18D8E954FFEDEBB73877C82BF471F41C6
SHA-256:	8F64E36A0C0EAC7D5527F9C8FAA0F890CFA0A925E8FB1ECCCE42E6119E0F40B7
SHA-512:	6204F397941993E95F26EC64AA3CFCDA172C3B6325998CFA967D0417D9B8308DB3F8D2D838D38B456817B5E8EC7F006080D4CD5C099D0A2DBD5762E37B8273E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x6dd9d3af,0x01d745bf</date><a ccdate>0x6dd9d3af,0x01d745bf</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>0x6dd9d3af,0x01d745bf</date><accdate>0x6 dda6fe7,0x01d745bf</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):	5.18122454037404
Encrypted:	false
SSDEEP:	12:TMHdNMNxxXy94nWimI002EtM3MHdNMNxxXy94nWimI00Ob6Kq5EtMb:2d6Nxdy94SZHKd6Nxdy94SZ7ob
MD5:	22F62DD9E0C3B3F6093468D1847C2BDE
SHA1:	DA840F1833576FCE396D8CACA766060DBA6D2F0F
SHA-256:	0571B1FC9FC17351408398F6AC6D57C811B332C83574C9E9E871AB3EAF466ED4

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
SHA-512:	CD6BC24ED9ABCBD0A231252143C789A439C2F68D5868653712BCDD2FAFD243314C3A6CD6A43656D5CD5A4FA24CB050AF570BE1DC4E9CFEEE71CD8E2A7A697A1
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x6dd93789,0x01d745bf</date><accdate>0x6dd93789,0x01d745bf</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>0x6dd93789,0x01d745bf</date><accdate>0x6dd93789,0x01d745bf</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):	5.136388909384995
Encrypted:	false
SSDEEP:	12:TMHdNMNxcUms4nWimI002EtM3MHdNMNxcUms4nWimI00ObVEtMb:2d6NxT4SZHKd6NxT4SZ7Db
MD5:	7B808732402B47E31EC156931267BA34
SHA1:	3C8A694E020EC60CE6FE89BBE2B2450B065DE16D
SHA-256:	F8C7E377A24575B3249115218105F93D7A0A67FD4851F0A625DCBE8A2436988A
SHA-512:	1B9AF7199268969A8FBFAC302861935FB44DADEFE4DC18DE0D09D8930C62406B25AE33E8E38D4AD5F408EBD1DC9B5BFA4800801AE6CB52AC99C4F6C856105E93
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x6dd62a3b,0x01d745bf</date><accdate>0x6dd62a3b,0x01d745bf</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>0x6dd62a3b,0x01d745bf</date><accdate>0x6dd62a3b,0x01d745bf</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):	5.105469790969519
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnUOs4nWimI002EtM3MHdNMNxfnUt4nWimI00Obe5EtMb:2d6Nxg4SZHKd6NxS4SZ7ijb
MD5:	1CFE37BC154499CAAEC5B0C1F8800FC1
SHA1:	A70BC25263413E7DD65AC09ACC1819317C74EF56
SHA-256:	FB374941C2D0F3CCAD81C00924085EECFA67281AD3E45745D26C20DE42EEEE48
SHA-512:	37F2AB5F13F8A56E13CF0597F161490AD9D0B4932B333529175DC63CB23CA3230210E701785470E323D59F6FFA9CAA92AE9ECCD258AE5CB602B722B126A3F824
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x6dd6c66a,0x01d745bf</date><accdate>0x6dd6c66a,0x01d745bf</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>0x6dd6c66a,0x01d745bf</date><accdate>0x6dd762ba,0x01d745bf</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	5893
Entropy (8bit):	7.7248999198725885
Encrypted:	false
SSDEEP:	96:ohuQ5Vo7FhknmWpYOxYbOLMHfmH0mgzdtsfNFeC933ktunIOys60yiiLEgY4yJVJ:oEQ07FhknOuM/muPs1Fqmd9nyiiZqL
MD5:	B8F07B749D55F84AC0F9129CC03B6360
SHA1:	1115F73EEF9F380C72FDEC7894FD501FB051D940
SHA-256:	58BAD10A038EC93F434CA165E3FF296E675B9407851F11FCE02B0FF57D3A2092
SHA-512:	5F3C590276CF5B031B43437E1735DE1F9BAAC4E0202B7143F5B45D3A769ED20FE084368474A794077EC8C6FA9D5BBE77D58E316A82D812E6CDCE11D8E2DFBCF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Preview:	(.h.t.t.p.s.:./././.l.o.c.a.l.c.o.r.o.n.a.v.i.r.u.s...c.o.m./.f.a.v.i.c.o.n...p.n.g......PNG........IHDR...@...A.....a5.{...7iCCPAdobe RGB (1998)..(....J.P....E.V...p'QPl...l[. X.C..IC.b.n.... .n.\.}.'G.A..|...C........9....b..Q..X.v......f...N..v.u..'q.......M..4...2..J.#`..e!.....1...j....N.5.O@....P.r..J..|._..s=..9..r_.L.]k.Z...Y.T.eY..&A$.....3....J...Q....`1.l7..V......=...en.G.@,=.YA x...U.;..b.p...azTd.7p....E.Z...<.....O..S?.....pHYs...#...#.x.?v....iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xm lns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xap/1.0 /sType/ResourceEvent#" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\-F63fjptAgt5VM-kVkqdyU8n1i8q0Q[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17868, version 1.1
Category:	downloaded
Size (bytes):	17868
Entropy (8bit):	7.9664031905869646
Encrypted:	false
SSDEEP:	384:9gXBQFQmgBnaQTyky3exU+qwRmwoL2ydtNz1NWTWiVgFCQ:CXBQm9nJT/KldLvHNznckh
MD5:	0C3DB5C13D8FFB2DDD28B9A42A59DC65
SHA1:	B93182204F3E0C0F69AC5085D55325A212A1FC1E
SHA-256:	21DBCB97EE4D5E7F34F98E87A5FAEF3B26CBF3B9A082C32A367E3480F2057E2F
SHA-512:	E5F9F0129B9E9BCC0D9BED6FAC626768BA9E6740DAD0B8B32024FC113E93B1EA9C60AB50BD1DC39B24946C29A81E74B348CA32FFFCE68DE52A4082042BA68 8C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/ibmplexmono/v6/-F63fjptAgt5VM-kVkqdyU8n1i8q0Q.woff
Preview:	wOFF......E................................GDEF.......@...R.d.RGPOS....... ... DvLuGSUB.......*...P.J..OS/2.......Y...`i. vcmap...h...v...,^...cvt ....@...@.6..fpgm... ....s.Y.7gasp........... ...!glyf...,..7...|.J.^head..>....5...6.h.xhhea..>H.......$...Ehmtx..>h...&....3.-.loca..?.........$..maxp..A.... ... .;.Oname..A........x..9epost..B....U.......Vprep..D.........'F.x.....@ @...}.27.1B.....Z.Z....W...Q..d..U..f..Q.q.k<5^..................DFLT...............x.M..npa.E..o...6.._m7n.6....v...F/.'...p.D.p.#..]..P....~.......g=...9.ms..\(....WMCA..^.i.n ...-Ej.p.. pe...8.M....[?.l....PbI%.B*h..N..a.....eQ.cY.gU.`S.d[.bG..@.Q.A..T.A..T.A..T.A..Bp..M..%..kh.l#[.8.U..|./+hO.Q6.b....1.k...7P....L.Bw.'..6....(*..Z..._..'. ,@..6...,..X.'...h.a...x.c`f.`.... .............I.M.....L..L.....@.l.(.t.U`p``P.b.......(...8.$....H)00........x.m.3.U.....m../.q.m.m.m.s..%....~.F.YE..U4......#.b.....h....f....'.gA. w.?..E..A.`x.?...$nY,... .@qeU.N..l...o.>....9.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\15168161373849[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1200x1474, frames 3
Category:	downloaded
Size (bytes):	533468
Entropy (8bit):	7.978764784772052
Encrypted:	false
SSDEEP:	12288:fxY4adgrESOk6UFT62M+EQOR9MmsHm8UejRpL94ZuhV1UmTJU:ZdadgIS7VT6jaOR2mt8ZRXzhV1UmTJU
MD5:	BD25A1C1C570D514F7087FECBECD1247
SHA1:	50CF521D9BE29CDDEA7192F2EDBB6053A40F940C
SHA-256:	8E9C2DA04133E2E1D812C3A426C2728BD6D9D7C6F3F191A050C006282F98771A
SHA-512:	19B08DA48C2B5FEA59BEC4DFE04712772BAA25EFCFDC3D6249AC8BD0DC0725966A1180BC0BD5EF214EA479C67831D82F5890E5503A7478CD92F2EFBDE355A E8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://phantom-expansion.unidadeditorial.es/45a148aa3fab38e202c7b4ba1e15612b/crop/0x0/2048x2515/resize/1200/f/jpg/assets/multimedia/imagenes/2018/01/24/15168161373849.jpg
Preview:	......JFIF.....`.`.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((...`.........................!1.A Q."aq...2..#B....Rb..$3r..C.....4Sc...%Ds..&5Td.6Et....u..e...U.................................l.......................!1..A."Qa.2q.........#BR...3.Sb....Cr.$.Tc..D...............?.. .0.`.MN..5g.O... .D%_.E.&.'.B...#.j<.....m*C..V...<P.|.Y.'&=l.'..*....8.*.;+.-1V...XCO....1...+..'..\S......c..n...Q..rL.K..yD..j...W.f...H..ob.{.Xq9\L.u....#.......6.5'.....T..#.x......#S...7Ez.p...lx..3.Xq...'....... w....7..V.'EjO.E.&X........J...u..3v.i.Z'u6.......{.N..[.3.p...X..c(.-H..Li*P...;....Mk.U....(.MZ...._..).....+.lB..D..7h..i..{7?.P...(.5..g......u.(n...;.Y.2..4S..[X..yx..f..:.PkVp.....wt....T;.N..?y P*<..Q-.a)aK-...9.T...P....`5.9..\[*.T....;..7..?..,.2...=.....8}......lk.L.-v.....S..~ufn...x.?.......D...%.^..M...t.v.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\72ad27b33e759b00fd877f033fbd4a79[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	34101
Entropy (8bit):	5.4442031886845745
Encrypted:	false
SSDEEP:	768:MYlgXjHxIRM4Y0sIFe9/pPPRHYmTrH9Kz+2o7H:MYl0jl43+/pPd
MD5:	72AD27B33E759B00FD877F033FBD4A79
SHA1:	CDA919082E8920AF2DF1AC6B76B6F69463BC870D
SHA-256:	A58367C4FACF289E6A8FC5402788855E13A43A05E091E1278D4B53F18C384C83
SHA-512:	DDB483679CB99C1F47532C9172CFD9F76ACA82580AEBE7866526714AFBD40B5316F6A95A54B9CA19A370C81A401671BA242851B9A38E0F7C5DBB78637A427DC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/mysidia/72ad27b33e759b00fd877f033fbd4a79.js?tag=mysidia_one_click_handler_one_afma

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\72ad27b33e759b00fd877f033fbd4a79[1].js	
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var q;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 glob al&&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 r=ca(this);function da(a,b){if(b)a:{var c=r;a =a.split(".");for(var d=0;d<a.length-1;d++){var f=a[d];if(!(f in c))break a;c=c[f]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&ba(c,a,{configurable:!0,writable:!0,value: b})}}.da("Symbol",function(a){function b(h){if(this instanceof b)throw new TypeError("Symbol is not a constructor");return new c(d+(h||"")+"_"+f++,h)}function c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\O29Y8020[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 980x550, frames 3
Category:	downloaded
Size (bytes):	93130
Entropy (8bit):	7.967914266793821
Encrypted:	false
SSDEEP:	1536:hH1xp6+9cn7QURnQOEe//xRpdxzvRN4XCA5AHrInlKK9vP56hGSA9jzd5DAYzMS:hjp6+9c7pWOEebpdxzv34XeEK2vohNqP
MD5:	F852F9779592FC0A075F9BE15FC62B9B
SHA1:	ABC701A7EB2572BA7815EE351D88346E7AA024CC
SHA-256:	070F00013798CF2F7579116CC9AA50A3249A5BF74146817A91ACDE321DA8056C
SHA-512:	87C3F72A752B77E5092AD28BC0F0355C9AFEF26C2B2AD85FE4ABC6E812E71547A2329D008DC04D73B774EEACB134688E2AC819CDD79FA4F58ADECD825B071 CF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.lavozdegalicia.es/default/2021/05/09/00121620573842504277471/Foto/O29Y8020.jpg
Preview:	......JFIF.....H.H.....XICC_PROFILE.....HLino....mntrRGB XYZ .....1..acspMSFT....IEC sRGB.....-HP .....cprt...P...3desc.....lwtpt.. .....bkpt.....rXYZ.....gXYZ...,....bXYZ...@....dmnd...T...pdmdd.....vued...L....view.....$lumi.....meas.....$tech...0....rTRC...<....gTRC...<....bTRC...<....text....Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1.....XYZ .....Q.....XYZ .....XYZ .. ....o...8.....XYZ .....b.....XYZ .....$.....desc.....IEC http://www.iec.ch.....IEC http://www.iec.ch.....desc.....IEC 61966-2.1 Default RGB colour space - sRGB.....IEC 61966-2.1 Default RGB colour space - sRGB.....desc.....,Reference Viewing Condition in IEC61966-2.1.....,Reference V iewing Condition in IEC61966-2.1.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ZLRC4GGW.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	19068
Entropy (8bit):	4.878838709954877
Encrypted:	false
SSDEEP:	384:ceYbOhw8HTDe4mHR1av2WjAESYhrlXUd63q1OOigM:9YOGfLYXXUo3O+D
MD5:	F9B51E1F350504CE873A01C9F5F7E6F4
SHA1:	B817CB420B8EA86156C37CA2FF24996FFAAAC1A5
SHA-256:	EE5E46AA94647590727B09C3CFC5FB156030BE7574BE4E6B4AC01D8D6C2DDE43
SHA-512:	A92E0453DF16DF7615AF3CEA7ADE292078966C0AADE21C253437F4B3CAD916D77314B6DE22F26DC06F86AD8B81497E69796E3C7A66418DE46953044EABF20BD B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19tracking.narrativa.com/
Preview:	<!doctype html>.<html lang="en">..<head>. <meta charset="utf-8">. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">. <meta name="description" content="Proyecto de seguimiento del COVID19. Narrativa">. <meta name="author" content="Narrativa">.. <title>Proyecto de Seguimiento del Coronavrius COVID-19. Narrativa</title>.. <link rel="canonical" href="https://covid19tracking.narrativa.com">.. Bootstrap core CSS -->. <link rel="stylesheet" href="https://fonts.googleapis.com/css?family=IBM+Plex+Mono">. <link rel="stylesheet" href="https://fonts.googleapis.com/css?family=IBM+Plex+Sans">. <link rel="st ylesheet" href="https://covid19tracking.narrativa.com/v2/bootstrap-4.4.1-dist/css/bootstrap.css">. <link rel="stylesheet" href="https://covid19tracking.narrativa.com/v 2/bootstrap-4.4.1-dist/css/custom.css">. <link rel="stylesheet" href="bootstrap-4.4.1-dist/css/custom.css"> -->... <script src="https://kit.fontawe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ads[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	71562
Entropy (8bit):	6.113959415653385
Encrypted:	false
SSDEEP:	768:aj9loMpWyoDGNWqCq2BVgeoMR1xS0RFmTCntA:I92yoDGNmZVoqxS0R85
MD5:	B93B663B1E6B7C26502B324300A2F108
SHA1:	7F02DDE70690C5722FB715F64C81DF6E4B47A7EE
SHA-256:	82A0AFCECF2DF97D154C8CBFB295E244D7116298250806409862DF8FFF9C0B43
SHA-512:	FCDC5D0B71BAA2C7DDE034CCF5A3958A9065026AE73086734E62E75B41B8D118FDBDEFB354BE160BF26498EC767FBF46E27B44CF9556A72CD19E9FD4F69C1B 5D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ads[1].htm	
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&h=280&adk=167372081&adf=1884181689&pi=t.aa~a.140049771~rp.1&w=1140&fwrn=4&fwrnh=100&lmt=1620666653&rafmt=1&to=qs&pwprc=4903144676&psa=1&format=1140x280&url=https%3A%2F%2Flocalcoronavirus.com%2F&flash=29.0.0&fwr=0&pra=3&rpe=1&resp_fmts=3&wgl=1&fa=40&dt=1620666653086&bpp=7&bdt=11708&idt=-M&shv=r20210505&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D246690374f7834b9-22e1539e0cc8007f%3AT%3D1620634217%3ART%3D1620634217%3AS%3DALNI_MaaSjGCWhXUyvXhhwrCEe0XJNKY9A&prev_fmts=0x0%2C1280x906&nras=3&correlator=4671373740448&frm=20&pv=1&ga_vid=554974179.1620666615&ga_sid=1620666647&ga_hid=935575969&ga_fc=0&u_tz=-420&u_his=1&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=70&ady=1434&biw=1280&bih=906&scr_x=0&scr_y=0&eid=44739524%2C31060711&oid=3&pvsid=4152744826714899&pem=88&eae=0&fc=1920&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=128&bc=1&ifi=3&uci=a!3&btvi=1&xpc=fq42uB7r0w&p=https%3A//localcoronavirus.com&dtd=134
Preview:	<!DOCTYPE html><html lang=es><head><meta charset="UTF-8"><script>var jscVersion = 'r20210505';</script><script>var google_casm=[];</script><style>HTML,BODY{height:100%;width:100%;margin:0;padding:0;overflow:hidden;}#mys-wrapper{height:100%;width:100%;overflow:hidden;position:absolute;top:0;left:0;align-items:center;display:flex;justify-content:center;line-height:normal;}.mys-wrapper A,.mys-wrapper A:visited,.mys-wrapper A:hover,.mys-wrapper A:active{color:inherit;cursor:pointer;text-decoration:inherit;}[dir=rtl] .flip-on-rtl{transform:scale(-1,1);transform-origin:center;}#mys-content{flex-shrink:0;position:relative;overflow:hidden;z-index:0;}</style><style x-ns-sdr30-l="banner-large-vanilla" x-phase="assemble">.ns-sdr30-l-banner-large-vanilla{opacity:.01;position:absolute;top:0;left:0;display:block;width:1140px;height:280px;}.ns-sdr30-e-0{line-height:1.3;border-color:#e6e7e8;border-style:solid;border-width:1px;box-sizing:border-box;display:-ms-flexbox;display:flex;-ms-flex-direction:co

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\angular[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	146434
Entropy (8bit):	5.3893877781701205
Encrypted:	false
SSDEEP:	1536:SDHxxf6y3U3OXsMKQ9/+UDWbgVRuVhOBnrTjCPLPbMe6K44qyEinaI9liHaLekyP:S7bEamUZVf3C8xKZXa3e+Yo4slTq
MD5:	E2FBE57C565AE7F43F366C970DE7386A
SHA1:	BE32C785E8859473CFABB611535452562079D5ED
SHA-256:	22B835B31BDC5147EAF4649997A999290B28D1FB65FA4E763C80A011CF2AE0E5
SHA-512:	6E3F4C575006A67D605986C98D8BE1CB128AF54583D22746E2D6A53211E8C81BE94C7AFB676AD6B40D21488ABDCAB50C1E0C2BBADF9CDCA5E1FBC8D2252B026
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/js/angular.js
Preview:	(function(N,W,u){'use strict';function G(b){return function(){var a=arguments[0],c;c="["+(b?b+":":"")+a+"] http://errors.angularjs.org/1.4.5/"+(b?b+"/":"")+a;for(a=1;a<arguments.length;a++){c=c+(1==a?"?":"&")+"p"+(a-1)+"=";var d=encodeURIComponent,e;e=arguments[a];e="function"==typeof e?e.toString().replace(/ \{[\s\S]*$/,""):"undefined"==typeof e?"undefined":"string"!=typeof e?JSON.stringify(e):e;c+=d(e)}return Error(c)}}function Da(b){if(null==b||Ya(b))return!1;var a="length"in Object(b)&&b.length;return b.nodeType===pa&&a?!0:H(b)||K(b)||0===a||"number"===typeof a&&0<a&&a-1 in b}function n(b,a,c){var d,e;if(b)if(B(b))for(d in b)"prototype"==d||"length"==d||"name"==d||b.hasOwnProperty&&!b.hasOwnProperty(d)||a.call(c,b[d],d,b);else if(K(b)||Da(b)){var f="object"!==typeof b;d=0;for(e=b.length;d<e;d++)(f||d in b)&&a.call(c,b[d],d,b)}else if(b.forEach&&b.forEach!==n)b.forEach(a,c,b);else if(lc(b))for(d in b)a.call(c,b[d],d,b);else if("function"===typeof b.hasOwnProperty)for(d in b)b.hasOwn

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\app[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2579
Entropy (8bit):	4.949620805821966
Encrypted:	false
SSDEEP:	48:MWtqx0PXRF9l09x0VF9l4x0PdvF939xOF9a9xiF9lX:MWtqy5loyFl4ylTtq2ilX
MD5:	6F4BC6EFFB9551DDA2CFFB046D0870DA
SHA1:	817DCDC17C7CB18828C2BC70A5A31884329D36A5
SHA-256:	F42C6E973109750DE6D8456C021B9369CBD9AD24E99635A6CECF8BF4ADD9D075
SHA-512:	3CDEED209A0F797AC226D474A1220AFC8C96A18CFFF594C9C2A23315624FDB8C4AD5BB9AAA19CA134DD89366EE23B62F80231CC54C7373AE252941014107BAE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/js/app.js
Preview:	var websiteApp=angular.module('websiteApp',[]);websiteApp.controller('FormController',function($scope,$http,$timeout){$scope.successStatus=true;$scope.formData={};$scope.checkOption=function(){$scope.selectOption=false;}.$scope.submitcotactusForm=function(data){$scope.successStatus=true;if(data==true){if(!$scope.formData.selectOption).$scope.selectOption=true;return false;}.else{$scope.message="".$http({method:'POST',url:'process.php',data:$.param({data:$scope.formData,gcapcha:a:document.getElementById("g-recaptcha-response").value,pageId:'contactUs'}),headers:{'Content-Type':'application/x-www-form-urlencoded'}}).success(function(data){$scope.successStatus=false;$scope.formData={};$('#success').fadeIn(1000);$timeout(function(){$('#success').fadeOut(10000);},10000);});};$scope.footerformData={};$scope.successStatus=true;$scope.submitfooterForm=function(data){$scope.successStatus=true;var status=true;if(data){return false;}.else{$http({method:'POST',url:'process.php',data:$.param({data:$

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bootstrap[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	197219

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bootstrap[1].css	
Entropy (8bit):	4.968606270301307
Encrypted:	false
SSDEEP:	1536:Dyy/lspGffCWUQW8znWV64wpHeASzjN+QTzNo+xwwCrd+//zDL4iDF4j3:DxTCWUYz/wC4//zDL4iDF4r
MD5:	BC7CEA8CF9F47F4316A6D5575054EDEE
SHA1:	0A2D6B0472522B1FD04D91A3C21F5AAFCB4977F7
SHA-256:	C3E1D4D469F80D226AEFB03E3EF30C01181438F1BBA0175824DDD3FF7EE046E3
SHA-512:	B81DC287DB09636E977BE7C6D005795C5FA11085BD5C414F9AA89A1757B81BBEA20F790E2D4D8288B1642DC276FDB34E2DD0B1CFD711FFB7667C40BDADA93E7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19tracking.narrativa.com/v2/bootstrap-4.4.1-dist/css/bootstrap.css
Preview:	/*!. * Bootstrap v4.4.1 (https://getbootstrap.com/). * Copyright 2011-2019 The Bootstrap Authors. * Copyright 2011-2019 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.:root {. --blue: #007bff;. --indigo: #6610f2;. --purple: #6f42c1;. --pink: #e83e8c;. --red: #dc3545;. --orange: #fd7e14;. --yellow: #ffc107;. --green: #28a745;. --teal: #20c997;. --cyan: #17a2b8;. --white: #fff;. --gray: #6c757d;. --gray-dark: #000000;. --primary: #007bff;. --secondary: #6c757d;. --success: #28a745;. --info: #17a2b8;. --warning: #ffc107;. --danger: #dc3545;. --light: #f8f9fa;. --dark: #000000;. --breakpoint-xs: 0;. --breakpoint-sm: 576px;. --breakpoint-md: 768px;. --breakpoint-lg: 992px;. --breakpoint-xl: 1200px;. --font-family-sans-serif: -apple-system, BlinkMacSystemFont, "Segoe UI", Roboto, "Helvetica Neue", Arial, "Noto Sans", sans-serif, "Apple Color Emoji", "Segoe UI Emoji", "Segoe UI Symbol", "Noto Color Emoji";. --font-fa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bootstrap[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	46884
Entropy (8bit):	5.097026809641287
Encrypted:	false
SSDEEP:	768:1LBtidRanpFkpHpb76uYdvytNqbdK+KSlEhYAPl641:XIcPhKh+KSZPR
MD5:	1F57084DD4489EB4B77C8F850177A787
SHA1:	BF0C3CF5D9A9775A5C6A73576E2BE1E00CAB6E33
SHA-256:	3684B7CD203DF98651F804F801A62884755D1BC1AF449778E5A51CFF1F563852
SHA-512:	1570700C4620463CF824BA988EC60CCF6E9814CF6E459504915A57F0F360CEA9A645A946C307BDB76F070BA02413DCA615E4882A83D8DCCEAF4DE639CD34CEE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/js/bootstrap.js
Preview:	/*!.* Bootstrap v3.3.5 (http://getbootstrap.com).* Copyright 2011-2015 Twitter, Inc..* Licensed under the MIT license.*/if(typeof jQuery==='undefined'){throw new Error('Bootstrap\'s JavaScript requires jQuery')}.+function($){'use strict';var version=$.fn.jquery.split(' ')[0].split('.').if((version[0]<2&&version[1]<9)||(version[0]==1&&version[1]==9&&version[2]<1)){throw new Error('Bootstrap\'s JavaScript requires jQuery version 1.9.1 or higher')}}(jQuery);+function($){'use strict';function transitionEnd(){var el=document.createElement('bootstrap').var transEndEventNames={WebkitTransition:'webkitTransitionEnd',MozTransition:'transitionend',OTransition:'oTransitionEnd otransitionend',transition:'transitionend'}.for(var name in transEndEventNames){if(el.style[name]!==undefined){return{end:transEndEventNames[name]}}}.return false}.$.fn.emulateTransitionEnd=function(duration){var called=false.var $el=this.$(this).one('bsTransitionEnd',function(){called=true}).var callback=function(){if(!call

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\coronavirus_mapa_localcoronavirus_slide_1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop CC 2018 (Windows), datetime=2020:03:11 15:06:00], baseline, precision 8, 1920x300, frames 3
Category:	downloaded
Size (bytes):	206887
Entropy (8bit):	7.89260750102466
Encrypted:	false
SSDEEP:	3072:VdN9qam4QnzkdaxCkPVOGsHEE8jq59GZgvLfE8u1zXp9xQf7agf3Muf99qVhV:VNqaCpxCC4E/q5mi48uxNQz/hf992
MD5:	2AC5010CB1563099923B56C3476EA347
SHA1:	C56091141290A054F57C52FAE3C18C56F967F0A6
SHA-256:	D21E2127BFF9C55CFE6ED2EE9C702C506938210341D3719C6601961745F1C2B0
SHA-512:	D1BB0351916F52A47F08B5B18FC9489DEAAC3A33C6D8DBA7726DE016841BCDB38D15970DB1692995B6AC39E522113C1ACDD23F4657CFA950C1A9414754011FD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/images/coronavirus_mapa_localcoronavirus_slide_1.jpg
Preview:	.....Exif..MM.*.....b.....j.(.....1....."...r.2.....i.....-....'..-....'.Adobe Photoshop CC 2018 (Windows).2020:03:11 15:06:00.....,.....".....*.(.....2.....H.....H.....Adobe_CM.....Adobe.d.....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?..{.....u7z^.-i.:..>....kE..;...iR5V@.D....'"....1..I.g..e..9.....=...(0.8....f>^.....$...f..qq....y.,.$.F@..H....K.: .x..v.W..NST...?..~.F:.k....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[1].css	
Category:	dropped
Size (bytes):	2906
Entropy (8bit):	5.290227902897662
Encrypted:	false
SSDEEP:	48:xOJa/OWaEOLxHOxTaYOCaLHOw6aJOS7rOJCOWbOLKOgPhOxTAOCuOw6lOMP:xOJa/OWaEOLxHOxTaYOCarOw6aJOS7rN
MD5:	945FB8178712AE2C2DFC24E50A8E49D8
SHA1:	26E232953561D40752A6FEF6C32B7EAEB9B3E4DC
SHA-256:	2E981F3FA57474A381C00BE7390B2E71AF67A5D35D05DEE637C047CAA4AC4E39
SHA-512:	FD2CCF423991D9E24626FB6C7F2A680CAC0CFB99E1542F387BC1773945C0BC0C8C52BEB594AD8285F16C0EAD86327237F75963EC249CCF8D614C8A812AF93DB
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Biryani';. font-style: normal;. font-weight: 200;. src: url(https://fonts.gstatic.com/s/biryani/v6/hv-TlzNxIFoO84YddYQyKTdYVA.woff) format ('woff');.}.@font-face {. font-family: 'Biryani';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/biryani/v6/hv-TlzNxIFoO84YddeAxKTdYVA.woff) format('woff');.}.@font-face {. font-family: 'Biryani';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/biryani/v6/hv-WlzNxIFoO84YdfUsTOg.woff) format('woff');.}.@font-face {. font-family: 'Biryani';. font-style: normal;. font-weight: 600;. src: url(https://fonts.gstatic.com/s/biryani/v6/hv-TlzNxIFoO84YddZQ3KTdYVA.woff) format('woff');.}.@font-face {. font-family: 'Biryani';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/biryani/v6/hv-TlzNxIFoO84YddfA2KTdYVA.woff) format('woff');.}.@font-face {. font-family: 'Biryani';. font-style: normal;. font-weight: 800;. src: url(ht

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	196
Entropy (8bit):	5.25122561532066
Encrypted:	false
SSDEEP:	3:0SYWFFWlIYCQWjh5RI5XwDKLRIHDfFRWdFTfqzrZqcdfFARVgQIAn6UYARNin:0IFFQW5+56ZRWHTizlpdfSUoLNin
MD5:	BD0ED96BADBE38EA6E5C3254D5AA4181
SHA1:	492CF68E6B5A7EE92D4225C48FE23F8295C198CB
SHA-256:	099F1DB7F6020358CD58FE41FF78640D230023FF32D959A779DE88BD23379B52
SHA-512:	76CBB2B08B1217897771C9AD59791F614C0A8C0CF1B31FD1D3C7847F1B893EA806F22733E11FF4B7F8D0C4112B25EAEA2383DD45CE2D672E05BD8F64ECD69C9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=IBM+Plex+Sans
Preview:	@font-face {. font-family: 'IBM Plex Sans';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/ibmplexsans/v8/zYXgKVElMYYaJe8bpLHnCwDKhdHeEw.woff) format('woff');.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\downsize_200k_v1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 399x209, frames 3
Category:	downloaded
Size (bytes):	12005
Entropy (8bit):	7.961418664008049
Encrypted:	false
SSDEEP:	192:Z5AgQs4hCLIijwx/YwnaDLI3+fe4K83CLhrqmmZ50L2Z7tcuoGE9O5HGqilU:vAnDCLIEiwwSL7fuqML2Z7eJ5c5+W

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\downsize_200k_v1[1].jpg	
MD5:	DA27E583D25F82EA4313FE1E53563295
SHA1:	958D50BE5B8508BDB29D31EC1DC57574D4F72700
SHA-256:	6D0E5B5EF2271F46330EF33ED94370A2BFA3FEC5692000A7119145A7750E52D0
SHA-512:	AD4F5A0CDD92B3795A06CCF7F6D491561CE3E3C212728FB1C43465E4CCC6126FB64F7B4BE574ABC9BE149CCB6412CDDF22EB24FCF329A2BE8C4B6C76377C 0FE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/3871948583101367734/downsize_200k_v1?w=400&h=209
Preview:	......JFIF....................................... ."" ...$(4,$&1'..-=-157:::#+?D?8C49:7..........7%.%77777777777777777777777777777777777777777777777777..........".......................................H.......................!.1."2AQaq.#3..R......$4Br.5..Cbst...%cd...ES...........................+....................1.!."2AQ.q..B.#3a.............?..327.).....7.1'...1...!6w$...w"(.[w.r ...2....~.}.k~5n.\.c.Q..."..S../l.k..N3.Z.F.r.#.r...$v.!7.....t...a8c../?.;..R....;.iX4..f5+...ff.[[jX.....e.*`-..q*..+.5.A..{.&.K.5..m.....hQ. .cF.[..T.x.....0....e.&.)...*a$.aJTQ...B..ST..D..P6...x...-~...UI%..8h#.O..n...p...e....6..3.ug.MOe.m.uUt.,O....#Zq.G..0....2.OS..7>..aR+.3Q...oQx....T.c..,M .....A.T..a.H.e. .#o.R.+.0yu[......?fJ.W.}..[.$.f.>IC.2.....??...v.;U..(..c..3. 5....V.WJ..-sA=.....\bJ..if.v...r....i.c8#..l....*.GQ..<...7.>).....m.7W..{.\H.ai.|...%%t5z.z..v.x....."....(wWMJ.i.....M.N......`...E..Qi%F..{C........6.2.+@.....B.^..B..Y.i%A_.%.l....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\downsize_200k_v1[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 600x314, frames 3
Category:	downloaded
Size (bytes):	20999
Entropy (8bit):	7.967120648941552
Encrypted:	false
SSDEEP:	384:1CO+7gt6sYST43odg4UWwolpxMUqfi/bATZfhAsCtrSozGQejSJ2+:1Cs4sYST4Y/UclbMRfiUTPAsCtr3GQoE
MD5:	824449B669C231966447772BD22CC11B
SHA1:	8DD1A086C29864027C8EC9E81479A3F69340A286
SHA-256:	0D66B927623AACB8BCFC7E2EC039F8DA6DF363499EC62C407E3E608A3B6CA3B8
SHA-512:	05E3E0EA1631805B1DD33561858AC4E3D8AB7352B9DF9CEE30BCC7C59AFDA406005188B3213000246A238A21136EC7A6CF5E12E24D5B55DB55D1810ECA27E9 F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/3871948583101367734/downsize_200k_v1?w=600&h=314
Preview:	......JFIF....................................... ."" ...$(4,$&1'..-=-157:::#+?D?8C49:7..........7%.%77777777777777777777777777777777777777777777777777......:.X.."......................................C.......................!1."A.2Qaq#3.....B....$Rr.b4Cc....5S................................*.....................!.1.A"2.BQa..q3C.............?.\...^......F.6..T..H..cd,..G.0.0w.....B..Z .v..G..T.T.`......YG.+..b.M.DQ.. =..KI.E.=.D.].Q..K+I...#./k.Z.^..17Mh.............`.k)...AS..s(.ML.,.c..H.tc.`...#.e.Y.X...R...iM(dm.SY..kIR.d.t..Y.u.......@......d.b.....H.......S(..@..P. )HX.<L`,..y..b.G....d`g.x0Yn..*..6.v...jdc%h... ...c..N#SWOI9...G.i.....kx'J.?..::.SH*j....z..)....Q..C..s........e..3E<R@j...Z]r._.0.uE'..vX....A..K...#.x..6......{F...@G....]....X.BR..zVI# \o...v..U..$J+.:;5.T.%...0..4..P..$....\...8....MQ.#......o.S....;.R....`H.Bt..MC.._%.t....j...`.........R.G...?@.....~......F.~..~S.o0?..G.}.#..IU.$.....Y.I..-qi.......Z.[....r.d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\espana[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	171313
Entropy (8bit):	4.580413615533876
Encrypted:	false
SSDEEP:	768:Y61RgST7w7w4jf2eDnNbF5SHJeaIehcwsWD5CQIZDVeToG0I2n32+TS35UTzkbTV:eknMJh2F
MD5:	62014A8DF56D9D74438AD0777F08DBDB
SHA1:	F3B4E977CAF85DF24823DD175A25194B6B371A9F
SHA-256:	51601E52A7BED7DA2EA5EF31A5DCBEE1E5F3C737AA13E35349937D1B1806414D
SHA-512:	61984B587C48DD86D94EA3BF5DADAEB1429CD6A5323B34809F40F332B2E89CD13DE388D14CB4D3BA42BD01BFB2E58D4E0105C2BFECE3745E04DF810BF0918 65
Malicious:	false
Reputation:	low
Preview:	[{"today_confirmeds":"120","today_deathss":"2","today_intensive_cares":"9","today_open_casess":"105","today_recovereds":"13","today_total_hospitalised_patients" :"31","date":"2020-03-09","today_new_confirmeds":"28","today_new_deathss":"0","today_new_intensive_cares":"3","today_new_open_casess":"23","today_new_ recovereds":"5","today_new_total_hospitalised_patientss":"15"},{"today_confirmeds":"2336","today_deathss":"34","today_intensive_cares":"110","today_open_casess" :"2139","today_recovereds":"163","today_total_hospitalised_patients":"50","date":"2020-03-10","today_new_confirmeds":"746","today_new_deathss":"11","today_new_i ntensive_cares":"26","today_new_open_casess":"686","today_new_recovereds":"49","today_new_total_hospitalised_patientss":"19"},{"today_confirmeds":"221","today_d eathss":"7","today_intensive_cares":"17","today_open_casess":"199","today_recovereds":"15","today_total_hospitalised_patients":"76","date":"2020-03-11","today_n ew_confirmeds":"89","today_new_deathss":"3","today

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\espana[2].json	
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):	171313
Entropy (8bit):	4.580413615533876
Encrypted:	false
SSDEEP:	768:Y61RgST7w7w4jf2eDnNbF5SHJeaIehcwsWD5CQIZDVeToG0I2n32+TS35UTzkbTV:eknMJh2F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\espana[2].json	
MD5:	62014A8DF56D9D74438AD0777F08DBDB
SHA1:	F3B4E977CAF85DF24823DD175A25194B6B371A9F
SHA-256:	51601E52A7BED7DA2EA5EF31A5DCBEE1E5F3C737AA13E35349937D1B1806414D
SHA-512:	61984B587C48DD86D94EA3BF5DADAEB1429CD6A5323B34809F40F332B2E89CD13DE388D14CB4D3BA42BD01BFB2E58D4E0105C2BFECE3745E04DF810BF0918 65
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/includes/json/espana.json
Preview:	[{"today_confirmeds":"120","today_deathss":"2","today_intensive_cares":"9","today_open_casess":"105","today_recovereds":"13","today_total_hospitalised_patients" :"31","date":"2020-03-09","today_new_confirmeds":"28","today_new_deathss":"0","today_new_intensive_cares":"3","today_new_open_casess":"23","today_new_ recovereds":"5","today_new_total_hospitalised_patientss":"15"},{"today_confirmeds":"2336","today_deathss":"34","today_intensive_cares":"110","today_open_casess" :"2139","today_recovereds":"163","today_total_hospitalised_patients":"50","date":"2020-03-10","today_new_confirmeds":"746","today_new_deathss":"11","today_new_i ntensive_cares":"26","today_new_open_casess":"686","today_new_recovereds":"49","today_new_total_hospitalised_patientss":"19"},{"today_confirmeds":"221","today_d eathss":"7","today_intensive_cares":"17","today_open_casess":"199","today_recovereds":"15","today_total_hospitalised_patients":"76","date":"2020-03-11","today_n ew_confirmeds":"89","today_new_deathss":"3","today

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\feedback_grey600_24dp[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 48 x 48, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	205
Entropy (8bit):	6.471232950817362
Encrypted:	false
SSDEEP:	6:6v/lhPmvbPM6ArwrgPowQka3cQhWb8i4NI1Q/2up:6v/7OvzZ6IRwIcQEb7461Q2c
MD5:	4087858E2C9DB9AA8F6A840AEDCFB533
SHA1:	D1FFE861DA6BD0E95FD1A365B0C3D3CEB6CD58A3
SHA-256:	4D45982F2DC34F36C9045EE46A75A1943666BB7FD64E103CAC8C7429E7012840
SHA-512:	541228667C513266FFAC017AA43CCACEA410E20BF27D30599276E9984FAC2C433AC58288C19F7A5BFEB1C9B4074B8C9C472080BF1C706303F97B2CE73DBD634
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/images/icons/material/system/2x/feedback_grey600_24dp.png
Preview:	.PNG.....IHDR...0...0.....1.....IDATx...1..1.DQ.f....@H.....%`..j.M&"....5...;...;.....\.....\..U.4..pe.<.P.....%... ...@....p.....@...X...5..{.$.x^....y=..z.....|.....+.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fontawesome-webfont[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), FontAwesome family
Category:	downloaded
Size (bytes):	68875
Entropy (8bit):	7.983346521768067
Encrypted:	false
SSDEEP:	1536:snQ7kmhONxJ4LAZVYamTFvefF35ZP5DwSieQX3wXSBxPQ:sRmafwVamliF/uZeoFx
MD5:	45C73723862C6FC5EB3D6961DB2D71FB
SHA1:	B3C2F08E73320135B69C23A3908B87A12053A2F6
SHA-256:	D4F5A99224154F2A808E42A441DDC9248FFE78B7A4083684CE159270B30B912A
SHA-512:	299BF41DA0CA937F4F5A0BC3FDD65EF7B53DF30E10554841004F9EB10C97B25BE1D4E21B6D00B2A405693D5ABAF87CF6A16A5AF2C680C09B25E5F5490D88EB E5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/fonts/fontawesome-webfont.eot?
Preview:	....%.....LP.....^ >.....F.o.n.t.A.w.e.s.o.m.e.....R.e.g.u.l.a.r...$.V.e.r.s.i.o.n. .4...4...0. .2.0.1.5...&.F.o.n.t.A.w.e.s.o.m.e. .R.e.g.u.l.a.r..... BSGP.....!.....Y.D.M.F..x...>.....)Y.....h..D....pj....K.....*....0....~.71.^..{.+rAP..u;..3.K.?].:..y..f..`..o.....&.d:.e.DgK...R..%.....q..H...:.....<Bt....]....Nbf..JH.%....~ ..S...G...8.I.a.U.-&..q..1...#`U.....W.L.g.E. q...y..:..g$8..eAV..3.e....u.j...z..i.@.....a.=%.0..O.\O... "3..ef.0c..@...$.....*...qD..E.".(./.Jv.....,^&N?.'c....-.1f*.}.....)..k\eL...e.....8 6Qp...f.vX...*X..C.;Ve..P CKW.a.Z..d....?.pK.U.<T.....I.....RT.....$*.Q.....YE.....e...OI....!.....FE].CE..r>.s..d.W....*0#....Q.T.....:...b....#...@Ym...{..D.t.....!..Z....d.....S. .....Qv'...x...U.L.89.....96.....,.Be.....r.R...+5....XW.....N.J.._;.J.....%.$...-n.pr..t....pL...V..{..@....L....."7....B...|..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\free-fa-brands-400[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Brands Regular family
Category:	downloaded
Size (bytes):	134346
Entropy (8bit):	6.285893732206211
Encrypted:	false
SSDEEP:	3072:BhPzoVcBscZS23Dukm6YSaj57FCvhf4UkWvLf:BhroVZifDfYN9kvhvvzf
MD5:	579CB5E5782CC1B0B5A05BC6C93DB68E
SHA1:	F8F83E4D27BDA632138CA19B370C8D14EE09BAA6
SHA-256:	D743B77099213F3D9BB6824B72145B3E0BD40D466BC7DBCC9AAAF82DA399E990

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\free-fa-brands-400[1].eot	
SHA-512:	FD71F2F773C766805DC1B84440C5835900063DECCF8ADB7D45901F08F2B7C5F8A1558D9011C2E0690603036ED9BAEC666955967DBCA1C272770707C075036C4E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.3/webfonts/free-fa-brands-400.eot?
Preview:	.....LP.....0..M.....:.F.o.n.t. .A.w.e.s.o.m.e. .5. .B.r.a.n.d.s. .R.e.g.u.l.a.r.....R.e.g.u.l.a.r...L.3.3.1...5.2.3. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r.s.i.o.n.:. .5...1.5...3.)...:.F.o.n.t. .A.w.e.s.o.m.e. .5. .B.r.a.n.d.s. .R.e.g.u.l.a.r.....PFFTM.._:...|....GDEF.*.....\....OS/21.V:...X...`cmap.!q.....gasp.....T....glyf.1.....x ....head.....6hhea.6.....$hmtxqD.....0loca.+Z~.....maxp.5.@...8... name.....`....postZGjY.....k.....K..M..0_.<.....v|2.....v|3..... ....='.....@.....L.f...G.L.f.....PfEd.....T.....:..... .....@. .....@.....@..... .....@.....@.....@.....p....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\free-fa-regular-400[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free Regular family
Category:	downloaded
Size (bytes):	34034
Entropy (8bit):	6.323740915979423
Encrypted:	false
SSDEEP:	384:TsILh/4eF1sQQbC5LbC4TH/s+v4B3Q89h8g6WIHL8ScQU5:TPLZ49tep3/8Bn9vIHL8ScQU5
MD5:	2FF042159499ED1D620A024733E4F65C
SHA1:	2FD0833B9EC62A4BCC13A8E0D23DC150DA0AEA58
SHA-256:	5C46B816B52A8468D6395A1FDA444481AD87779708D2A8CF74674CD2DA068BED
SHA-512:	DB54BAFE1EE611F475ADF5A0724BA801ADA5486D42F3029EDE698706512FEB952EC4AA4DDC804BA9AF88FC5ED34C53F21CB2F3D48249382EC3878A2CDF1012A3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.3/webfonts/free-fa-regular-400.eot?
Preview:	.....LP.....6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....R.e.g.u.l.a.r...L.3.3.1...5.2.3. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r.s.i.o.n.:. .5...1.5...3.)...6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....PFFTM.._5.....GDEF.*.....OS/2A.S....X...`cmap.....gasp.....glyf.;y.... ..m\head.....6hhea.5.....$hmtx...t.....Tloca..H.....6maxp.....8... name:.>"..v|...[post.iA...{.....K.....<.....v|-.....v|3.....@.....L.f...G.L.f.....PfEd.....T.....:..... .....@.....@.....@.....@.....@...@.....@...@.....`..... .....@.....@.....@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\free-fa-solid-900[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free Solid family
Category:	downloaded
Size (bytes):	203030
Entropy (8bit):	6.347367233249361
Encrypted:	false
SSDEEP:	6144:ZtrDdlZG2nqJElpL3im9+3Kz9BngKbtPLLd5Mn:36TnSEl1yt6zzng0Lu
MD5:	D5DE805D9CC4E0665FB04CA2D2336EE8
SHA1:	89D5DBEBA993F33C0B5BE98C0DF0D87B03AD1B37
SHA-256:	BC0CCA590079A0D7921FF7445BB4EBD55928D00ADA1C9E6F41E16918AAFC8171
SHA-512:	576721318162E4E82F50D624EA37382CB52137332FBA5B4A868EB4D67F591CFB5F3E3A35D658EBE0A791625006294CA09C50B61D0A83E96A3E9837E20A233D08
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.3/webfonts/free-fa-solid-900.eot?
Preview:	.....LP.....W.ve.....2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o.l.i.d.....S.o.l.i.d...L.3.3.1...5.2.3. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r.s.i.o.n.:. .5...1.5...3.)...2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o.l.i.d.....PFFTM.._6.....GDEF.*.....OS/23.V`...X...`cmap.j.4...h....gasp.....glyfT....-....lhead.....6hhea.C.-.....$hmtx.....loca..jD...8....maxp.N.]...8... name%.1....X...+post..Fa.....1.....K..ev.W_.<.....v|.....v|3.....Z. .....@..... .....L.f...G.L.f.....PfEd.....T.....:..... .....@.....@. .....@.....@.....@..... .....@.....`.....@.....@.....@.....@....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\httpErrorPagesScripts[1]	
Reputation:	low
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery-1.11.3.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	95957
Entropy (8bit):	5.39099763946861
Encrypted:	false
SSDEEP:	1536:OP10iSi65U/dXXeyhzeBuG+HYE0WEeLDFoNqLTW8+S5VRZIVI6xSb8xh2ZbQnRmc:R+41ZqLTW8xRrqSb8qGH77da98Hrf
MD5:	895323ED2F7258AF4FAE2C738C8AEA49
SHA1:	276C87FF3E1E3155679C318938E74E5C1B76D809
SHA-256:	ECB916133A9376911F10BC5C659952EB0031E457F5DF367CDE560EDBFBA38FB8
SHA-512:	C40111C3CC0754E90CF71F72F7F16F43B835B7E808423DFD99F90DD5177538B702E64FF1D9EE8D3BC86AEAA11B6F7A0EF826184E354B162158839FFB75D174C(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/js/jquery-1.11.3.min.js
Preview:	/*! jQuery v1.11.3 | (c) 2005, 2015 jQuery Foundation, Inc. | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l="1.11.3",m=function(a,b){return new m.fn.init(a,b)},n=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,o=/^-ms-/,p=/-([\da-z])/gi,q=function(a,b){return b.toUpperCase()};m.fn=m.prototype={jquery:l,constructor:m,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=m.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return m.each(this,a,b)},map:function(a){return this.pushStack(m.map(this,function(b,c){ret

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.revolution2[1].js	
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):	2076
Entropy (8bit):	5.127084396933464
Encrypted:	false
SSDEEP:	48:uxL+30E7fnJaV18GMgkjx4htDzY3asN+AJslU3gewDaus464gJgdyBi52e:uluFnMMEzOL+AtgzDaL/ZJgdyBi3
MD5:	7DF34DFBE6CAE6037D92D7D4A1C50248
SHA1:	DB0CF130A10F72F8E5B38DFB36A820D991E2ADB7
SHA-256:	2C66256720115B85BF2434D382E9621870C379AB08FFC05771973CDD03367AF9
SHA-512:	4C0C5CA3FBA761BE1B92E01EF4B42B8CFE7CF0FF6AABAAA547ED3FD2450B19B0B64571B71BE3B6AAD63035FA66F50C464DA81FDA3072F8FF687147DBD79C553F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/js/jquery.revolution2.js
Preview:	var tpj=jQuery;var revapi34;tpj(document).ready(function(){if(tpj("#rev_slider_34_1").revolution==undefined){revslider_showDoubleJqueryError("#rev_slider_34_1");}else{revapi34=tpj("#rev_slider_34_1").show().revolution({sliderType:"standard",jsFileLocation:"assets/",sliderLayout:"fullwidth",dottedOverlay:"none",delay:4000,navigation:{keyboardNavigation:"on",keyboard_direction:"horizontal",mouseScrollNavigation:"off",onHoverStop:"on",touch:{touchenabled:"on",swipe_threshold:75,swipe_min_touches:1,swipe_direction:"horizontal",drag_block_vertical:false},arrows:{style:"gyges",enable:true,hide_onmobile:false,hide_over:778,hide_onleave:false,tmp:'',left:{h_align:"right",v_align:"bottom",h_offset:40,v_offset:0},right:{h_align:"right",v_align:"bottom",h_offset:0,v_offset:0}},tabs:{style:"erinyen",enable:true,width:250,height:100,min_width:250,wrapper_padding:0,wrapper_color:"transparent",wrapper_opacity:"0",tmp:' {{title}} {{description}}</

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.themepunch.revolution.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	46395
Entropy (8bit):	5.22671237988595
Encrypted:	false
SSDEEP:	768:+s8axW3CvO++P3yp+KqbwgdJncRwrsM//Gm9K8WxzvCkPKBXLn:+s8aM3Cvr+vyp+NbwgdJncU//fK5VCkK
MD5:	5B265D7036C5738DD9A638C435241F72
SHA1:	440E3ACB5316BCDA701DD13714E0D4B27EF95B61
SHA-256:	813FCB4E4CBE9877CAE2CD703A9002A809E47B86E1A5699A578BC21CE103331C
SHA-512:	75B5A81F0112FF5087D9641FB924588ACEF42EA72E9B6CB42C7E4DAFAF7DBD81C4561FC2796654F460DFBC197CAE107D950F4DD72FD8B0335E2820CB2FC8AC5
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.themepunch.revolution.min[1].js	
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/js/jquery.themepunch.revolution.min.js
Preview:	/**********. * jquery.themepunch.revolution.js - jQuery Plugin for Revolution Slider. * @version: 5.1 (20.10.2015). * @requires jQuery v1.7 or later (tested on 1.9). * @author ThemePunch.**********/.!function(e,t){"use strict";e.fn.extend({revolution:function(a){var n={delay:9e3,responsiveLevels:4064,visibilityLevels:[2048,1024,778,480],gridwidth:960,gridheight:500,minHeight:0,autoHeight:"off",sliderType:"standard",sliderLayout:"auto",fullScreenAutoWidth:"off",fullScreenAlignForce:"off",fullScreenOffsetContainer:"",fullScreenOffset:"0",hideCaptionAtLimit:0,hideAllCaptionAtLimit:0,hideSliderAtLimit:0,disableProgressBar:"off",stopAtSlide:-1,stopAfterLoops:-1,shadow:0,dottedOverlay:"none",startDelay:0,lazyType:"smart",spinner:"spinner0",shuffle:"off",viewPort:{enable:!1,outof:"wait",visible_area:"60%"},fallbacks:{isJoomla:!1,panZoomDisableOnMobile:"off",simplifyA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.themepunch.tools.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	104627
Entropy (8bit):	5.453416083788646
Encrypted:	false
SSDEEP:	3072:iSICVnIZ6Qw/72VcPTYld0pQTHyLE7ryx:iSIEnI0QwiVk6SGHyLE7U
MD5:	98ABAE2BEADBFDAD0DCC77994E08663C
SHA1:	71C896294278693680 96A28FB6917C01BB520F1E
SHA-256:	7C98661F1D1E8C9520747DC08681752E45CF4C5D3CEB1D28642CFDCAFC10E896
SHA-512:	B6A7E2A056B2A5E1300F0EF438D1839D25B1E502397BD7CF78F1B84DC65AC5792CB4DB8D329661EA03E1090EADD7024889A5B6CAA733609D9D9312069C0F773
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/js/jquery.themepunch.tools.min.js
Preview:	/**********..-.THEMEPUNCH TOOLS Ver. 1.0 -.. Last Update of Tools 27.02.2015.**********/.../*.* @fileOverview TouchSwipe - jQuery Plugin.* @version 1.6.9.*.* @author Matt Bryson http://www.github.com/mattbryson.* @see https://github.com/mattbryson/TouchSwipe-Jquery-Plugin.* @see http://labs.skinkers.com/touchSwipe/.* @see http://plugins.jquery.com/project/touchSwipe.*.* Copyright (c) 2010 Matt Bryson.* Dual licensed under the MIT or GPL Version 2 licenses..*.*/...(function(a){if(typeof define==="function"&&define.amd&&define.amd.jQuery){define(["jquery"],a)}else{a(jQuery)}}(function(f){var y="1.6.9",p="left",o="right",e="up",x="down",c="in",A="out",m="none",s="auto",l="swipe",t="pinch",B="tap",j="doubletap",b="longtap",z="hold",E="horizontal",u="vertical",i="all",r=10,g="start",k="move",h="end",q="cancel",a="ontouchstart" in window,v=window.navigator.msPointerEnabled&&!window.navigator.pointerEnabled,d=window.navi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\less[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	58340
Entropy (8bit):	5.353396398134769
Encrypted:	false
SSDEEP:	1536:EMqHjUn7LPtTj0BBtN4enUNp+GTj4EstFvM7aignjNKwDQR0w:JnOBBGv
MD5:	ED1DA2AC01AA1ED3DF7F35A5EA59406D
SHA1:	1A7E908E454BC79EFD4B1B0BD6E2CE4B171C5EA1
SHA-256:	C89D024AC83B837C05981B38F80B2D248CF248A506524A693E3B1D5A900E9CD4
SHA-512:	3016E2A24AC50CA85F99714CEF35C708303D35C161BDB0D35FD8F6E44E5C9CF55FBFB668F093B267E8C1D794E2FB28183498DCEC04A4DD852354AB7FA72AAD1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/js/less.js
Preview:	(function(e,t){function n(t){return e.less[t.split("/")[1]]}.function f(){r.env==="development"?(r.optimization=0,r.watchTimer=setInterval(function(){r.watchMode&&g(function(e,t,n,r,i){t&&S(t.toCSS(),r,i.lastModified)})},r.poll)):r.optimization=3}.function m(){var e=document.getElementsByTagName("style");for(var t=0;t<e.length;t++).e[t].type.match(p)&&(new r.Parser({filename:document.location.href.replace(/#.*$/,""),dumpLineNumbers:r.dumpLineNumbers})).parse(e[t].innerHTML||"",function(n,r){var i=r.toCSS(),s=e[t];s.type="text/css",s.styleSheet?s.styleSheet.cssText=i:s.innerHTML=i})}.function g(e,t){for(var n=0;n<r.sheets.length;n++).w(r.sheets[n],e,t,r.sheets.length-(n+1))}.function y(e,t){var n=b(e),r=b(t),i,s,o,u,a="";if(n.hostPart!==r.hostPart).return "";s=Math.max(r.directories.length,n.directories.length);for(i=0;i<s;i++).if(r.directories[i]!==n.directories[i]).break;u=r.directories.slice(i),o=n.directories.slice(i);for(i=0;i<u.length-1;i++).a+="../";for(i=0;i<o.length-1;i++).a+=o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\madrid[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 75", baseline, precision 8, 1200x675, frames 3
Category:	downloaded
Size (bytes):	84814
Entropy (8bit):	7.954496066185703
Encrypted:	false
SSDEEP:	1536:iVbRV0sFwKRcHz86wSGv8S43fjSesgzYBQ/sGOWGxlf9Y+xpVI/GkSisk:oRuYR4aE32wnsF9bHVlj0k
MD5:	98F10F7E6DA555278FEE7A64EAD7E93D
SHA1:	217B7CCCD2D8958599550F668FB50519D35D0313
SHA-256:	14964D2349E8E8BE27E76FA1FFF90995E2A7A2E19C11F86E8B52BD9F2437974F
SHA-512:	FBC0820AB3173814A9DC6E714BB66002541FAFCF94C9728CB5D4F6BE490EED5A612DBB9A62E8668025BDF27F1E836A6712CB873712C0758B5450AC3D20C6FD4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\madrid[1].jpg	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://imagenes.20minutos.es/files/og_thumbnail/uploads/imagenes/2021/05/09/madrid.jpeg
Preview:	......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 75....C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222 2222222222222222222222222222222222222222..........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTU VWXYZcdefghijstuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEF GHIJSTUVWXYZcdefghijstuvwxyz...?....(... (...(..g..}...U...d..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\more_vert_white_48dp[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 96 x 96, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	233
Entropy (8bit):	6.66066908308459
Encrypted:	false
SSDEEP:	6:6v/lhP2HPr8XzFTBS7wmJymSMvgPeO8DLHTkHsWIhAblVp:6v/7coTBS7wmJhFvQt0HTx1hAB7
MD5:	8BBCFD6FD59DF71682723841BFD0B533
SHA1:	0826F7230D57DEF27AE74BE14DDC76C1478457AE
SHA-256:	B68D6252E63C5207F080A8969AA75600D5D252F67D454FD9A0A8A7E3E89D0686
SHA-512:	A0EEAAE90590B852681C38F14FB328F2707C9A623953B16CE937363655044D3168C3D8E8F200722C1E42BF71189165E602C697316CC8F4ADBBA399C83392E56B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/images/icons/material/system/2x/more_vert_white_48dp.png
Preview:	.PNG........IHDR...`...`.....H.......IDATx...m.0....4.68L3.')^..h.GK.M........-]..|.3%K....-c~..'c....5....!c.....?9...%5.........>S.i......k.CV...-..a/..y....C........*...r.z..B.4.x..BwH/tyz!....\..2 ..8.....'..........IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\o-0bIpQoyXQa2RxT7-5B6Ryxs2E_6n1iPErd5a7dvQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 10864, version 1.1
Category:	downloaded
Size (bytes):	10864
Entropy (8bit):	7.943184055836693
Encrypted:	false
SSDEEP:	192:JcH2ZaN76gOwuB/1+abBOA9HtrcUXkEg8jRu5pivx3TY7+42PBdZthaB8RlmB:mHWm6gTGN+abB9HZPXLjRyUvxjY7+F/C
MD5:	6F193384ACF462D1738C285CA6CA9A57
SHA1:	B8C76247E6A2CCC4B683255035749E39F062AD6A
SHA-256:	F259DD55C6495C34BCC033C09AA61154AE9E2F8BAE6C86B720D21B8ABD630AA6
SHA-512:	B1059014654C5959BCB8DD6CF29A5408959B2C0445B9F2CD1395F741B6A79818E920A8A139ACFA3BDBF971796CE4BF834095A0D338AF517AC207743169B9BBF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/catamaran/v8/o-0bIpQoyXQa2RxT7-5B6Ryxs2E_6n1iPErd5a7dvQ.woff
Preview:	wOFF......*p......E.........................GDEF...l...4...F....GPOS....... ... DvLuGSUB....... ... .OS/2.......O...`e...STAT...0...&...*y.j.cmap...X...^.....+.Agasp................glyf......!u..94 7.R(head..%8...6...6.#..hhea..%p.......$....hmtx..%............loca..'d........2.#tmaxp..)........ ....name..)4.......x<.].post..*T....... ...2prep..*h........h...x......@...y......f]c..F..&.\c..Zc.q .8]....'~].!..............DFLT...........................taml..tml2..........x.c`arg.......................@...:H......f8...$.............d...S..@J....&g.Q.x.c`.B. f`...2.L...% &....bde.....-.....x..........m.w.5f{... m.mM.m.C.|;...;.@(.E.......5....*.....l....ObB.4.=..0.q.%....".."A..N00.\ 22Sd..$.@9...N.#.q.u.\|.ch..9...l`...CH...$.41G!f.1..)A......o~..|.....<...z<..l..cO...U..].]_..kB.......t.F[l..)..... ...w.Z.l..v..U..{..@.U.Zd.%.z..[...yn..........K...k.[...:...i..^z.~.h.....d.&Z.b.a..a.6Z.l....n...i.(....\................x..;.t[G.3#.eK.,xbz..l.-..2H.,..$.:.c..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\o-0bIpQoyXQa2RxT7-5B6Ryxs2E_6n1iPKba5a7dvQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 11144, version 1.1
Category:	downloaded
Size (bytes):	11144
Entropy (8bit):	7.935980679489796
Encrypted:	false
SSDEEP:	192:ofyiX2/SfrNgKBlRTUemLC/XSuFniOlrBeYOga6TCevG:8yiX7jmKbmm/XJdlfOV
MD5:	ADB84AD27051A8609A6F06024749DFAE
SHA1:	B8032F09901CCBE6C330254E6E81DA53C4A846EA
SHA-256:	4792B076D086A708C1D229F46E17A9C1514DD331EC47333A5AE74B8D9C3F064C
SHA-512:	63D17E38A5EB71200C7F149BDE9821D1F0FCD8157494AA93F351A04CF285E9A21EFA5B541397FC95C9563AC6B8CAB8A8ACE6520445D24FB40693888DC9493AF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/catamaran/v8/o-0bIpQoyXQa2RxT7-5B6Ryxs2E_6n1iPKba5a7dvQ.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\o-0bIpQoyXQa2RxT7-5B6Ryxs2E_6n1iPKba5a7dvQ[1].woff	
Preview:	wOFF.....+.....E.....GDEF...l...4...F....GPOS..... ... DvLuGSUB..... ... .OS/2.....M...`fb..STAT...0...&...*y.j.cmap...X...^.....+.Agasp.....glyf....."...9.5..%head..&H...6...6.#..hhea..&.....$....hmtx..&.....m..loca..(|.....0.![maxp..*,..... ....name..*H..."....>\|_Wpost..+l..... ...2prep..+.....h...x.....@...y.....f]c..F..&.\c..Zc.q.8]....'~].!.....DFLT.....taml..tml2.....x.c`arg.``e``.....1...Q...400...a...`....J.,>..00..0.(00L..1>eZ....X..@.....x.c`.B. f`...2.L...% &....bdc.``.,..^..x.....m.w.5f{...m.mM.m.C.\|;...;.@(.E.....5....*.....l....ObB.4.=..0.q.%...."."A..N00.\ 22Sd..$.@9...N.#.q.u.|.ch..9...I`...CH...$.41G!f.1..)A.....o~..\|.....<...z<..l..cO...U..].]._..kB.....t.F[l..).....w.Z.l..v..U..{..@.U.Zd.%.z..[...yn.....K...k.[...:...i..^z.~.h.....d.&Z.b.a..a.6Z.I....n...i.(....\.....x..{.x.G...(..-i..V.X+i.Ek..$.1..N.I..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\owl.carousel[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):	1178
Entropy (8bit):	4.7718958348113585
Encrypted:	false
SSDEEP:	12:e7ALAfYp9PYyKH47/KdtS7n7fywR+y8lycy5JypxcsRK6gM2XdHY8pZO2YMG7nHk:eMDpZp4tS73DuwxgNHhZO9MGDH+IYDLH
MD5:	3EB95D045E10173C5F0512F703E83B9B
SHA1:	5C1D3349B7DD36E7C4CE41038068949ADAE323E0
SHA-256:	EEE2832920DE823A77ADE71DDF71F135EF58D3D7AA14C2E48036E1FAEC3C2762
SHA-512:	980F58164289BDFA4BC393F482597A4B10AA73F48EFC0F8E929BDF20E1BF0615C376AB2C7A1C78943B8B62E04519588C46D9175A1530B18B76E5E36068A1DBDA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/css/owl.carousel.css
Preview:	.owl-carousel .owl-wrapper:after{content:".";display:block;clear:both;visibility:hidden;line-height:0;height:0}.owl-carousel{display:none;position:relative;width:100%;-ms-touch-action:pan-y}.owl-carousel .owl-wrapper{display:none;position:relative;-webkit-transform:translate3d(0px,0px,0px)}.owl-carousel .owl-wrapper-outer{overflow:hidden;position:relative;width:100%}.owl-carousel .owl-wrapper-outer.autoHeight{-webkit-transition:height 500ms ease-in-out;-moz-transition:height 500ms ease-in-out;-ms-transition:height 500ms ease-in-out;-o-transition:height 500ms ease-in-out;transition:height 500ms ease-in-out}.owl-carousel .owl-item{float:left}.owl-controls .owl-page,.owl-controls .owl-buttons div{cursor:pointer}.owl-controls{-webkit-user-select:none;-khtml-user-select:none;-moz-user-select:none;-ms-user-select:none;user-select:none;-webkit-tap-highlight-color:transparent}.grabbing{cursor:url(grabbing.png) 8 8,move}.owl-carousel .owl-wrapper,.owl-carousel .owl-item{-webkit-backface-visibil

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\owl.carousel[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	29950
Entropy (8bit):	5.0955505612852185
Encrypted:	false
SSDEEP:	384:jLKyIzA0FLkQ3QH+R0Ktd1T169Hzo3A0DErDyLK:X1InLt3Nv49HU/DErj
MD5:	6694ABB95CBB744D54697BDC483F113E
SHA1:	AEC44AF3255E9036931D6A773735729C42E459AE
SHA-256:	DC3AB5D8B09A57E4092E05B3E367D71CE7A91E742A20C06EE65890DC0A821D52
SHA-512:	AFDBB72C9A58FD55912CD2A38AE7310397F40C129410F3A137384EE92CB4C3578A42A5E60184AA1E25526AD7044E1BCC5BA896970D7C27744BC1D860FD9A3FE4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/js/owl.carousel.js
Preview:	if(typeof Object.create!=="function"){Object.create=function(obj){function F(){}.F.prototype=obj;return new F();};}.(function($,window,document){var Carousel={init:function(options,el){var base=this;base.$elem=$(el);base.options=$.extend({},$.fn.owlCarousel.options,base.$elem.data(),options);base.userOptions=options;base.loadContent();},loadContent:function(){var base=this,url;function getData(data){var i,content="";if(typeof base.options.jsonSuccess==="function"){base.options.jsonSuccess.apply(this,[data]);}else{for(i in data.owl){if(data.owl.hasOwnProperty(i)){content+=data.owl[i].item;}}.base.$elem.html(content);}.base.logIn();}.if(typeof base.options.beforeInit==="function"){base.options.beforeInit.apply(this,[base.$elem]);}.if(typeof base.options.jsonPath==="string"){url=base.options.jsonPath;$.getJSON(url,getData);}else{base.logIn();}},logIn:function(){var base=this;base.$elem.data("owl-originalStyles",base.$elem.attr("style"));base.$elem.data("owl-originalClasses",base.$elem.att

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pixel[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1 x 1, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	510
Entropy (8bit):	5.335916817166796
Encrypted:	false
SSDEEP:	12:6v/7CQ2s/6TdKXIMKev/7CQ2s/6TdKXIMKev/7CQ2s/6TdKXIMKr:M2s/65KXILo2s/65KXILo2s/65KXILr
MD5:	D206110E720D6FC4F73739B710EBB247
SHA1:	89E0FC545787CCEAAFD76765DACF84FADEBC8C07
SHA-256:	1D1DF638F63ED0471D8AB33B8808EB9494EA41E27BA35859C1156950F017D33D
SHA-512:	5B923A51AECB5EDFFF8CAA56259833E45B3A533167D3FC317BE0DB458D2E29EF7913E63103D4142B236EA9BC4893745E6D2D5509EB727B9AF7EC52736E1EE619
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pixel[1].png	
Preview:	.PNG.....IHDR.....bKGD.....pHYs.....tIME.....-Q.7n....tEXtComment.Created with The GIMP.d%n....IDAT..c.iy.....+.....IEND.B`...PNG.....IHDR.....bKGD.....pHYs.....tIME.....-Q.7n....tEXtComment.Created with The GIMP.d%n....IDAT..c.iy.....+.....IEND.B`...PNG.....IHDR.....bKGD.....pHYs.....tIME.....-Q.7n....tEXtComment.Created with The GIMP.d%n....IDAT..c.iy.....+.....IEND.B`..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pixel[2].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1 x 1, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	170
Entropy (8bit):	5.335916817166796
Encrypted:	false
SSDEEP:	3:yionv//thPlE+tnM5OCAadCmy42/uDlhlbGlo+4/iRXTECLrlxyxtyaC/tIlsg1B:6v/lhPfZMQC19s/6TdKXTECL6yR/iVB
MD5:	E7673C60AF825466F83D46DA72CA1635
SHA1:	FC0FCBEE0835709BA2D28798A612BFD687903FB5
SHA-256:	0B8A20373C6DD04E091902226D922B3688143A8938AFB9D283D889DE7B55CEB5
SHA-512:	F1C33E72643CE366FD578E3B5D393799E8C9EA27B180987826AF43B4FC00B65A4EAAE5E6426A23448956FEE99E3108C6A86F32FB4896C156E24AF0571A11C498
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....bKGD.....pHYs.....tIME.....-Q.7n....tEXtComment.Created with The GIMP.d%n....IDAT..c.iy.....+.....IEND.B`..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\revolution.extension.layeranimation.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	50765
Entropy (8bit):	5.406783791470186
Encrypted:	false
SSDEEP:	768:TMWnklSBI13hxS4rU3i08gqM+hvAfN64hT5jLqROq:TMy6HlGxhsN
MD5:	7FE78C8164CA4153681F7B00D4D4D89C
SHA1:	0675260BF9246E32D45739C30597B63F2B21611E
SHA-256:	F76B9458B63B2DFF156DBC21C539453EDE466C39A642D4987C4D2B485535F506
SHA-512:	9F9C7282C309E54085EC4A6F91B9A9DBCC752ED9A1924EECFB180C292A2F4CBCA67B01BB4F91F36885C2D1002A6DE48E97AD5646B76AF89CD4A95EACF55029 4F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/extensions/revolution.extension.layeranimation.min.js
Preview:	/**********. * REVOLUTION 5.0 EXTENSION - LAYER ANIMATION. * @version: 1.1.5 (23.10.2015). * @requires jquery.themepunch.revolution.js. * @author ThemePunch.**********/..(function($) {..var _R = jQuery.fn.revolution,..._ISM = _R.is_mobile();..////////////////////////////////////// ////.// .EXTENDED FUNCTIONS AVAILABLE GLOBAL //.////////////////////////////////////.jQuery.extend(true,_R, {...// MAKE SURE THE ANIMATION ENDS WITH A CLEANING ON MOZ TRANSFORMS. .animcompleted : function(_nc,opt) {.....var t = _nc.data('videotype'),....ap = _nc.data('autoplay'),....an = _nc.data('autoplayonly firsttime');.....if (t!=undefined && t!="none")... if (ap==true || ap=="true" || ap=="on" || ap=="1sttime" || an) {......_R.playVideo(_nc,opt);.....if (an || ap=="1sttime") {....._nc.data('autoplayonlyfirsttime',false);....._nc.data('autoplay',"off");....}... }.else ... if (ap=="no1sttime") ...._nc.data('autoplay','on'

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\revolution.extension.navigation.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	22955
Entropy (8bit):	5.2395230939537685
Encrypted:	false
SSDEEP:	384:udu1VJRyVIzV2Ni4kUAtJsxwfB+icxIwpX2wgexB:ukDyVIzV2N8pvuxB
MD5:	986BCB52131428E8C489AE74ED6B3ACD
SHA1:	5B42148ACE79D164CC34F55DEBB3C9C47786B223
SHA-256:	1EC562DA78E7F254770ECE85B4433D02F035247F4C64EB51409696A56BFAD4F6
SHA-512:	A88267773C35334833F591468072F3B16B71B9400CCE4F934E96A8F2151A6535AAE63F735F2B0D2B26F57182F41E519EE1400CCFDA859DB0379B1276C42213F9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/extensions/revolution.extension.navigation.min.js
Preview:	/**********. * REVOLUTION 5.0 EXTENSION - NAVIGATION. * @version: 1.0.3 (25.09.2015). * @requires jquery.themepunch.revolution.js. * @author ThemePunch.**********/.!function(){var t=jQuery.fn.revolution,e=t.is_mobile();jQuery.extend(!0,t,{hideUnHideNav:function(t){var e=t.c.width(),i=t.navigation.arrows,a=t.navigation.bullets,n=t.navigation.thumbnails,r=t.navigation.tabs;h(i)&&y(t.c.find(".tparrows"),i.hide_under,e,i.hide_over),h(a)&&y(t.c.find(".tp-bullets"),a.hide_under,e,a.hide_over),h(n)&&y(t.c.parent().find(".tp-thumbs"),n.hide_under,e,n.hide_over),h(r)&&y(t.c.parent().find(".tp-tabs"),r.hide_under,e,r.hide_over),x(t)},resizeThumbsTabs:function(t){if(t.navigation&&t.navigation.tabs.enable||t.navigation&&t.navigation.thumbnails.enable){var e=(jQuery(window).width()-480)/500,i=new punchgs.TimelineLite,n=t.navigation.tabs,r=t.navigation.thumbnails;i.pause(),e=e>1?1:0>e?0:e,h(n)&&n.width>n.min_width&&a(e,i,t.c,n,t.sl

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\revolution.extension.parallax.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7952
Entropy (8bit):	5.293547913779524
Encrypted:	false
SSDEEP:	192:/C0Un9q1+1t1XYOGvIRp6yZUOZhpdyZUOkeLVpoZg/R:T1+1t1XYlv6pJbhpYGexpoq
MD5:	FBE22B59382A867C7724D896A5D8970B
SHA1:	098668D6CF4583F8F94B25BC9A14E266DCF77345
SHA-256:	756BC914C7F24DB5A3F8E3DA4CEF7C2035C92BBD2D1683D993906F66C9973A84
SHA-512:	3D03B5373882F7B97F151CB95DBAADF5DCB3B2B3407494263D94078B170FB454FC2D78A34D1F67717A6DFDB6F61EF84CC737398CC3BDC205C89E749FCE9AAC A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/extensions/revolution.extension.parallax.min.js
Preview:	/**********. * REVOLUTION 5.0 EXTENSION - PARALLAX. * @version: 1.0.5 (20.10.2015). * @requires jquery.themepunch.revolution.js. * @author ThemePunch.**********/.!function(){var e=jQuery.fn.revolution,r=e.is_mobile();jQuery.extend(!0,e,{checkForParallax:function(a,t){var o=t.parallax;return r&&"on"==o.disable_onmobile?!1:(("3D"==o.type||"3d"==o.type)&&(punchgs.TweenLite.set(t.c,{overflow:o.ddd_overflow}),punchgs.TweenLite.set(t.ul,{overflow:o.ddd_overflow}),"carousel"!=t.sliderType&&"on"==o.ddd_shadow&&(t.c.prepend(' '),punchgs.TweenLite.set(t.c.find(".dddwrappershadow"),{force3D:"auto",transformPerspective:1600,transformOrigin:"50% 50%",width:"100%",height:"100%",position:"absolute",top:0,left:0,zIndex:0})),t.li.each(function(){var e=jQuery(this);if("3D"==o.type||"3d"==o.type){e.find(".slotholder").wrapAll('<div class="dddwrapper" style="width:100%;height:100%;position:absolute;top

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\revolution.extension.slideanims.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	28147
Entropy (8bit):	5.409789576839525
Encrypted:	false
SSDEEP:	384:iF1EXOo+fkNgPwEN8v205g4f8QWwwBWCp1SjXUAgQN8yDFpkkmm:OrPwEN8ej49RjTkBm
MD5:	64D7B2C4F4E5A1E8787FB4DFB67A2085
SHA1:	E945B7335AA99F512069057D5C76835368510F96
SHA-256:	5AFCFB387C3B0E7B0D61511B722F0F5F64E7474C8D24F18E128819694395A929
SHA-512:	73437419D57D65BF38485A9B5F254BFBD6D0FAE5D27FF628F581593F249F7249C096AF445FA28418735BDE5406CF9A5491AAA015304AFA357A1B81AF2F0BD396
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/extensions/revolution.extension.slideanims.min.js
Preview:	/**********. * REVOLUTION 5.0 EXTENSION - SLIDE ANIMATIONS. * @version: 1.0.5 (20.10.2015). * @requires jquery.themepunch.revolution.js. * @author ThemePunch.**********/.!function(){var t=jQuery.fn.revolution;jQuery.extend(!0,t,{animateSlide:function(t,e,o,a,n,r,s,l,d){return i(t,e,o,a,n,r,s,l,d)}});var e=function(e,o,a,i){var n=e,r=n.find(".defaultimg"),s=n.data("zoomstart"),l=n.data("rotationstart");void 0!=r.data("currotate")&&(l=r.data("currotate")),void 0!=r.data("curscale")&&"box"==i?s=100*r.data("curscale"):void 0!=r.data("curscale")&&(s=r.data("curscale")),t.slotSize(r,o);var d=r.attr("src"),h=r.css("backgroundColor"),f=o.width,c=o.height,p=r.data("fxof"),u=0;"on"==o.autoHeight&&(c=o.c.height()),void 0==p&&(p=0);var g=0,w=r.data("bgfit"),v=r.data("bgrepeat"),m=r.data("bgposition");switch(void 0==w&&(w="cover"),void 0==v&&(v="no-repeat"),void 0==m&&(m="center center"),i){case"box":var x=0,y=0,T=0;if(x=o.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\rx_lidar[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	118920
Entropy (8bit):	5.331463997856821
Encrypted:	false
SSDEEP:	1536:EMadkwQKHeH2hZJBQADzlHCukXIdOyBIx0nTKYGSaC/BE60ZkA06O5JpneNhpvvS:Opm2h/zxKIcEIVcIIzvdsx+O
MD5:	D52526AE2D4840E82E35DF619D64C386
SHA1:	B747B12F8AF4DA1F61E16415CE036B0DC7075E4C
SHA-256:	8D0699772B8CA80D6EF1AC55871141AFD77CDA372F15F1A97B74B41DAE70AB25
SHA-512:	0B96C503842D8D7D36D884208781717D33B2FC3B784066EDCE1CF9697ABB4FEAAD976E19B5FA58397E3EF86B55E3897F952976A96A6553B86D4B932C27130F60
Malicious:	false
Reputation:	low
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n,ba=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},da="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},ea=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("a");},p=ea(this),.r=function(a,b){if(b)a:{var c=p;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&da(c,a,{configurable:!0,writable:!0,value:b})}};.r("Symbol",function(a){if(a)return a;var b=function(f,h){this.vd=f;da(this,"description",{configurable:!0,writable:!0,value:h})};b.prototype.toString=function(){return this.vd};var c="

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\rx_lidar[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	118920
Entropy (8bit):	5.331463997856821
Encrypted:	false
SSDEEP:	1536:EMadkwQKHeH2hZJBQADzlHCukXIdOyBIx0nTKYGSaC/BE60ZkA06O5JpneNhpvvS:Opm2h/zxKIcEIVcIlzvdsx+O
MD5:	D52526AE2D4840E82E35DF619D64C386
SHA1:	B747B12F8AF4DA1F61E16415CE036B0DC7075E4C
SHA-256:	8D0699772B8CA80D6EF1AC55871141AFD77CDA372F15F1A97B74B41DAE70AB25
SHA-512:	0B96C503842D8D7D36D884208781717D33B2FC3B784066EDCE1CF9697ABB4FEAAD976E19B5FA58397E3EF86B55E3897F952976A96A6553B86D4B932C27130F60
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagservices.com/activeview/js/current/rx_lidar.js?cache=r20110914
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n,ba=function(a){var b=0;return function(){return b<a.length?{done:!1, value:a[b++]}:{done:!0}}},da="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.v alue;return a},ea=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&& global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("a");},p=ea(this),.r=function(a,b){if(b)a:{var c=p;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&da(c,a,{configurable:!0,writable:!0,value:b})}};.r("Symbol",function(a){if(a)return a;var b=function(f,h){this.vd=f;da(this,"description",{configurable:!0,writable:!0,value:h})};b.prototype.toString=function(){return this.vd};var c="

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sd[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	2.9889835948335506
Encrypted:	false
SSDEEP:	3:CUkxl7/lHh/:slf/
MD5:	B4491705564909DA7F9EAF749DBBFBB1
SHA1:	279315D507855C6A4351E1E2C2F39DD9CD2FCCD8
SHA-256:	4E0705327480AD2323CB03D9C450FFCAE4A98BF3A5382FA0C7882145ED620E49
SHA-512:	B8D82D64EC656C63570B82215564929ADAD167E61643FD72283B94F3E448EF8AB0AD42202F3537A0DA89960BBDC69498608FC6EC89502C6C338B6226C8BF5E14
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\settings_grey600_24dp[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 48 x 48, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	604
Entropy (8bit):	7.573620174038291
Encrypted:	false
SSDEEP:	12:6v/7dkfFQPHl09Kor6EHz1g+WVmObBbBbaLPIpTIiVojx5cF8NonhstcAzhu1:CkEl0nr6EHz1VWV33ePIpTzVojx5p6nH
MD5:	7BD42E5A35B5FB3FF852D6EA9191CA83
SHA1:	8A141EB392A05A2DEA3DCD83B97940EF70A81EBC
SHA-256:	5C4A713EE4250851232BE9F9F68D41586BE39B299528CFC7266E0B0E7E582E1B
SHA-512:	6FF31ACB937D6944570A837BB77AED92DAE41D71681440DC4765758FC40585F55999F2CDD78C4CE76A5AB414331BA9959BAFCFEF7E85B756AAB899C247F0289
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/images/icons/material/system/2x/settings_grey600_24dp.png
Preview:	.PNG.....IHDR...0...0.....1....#IDATx...MKTQ...3...K...gP.Eo.Z$..6....."0..."..E-Z...C....+..E.T...JH/.HC.$d...y..."..W...w.3..3..9... ^..Fr4R.Q.....H<...\...V.[...v.L.D...y.wYQ....].. ..w&...|F...iz8..b.s.r..[.H..5..5D..[@.ed.-...O..=..G..lpD.R.F".J..... .. y*..$>.)V.`..quuP4.W9.}....*..y.....~E}.7....IU.~.!.Ak.>....A..o..._.....7.4...{.K..6o.O..5.0n.`..z...V."^. 0.x=. .^M...*t...H..9.B.(UD..>heD....."....W..T.E..0D.fYfI..3.-.G".....#.p....q.....Bv..{5.!u.F.i.....[.s.)....I....v.....Y.P.5?...n.'.....:...T.....f.....Q...~...8.....h.....T3<.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\simple-line-icons[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):	12416
Entropy (8bit):	4.829541145478792
Encrypted:	false
SSDEEP:	96:7AidDuwqMguW0umJY9ZbgJ1lgraDBi9vUc1ZQFj2kwgu6QdC2L:sOXYuZuVZoElqF9VsDL

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\simple-line-icons[1].css	
MD5:	9FABF4481822D95CC7F2F8534A5D6681
SHA1:	0F8729AF4D8B21AC6B29BD95D1DBCF22A3410016
SHA-256:	3B26B2B2C5CA741489556C07FD4B5F0C84608C2A48FEB28F9452034FBED4DFE0
SHA-512:	3C69D0757FE547B0B71143B6576282FC4E26D74A283717F23754736E4E344587E5B202014CC1031CE9682DEE2FECA663EBE7F3435452E203260084468D056CAD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/css/simple-line-icons.css
Preview:	@font-face{font-family:simple-line-icons;src:url(../fonts/Simple-Line-Icons.eot);src:url(../fonts/Simple-Line-Icons.eot?#iefix) format('embedded-opentype'),url(../fonts/Simple-Line-Icons.woff) format('woff'),url(../fonts/Simple-Line-Icons.ttf) format('truetype'),url(../fonts/Simple-Line-Icons.svg#Simple-Line-Icons) format('svg');font-weight:400;font-style:normal}[data-icon]:before{font-family:simple-line-icons;content:attr(data-icon);speak:none;font-weight:400;font-variant:normal;text-transform:none;line-height:1;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.icon-user-female,.icon-user-follow,.icon-user-following,.icon-user-unfollow,.icon-trophy,.icon-screen-smartphone,.icon-screen-desktop,.icon-plane,.icon-notebook,.icon-moustache,.icon-mouse,.icon-magnet,.icon-energy,.icon-emoticon-smile,.icon-disc,.icon-cursor-move,.icon-crop,.icon-credit-card,.icon-chemistry,.icon-user,.icon-speedometer,.icon-social-youtube,.icon-social-twitter,.icon-social-tumblr,.icon-soci

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\site[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3457
Entropy (8bit):	5.272381202190546
Encrypted:	false
SSDEEP:	48:moaoWoO3Ql1AXvQCADW1dgcZs7LvW44oBLdyWce3Sh73h+DZw923h+2PYrZw1Oa2:mjoOmAXvj+W1dgcCcoDFw9mSwY
MD5:	4F9930BFA115FE93FE5897ED298AAC9E
SHA1:	C7D6F43D92693BF7EB78F3230EA1E56EC2CD1745
SHA-256:	6E95982CABF33B096255F062D2A3F2A357F33E5DEE957760014D286C2D430A06
SHA-512:	59DB2802AE8445D20C09DF2A5DE757A6ECE842E6FBC96F4A34B842CF0653941D82EFE2A4C47D60040194F48B6C07DFBB030A8708EE8717806F2DA00DCCC6A8E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/js/site.js
Preview:	$(function(){"use strict";var stickOnScroll;var header_top=$('.header-three-margin').height()-96;$('#header').addClass('normal');$(window).scroll(function(){if($('#header').length){var scroll_t=$(window).scrollTop();if(header_top<scroll_t){$('#header').addClass('bg_color');}else{$('#header').removeClass('bg_color');}}.if(scroll_t==0){$('#header').removeClass('bg_color');}}).if($('#owl-slider').length){$("#owl-slider").owlCarousel({autoPlay:3000,items:3,itemsDesktop:[1199,3],itemsDesktopSmall:[979,2],itemsMobile:[600,1]});}.if($('#owl-slider-clients').length){$("#owl-slider-clients").owlCarousel({autoPlay:3000,items:6,itemsDesktop:[1199,6],itemsDesktopSmall:[979,6],itemsTablet:[768,3]});}.if($('#owl-slider1').length){$("#owl-slider1").owlCarousel({autoPlay:3000,items:3,itemsDesktop:[1199,3],itemsDesktopSmall:[979,3]});}.if($('#owl-slider2').length){$("#owl-slider2").owlCarousel({autoPlay:3000,items:6,itemsDesktop:[1199,6],itemsDesktopSmall:[979,6],itemsTablet:[768,3]});}.$('.nav ,.blog-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sprite[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 400 x 400, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2065
Entropy (8bit):	5.169795031947611
Encrypted:	false
SSDEEP:	48:qwqNn2SpVd6pJ3JJ3Ewttttttntttttltttttt W:62qVd65J3EV
MD5:	DF0B4A54DE826192EA607E45B9619BDA
SHA1:	EE3A240D1EB8E0B4D4B3B6AFC1E5E4BC600E6FFD
SHA-256:	59EED6D1CDC8942A7318F82CF83A577EB30DDB9EAEA1302617515231A592E367
SHA-512:	95516A9149D3FF2FF2E76590D54BFD60448ADA8B7563D968B270E84B0C161D56D96BC97B5C348FB7473EFA750485B6B3905CD9DEBCAD6CEB9B4D29DEFA899FC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/images/sprite.png
Preview:	.PNG.....IHDR.....6.....tEXtSoftware.Adobe ImageReadyq.e<..."iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c061 64.140949, 2010/12/07-10:57:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CS5.1 Windows" xmpMM:InstanceID="xmp.iid:8E4BD8B3822E11E5A688E7E2F1064E27" xmpMM:DocumentID="xmp.did:8E4BD8B4822E11E5A688E7E2F1064E27"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:8E4BD8B1822E11E5A688E7E2F1064E27" stRef:documentID="xmp.did:8E4BD8B2822E11E5A688E7E2F1064E27"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...C....IDATx...1.....0._...M".O.v..*.....` .....` .....` .....` .....` .....` .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sw[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):	732
Entropy (8bit):	5.105609416920151

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sw[1].css	
Encrypted:	false
SSDEEP:	12:+jcw/4RB/w2VqHKsMlkSRyvuED7ksSMFESKvGVjXuE1R/LcvuYj:oyeHKsMlNqug7/F9KCuEHwuYj
MD5:	6889EA45B54EA91720390AAAA3E53BFB
SHA1:	E45F445859AC7104BB6F94A3A45BF713DDC0877D
SHA-256:	EA4276F173A5D07A5120F0CED60CF7923E3D6AC53131A47BEA6A25328535B774
SHA-512:	19BB23878DC6FC3BB63D9D7996127ACBC091A68960D5BCFCDF4F0BF3778A77B906432127CBBCC0A21081992484F490AF689536D6F73B8F7CE821BED343BB794
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/sw/sw.css
Preview:	.pw_cont_button_01,.pw_cont_button_01 *{box-sizing:border-box;padding:0;margin:0}.pw_cont_button_01{font-family:sans-serif;background:#fff;position:fixed;bottom:-500px;left:0;width:100%;padding:10px 20px;font-size:16px;box-shadow:0 -2px 7px rgba(0,0,0,.7);z-index:999999999999999;animation:pw_cont_button_animation_01 .3s ease-in 1s 1 forwards}.pw_close_01{float:right;font-weight:700;padding:4px}.pw_close_01::before{content:'x'}.pw_add_button_01{background:#146657;margin:15px 0 0;padding:10px;color:#fff;font-size:1.3em;text-transform:capitalize;cursor:pointer;box-shadow:0 2px 7px rgba(0,0,0,.7);text-align:center}.pw_add_button_01:hover{background:#13483e}@keyframes pw_cont_button_animation_01{from{bottom:-500px}to{bottom:0}}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sync[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	129
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CUnl/7yltxlHhqwnl/7yltxlHhqwnl/7yltxlHh/:/+qA+qA+/
MD5:	5B01021BF6BC7111789FC32243207567
SHA1:	A08FD8F9F5328FF2795C5258548F285BB3F974F6
SHA-256:	F55F80F9A4335CFC32FD48D8CDDDBBF25F7D1D5DA26AFDE07CCB00DC0535227B
SHA-512:	8B5647C214464EC972ED3171BCE870824B10D1F47EB1F260FDB530C2D9D882098AF150DFF35174B9122BADE092B7E588EA80B74FF3D1571C6A2490021E54B120
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;GIF89a.....!.....,.....D..;GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\trk[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	2.9889835948335506
Encrypted:	false
SSDEEP:	3:CUkxl7/lHh/:slf/
MD5:	B4491705564909DA7F9EAF749DBBFBB1
SHA1:	279315D507855C6A4351E1E2C2F39DD9CD2FCCD8
SHA-256:	4E0705327480AD2323CB03D9C450FFCAE4A98BF3A5382FA0C7882145ED620E49
SHA-512:	B8D82D64EC656C63570B82215564929ADAD167E61643FD72283B94F3E448EF8AB0AD42202F3537A0DA89960BBDC69498608FC6EC89502C6C338B6226C8BF5E14
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\1436723653-kos--1024x512@abc[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 34x34, segment length 16, baseline, precision 8, 1024x512, frames 3
Category:	downloaded
Size (bytes):	102718
Entropy (8bit):	7.978169539557044
Encrypted:	false
SSDEEP:	1536:GTmKKr5DA0ZAraqolmDlhp6gj5OrTHidpbmbyoshbVHY1GpJ8DUjdMxODLrb:GBKrDE2ls0pB5GTm+NshpFyUqEf
MD5:	D75AD78E511E69EAE31F61F2953E4AEB
SHA1:	3DD10B93ACBE5EEA8FF0DC243FCC8978282136DE
SHA-256:	19FFA44071E7AB1D0359C374026801CC50852BBFC7592E0C75C6130754D46720
SHA-512:	2C9434941329047427712 7FFD266BFF5BA954A035571127812E7C92CECEE6B128469C4B415AE073FEF30F26EE6B4876DEB4F80BEC60EC031EB55EEA697ABB8E5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static2.abc.es/media/espana/2021/05/10/1436723653-kos--1024x512@abc.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\1436723653-kos--1024x512@abc[1].jpg	
Preview:	.....JFIF.....".".....,Photoshop 3.0.8BIM.....".....".....C.....C....."..... .....C.....!.1.."AQ.2a#q.BR...3...$Cb..4Sr..%.D..c.....*.....!.1.A.".2Q.B#aq.....?...J*#.BG..b.JQ.K..Vy.....+.r..U....N.A.....|.|..`... (.0...@W..72p.erHD.r{sF.....j.hZ0v.*..~..j.(.8.g.2..W..f....K..Q...)G...I.@Y..]..{mB.WV....*..z.^.Z=^..k.j.&.ZN.P8.C..z.^..!.R..m....;^.W.....].^^./u. .1^.}..>.VC...\.O.+..L.....q^...D=. {.....m.....Zt@]...A....Wd...t.....a.*9.7H.....u#/..H...M.....j>`....qJ...eu\.E,.W...(.$&2~i.^h.3.{SR.h.....M..h...j.j. .&.....zp.5..2*.pq....t.....`/ b..4e.r(rH.-...).F..O....".h.0c.... {.O4r8.6\aF1T.C...3~k.....O&v...Q.....\.5k.....9...7...xF...O\,.....Y...yK....zP..~s^..W.g.k..j..Y.{.....Lr.\T...-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\1617127710560[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 1600x900, frames 3
Category:	downloaded
Size (bytes):	495325
Entropy (8bit):	7.968338022096609
Encrypted:	false
SSDEEP:	12288:P4gctO6vc9hLVBcwr/u7IML5fydtoI8rTIDUIvEcurYK+:P4F5vc9KecB58aT+5pK+
MD5:	F4533B591C9898660B59C971A75DA0D2
SHA1:	2B91247517B667F53C03E29190264C7E271F9F5F
SHA-256:	79AD750CBA1A0A38A9633AAB2ED4528A057D36D027A314C4EBD319F868410792
SHA-512:	823C0FE092AD7F2B5B17945CF88500DBBD5D1A8CB1574060BD7CC1B705F716E9672B70F913C4EBBD04799656A0F30994E4167E53E3DAAD237311EEE915F0461
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img2.rtve.es/imagenes/asi-avanza-vacunacion-cada-comunidad-autonoma/1617127710560.jpg
Preview:	.....JFIF.....Exif..II*.....$ICC_PROFILE.....appl....mntrRGB XYZ .....acspAPPL....APPL.....-appl..A....P.bEt.V.....desc.. .....ecprt...d...#wtpt.....rXYZ.....gXYZ.....bXYZ.....rTRC.....chad.....,bTRC.....gTRC.....desc.....HP ENVY 24..... .....text....Copyright Apple Inc., 2021..XYZ .....XYZ .....d...2....$XYZ .....j....3....XYZ .....(.....para.....sf32.....W...).....~http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c002 79.164352, 2020/01/30-15:50:38 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmln

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\16206244273434[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1200x683, frames 3
Category:	downloaded
Size (bytes):	133939
Entropy (8bit):	7.981377669495542
Encrypted:	false
SSDEEP:	3072:0QRjSl/wjPsBp7V8FxnT2VZ1HERcR38TeAuXu/kxReYjoi:bRjSlRHV8Fx6Zh8CH+oRdUi
MD5:	80C1FB2A5DABEE6DCB94CBE105C2F9A9
SHA1:	ADB1C66F8E8193E01B9F40DCBBF847A1455DEA3E
SHA-256:	222F1187A5E4765D316822A8D507B339D5F1774BD4E14196E41069A5E53A1E7E
SHA-512:	4063C23F4412AF1E436F39EC992DAF68BACCCBC6A9D0A637E9973DBF936DA16BDE9F0385F0D89DFB445997CCD19B72B0BD68F2D0E6C03F63F3E6471A15476F0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://phantom-elmundo.unidadeditorial.es/de450e428f4bd13b9bd4d4d7d5445edc/resize/1200/f/jpg/assets/multimedia/imagenes/2021/05/10/16206244273434.jpg
Preview:	.....JFIF.....`.`.....C.....%...#... , #&')*)..-0-(0%()(...C.....(...(((.....[.....!.1..AQ..aq"...2....#B..3Rb...$4r....%5CSst.67c.....&DTdu.'V.....F.....!1.AQ.."2aq...3R.....#BS.....4CDb..5Tr.$s.....?..t..@....T.dc....%...v@.. .*.....y.....p...K.\2is."!z..u".....:-.<...Ca. .Q;wt....r.V..s...N\.V..e.....H....B.i....V..Z..%&..ek..Xr.5.o)..A..h..wa.b.%.l|.a..S}...ZZ.L..v..H...Sl.$..YS..w.....B.x.....R..s.y... ..+.n....P .....?.....R....."=..A.....&...v(.}.'.#...8.z.^....#.w..s.KT..V.[7...Wf<s..>K.cY....&W|N..^.....P.M.:zAV..nU#.FO....Ch.b&7...c.J.d.@...+....z..RV.D..PDe..V,.....:...,..z..{..yG ....Oez....T...g...;2Z.....0..Sm1..]F.....27.:.....6D.w....%....m.A .C. m....@..... ."N=PR(.A6.....9...F.a.....]..-.[.&....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\6098cbc1260000e269b4296a[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 1200x630, frames 3
Category:	downloaded
Size (bytes):	143294
Entropy (8bit):	7.959815478538268
Encrypted:	false
SSDEEP:	3072:aVXUtVG6DzK+7HEq6GCCA+CHgibidLB7zJ8m603vKcQjHxu+IP:GXUt9D7gx+smVfKHjY+Y
MD5:	0B001090F5F7C32F2B78326674904E11
SHA1:	1B932B14C11EA7268740237A893ED7EA00B996A0
SHA-256:	90F84293AE4C2251B14DA8291099241517B97F1B51854272376E2A745DE31730
SHA-512:	8E80477586FF3DD7070ADBA057091637D4C8906481F73924D5BB71F1DE6F0669BFAD326AD606D6AEE6A1D13B512477A6A15ED33676D3D63B34F61C1FC0A85D6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img.huffingtonpost.com/asset/6098cbc1260000e269b4296a.jpg?ops=1200_630

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\6098cbc1260000e269b4296a[1].jpg

Preview:	.....C...................................%...#... , #&')*)..-0-(0%()(...C..........(...((......v...."......................................H......................!..1AQ.."aq... 2...#BR...3...$b.r%CS...&45.s..Dc..............................3.....................!.1A."Qa.2q....#B...R....3............?...\|W.3J...R.t.<..#4.O.v..>.^RO ..@ LriI.........)...R.=i ..J.....(..W..4 +.E8.29.."......$.s.M.lt...S.v.NE.#. ....4.@.G|......;......8BU....3..S..8.E..S'..FS......s...$I.:.m..`0L.........*N>i\|...O..."e....h..c.q'`.'.......x...w.D..<.\_..J}.2.U.GAm..5!....m..Ii.....C.E..^ .@3...A%]i+....[!4...h.s....BO=.I.$.@.;.F.:..^...+.....DKL..M.3.:Q.!I!b..0G.M.Q.ds^...m0I.+....U@'S.);.P=.{.. .).d.1.|S...G.:...2.FjW.P...0.T{.*..L..Z........H...$......O.!.(RS'..d .Gj%..>...2O5O.,..q^.............x....s^..Y=c....x..q.x..f.b{.x.I9...A q^..zs....z.BLH..&f)L..+.$u......&A......^9.i.A#...3....W..A.....{..\D.i#.M....S.h.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\HpwNkB4r-iltD3wVs4tNs86Vb9pM92Oc366-IABnofE[1].js

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):	20974
Entropy (8bit):	5.505895657797031
Encrypted:	false
SSDEEP:	384:Sujvjh9iTJMKJu9UQWUuvfUjUmh5+xsGPuKNqgadY:S+vjh9itJIDWUJQuGPuKcvY
MD5:	066DC1E1312E946B968D68974877BFB4
SHA1:	FB2AA656DB99A0C195FD9F09ECD1B12051B9E2F5
SHA-256:	1E9C0D901E2BFA296D0F7C15B38B4DB3CE956FDA4CF7639CDFAEBE200067A1F1
SHA-512:	E7F253B8E53B765A2D9CAF752BBA684D5B812EA5EAC3EC61EDB1FA5ADA065707D087B559A3964BEC93DB4B8A200C1A1E8ACD30374DD036D4BE2F80F85EF800D7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/bg/HpwNkB4r-iltD3wVs4tNs86Vb9pM92Oc366-IABnofE.js
Preview:	(function(){var b=function(L,n){if(L=(n=u.trustedTypes,null),!n||!n.createPolicy)return L;try{L=n.createPolicy("bg",{createHTML:w,createScript:w,createScriptURL:w})}catch(f){u.console&&u.console.error(f.message)}return L},w=function(L){return L},u=this||self;(0,eval)(function(L,n){return(n=b())&&1===L.eval(n.createScript("1"))?function(f){return n.createScript(f)}:function(f){return""+f}}(u)(Array(7824*Math.random()|0).join("\n")+'(function(){var LW=function(L,f){function n(){}L.d0=(L.J=(n.prototype=f.prototype,f.prototype),L.prototype=new n,L.prototype.constructor=L,function(w,B,u){for(var b=Array(arguments.length-2),r=2;r<arguments.length;r++)b[r-2]=arguments[r];return f.prototype[B].apply(w,b)})},I,fW=function(L,f,n,w,B){return{invoke:(B=nW(L,function(u){w&&(f&&l(f),n=u,w(),w=void 0)}),(w=function(){},n=void 0,!!f))[0],function(u,b,r,D,J){if(!b)return b=B(r),u&&u(b),b;(J=function(){n(function(X){l(function(){u(X)}}),r)},n)?J():(D=w,w=function(){D(),l(J)})}}},uy=function(){},nW=funct

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOlCnqEu92Fr1MmSU5fBBc-[1].woff

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20404, version 1.1
Category:	downloaded
Size (bytes):	20404
Entropy (8bit):	7.970248785137973
Encrypted:	false
SSDEEP:	384:8uFoOxqigBacqKz8RGLv6K5a+jZ/rFSyeM5B8r/WjRy0BsM16t/PJ:PFlIvUKz8R+t5N53eGar/gY0Bv6tp
MD5:	BF0F407102FAF3A0B521D3B545F547A5
SHA1:	CA357CD0DE5DD0242E8EFACFB8D24AB60FDC86AB
SHA-256:	855A06974032BB69157D469ABA6F63440E8BE47C421F45C3F396F4E0B87B6DE8
SHA-512:	85359028F7FE49B1DF90B72E48DC7DE4B21F1B65E8BF109595705A3F4EAF9FA79854B5AEF060FE266291C5ECE9D04FCEAD1DE09BAA2C5E20601E15792125200C8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmSU5fBBc-.woff
Preview:	wOFF......O........x........................GDEF.......G...d....GPOS...............!GSUB................OS/2...L...P...`t6..cmap..............#cvt ....X...X/...fpgm.......4......".gasp...@............glyf.. .L..<'..m..]5Yhdmx..Ht...m....),..head..H....6...6.Y.ihhea..I.... ...$....hmtx..I<.........Dd.loca..K............maxp..M.... ... .4.\name..M........\|..9.post..N........ .m.dprep..N........:z /.Wx...1..P......PB..U.=l.@..C)..N4C.\.51.3.......q.q.qu.O...OjC.cA......R.x...l\..F..3...N..q)..a\|.....^..33..c......p"y.iT....<Gg...!.3...T1...{.g0.u.y........m.\|.k..NF......mox.;...7&.Y.. C.R_[.T.c..-.=...9:...a*j.G..............O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..".).[...._.T..T... ..+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.l..F.$.2#.e..].[.....yR...e.|{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOmCnqEu92Fr1Mu4mxM[1].woff

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20332, version 1.1
Category:	downloaded
Size (bytes):	20332
Entropy (8bit):	7.970235088150752
Encrypted:	false
SSDEEP:	384:U0iwaxoOUPVkOJJSu6SsCKTIRDqG9oHKwZh98OSv+MsgkAOY:75mlUmOSu1guh+fZhLSxkAr
MD5:	DC3E086FC0C5ADDC09702E111D2ADB42
SHA1:	B1138B84FF19EAC5F43C4202297529D389BD09B7
SHA-256:	EA50AC7FDDB61A5CE248A7F8B3A31A98FE16285E076B16E6DA6B4E10910724BB
SHA-512:	10123C785C396CF0844751A014413ECF4D058AD0C00CAAEF5F8FFEF504C370F03EACD0B3C2A49211EEE0877B7AE7D0EF6E01264F04FC910C2660584B5E943BE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Preview:	wOFF.....Ol.....x.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...P...`t...cmap.....#cvt .....T...T+...fpgm.....5....w.`.gasp...@.....glyf.. .L.;...m.&.x.hdmx..H....m..../.head..H....6...6.j.zhhea..H.... ...$....hmtx..H.....]uloca..Kp.....m,maxp..Mp... ... .4..name..M.....t.U9.post..N`..... .m.dprep..Nt.....I .f..x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a\|...^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.\|.k..NF.....mox.;...7&.Y. .C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..").).[...._.T..T.. ...+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.I..F.$.2#.e..].[.....yR...e.\{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\LOGO-WEB-MIN[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 2921 x 1224, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	101607
Entropy (8bit):	7.7502956138982535
Encrypted:	false
SSDEEP:	3072:ZabyiM/2HSLy456mkvB/dQL9ILqUDSGtk2iJf5:ZIyb/2yLye6mkZ/dQL9iDO2iJB
MD5:	AAD2A1DB4345246F997940CDF22A7E7D
SHA1:	1A42EE6332E3D000D74A9CD9FE0D6E51DAB57719
SHA-256:	0FE93D2ADCFF1A195547AF7D4A0BB6299105CD06759A668A04D4BD39FBCAA9B1
SHA-512:	A1C5814910F40E49F048B5AD9D642319FE98E112FAD665DD87BD2F7312756269A423558E30DF01F5B2628C377A125DDD5409BC2881A92FC219DC677DDE4C31F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/images/LOGO-WEB-MIN.png
Preview:	.PNG.....IHDR...i.....<.l&....pHYs...#...#.x.?v.. .IDATx...o.U.'..izS...kz..l....*g..3.h.U...i..2..K#..+#..W...8+#5.p.._YUiX...`.7... 3.....IW..%A...TQ.....z.O%e_..?..=...G*..9...s.. =..H....$.....r...8...!.5m....._.+!..y.....l.....^i.;.....T..1p]._...._..~.s.`v.;...a..3a.....m&..P@Y...g.....].....n.....LH.....e..{..{.q.....0'!m...%.L:...*..7+.M9....:+ .}.>>:e}.....KH.`..0.@....06.v!6n...i.{..... ...@Y.....Aal..B..Oy.....(.!m...J;._.....-q=.n..L..>>:e.....IH....!{`V.{..3.....6P9Y...A.o.....Wf....W.....@..i....d..d.XqJ d*.m.4.m_.....'....P._.}V.....SN.....P6<..6.....@..i.]E(..m&..a}].q.....6PxY.....b.R.g.l_1Z.....'o..f.B.6.gZ.....,.6P....c.U.B..l....^.$.....#..tD...<.. #.0.B.Y.(...>.C.....`nB.@.dI...`6..f..m.>>:e.....DH.XQY....WB.....4..>-..... ....<..J..g.P).....@..i.-.%i.c....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\VUUSS9Y4.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	118722
Entropy (8bit):	5.204009412810923
Encrypted:	false
SSDEEP:	1536:fL83LI+7/nygB7DmzS1ZqFxQb0tDawuvXy3Qqa0MH1w0Sz:fY35ygNDmzSsJtDawuvXy3QqaJOz
MD5:	0E44D582F7BA01CCD54FECF0562C96E1
SHA1:	C71EADDEFC44F26F7D02A00294D90E1786A53D92
SHA-256:	5CC860F642DE32A48BCBB36944DC162E3263FA661B7B96500109E1714F66A16B
SHA-512:	0D5CF803E48F0AC2877A385BAD2DE7FAD227EBFC95B358778ED5C24E7ED41DEB04250110797A86F2130514A76274C307CA18B0883469372BD6C7EB18B0F7640
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html lang="es-ES">.<head>.<meta charset="utf-8">.<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no">.<title>. Local Coronavirus Espa.a . .ltima hora .</title>.<meta name="description" content=". Coronavirus Espa.a. . .ltimas Noticias y . alertas locales de Coronavirus Espa.a.">.<meta name="keywords" content="Espa.a Coronavirus, informaci.n Espa.a Coronavirus, alertas Espa.a Coronavirus, estad.sticas Espa.a C oronavirus, .ltima hora de las noticias en Espa.a Coronavirus">.<link rel="shortcut icon" type="image/png" href="/favicon.png">.<link href='https://fonts.googleapis.com/css?family=Catamaran:100,400,200,300,500,600,700,800,900%7CBiryani:100,200,400,300italic,300,400italic,600,600italic,700,700italic,800,800italic' rel='stylesheet' type='text/css'>.<link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.css" media="screen">.<link rel="stylesheet" type="text/css" href="/assets/css/f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4_europapress2721462cremafallamunicipalvalencia17marzocoronavirus_9cab9921[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 1200x675, frames 3
Category:	downloaded
Size (bytes):	106208
Entropy (8bit):	7.9716424141893745
Encrypted:	false
SSDEEP:	1536:xwkVd6fbB5Lzak/lBwsEPCVvPx6i8NkWr7qKBatxjNE2/VYp1Wl+OEkR682F3HJ5:xxVd6PksIXLruOaPpJfDC3HM/U
MD5:	C140AB4AAAA5227C699D38A54AD50868
SHA1:	26FCDB8765E947F67C1B67CE37DE71F48FF4E479
SHA-256:	6DDCD16A58F84C7A21E0A742A9B832D2A4262C099772987251C8B7B3B229EDE0
SHA-512:	A35D1799F58B5E914849D7EA8E4C887B1DAFFF6C81304786C6780F033D50A3DA537734F55E61DB0C35C0DEF4D0D16953B9BAAC65A6A234091B870F1A08BC13F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d3cra5ec8gdi8w.cloudfront.net/uploads/imagenes/social/2021/05/10/_europapress2721462cremafallamunicipalvalencia17marzocoronavirus_9cab9921.jpg?320f952da5bd9895b027428e2460627c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4_europapress2721462cremafallamunicipalvalencia17marzocoronavirus_9cab9921[1].jpg	
Preview:	.....JFIF.....,.....XICC_PROFILE.....HLino....mntrRGB XYZ .....1..acspMSFT....IEC sRGB.....-HP .....cprt...P...3desc.....lwtpt.. .....bkpt.....rXYZ.....gXYZ...,....bXYZ...@....dmnd...T...pdmdd.....vued...L....view.....$lumi.....meas.....$tech...0....rTRC...<....gTRC...<....bTRC...<....text....Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1.....XYZ .....Q.....XYZ .....XYZ .. ....o...8.....XYZ .....b.....XYZ .....$.....desc.....IEC http://www.iec.ch.....IEC http://www.iec.ch.....desc.....IEC 61966-2.1 Default RGB colour space - sRGB.....IEC 61966-2.1 Default RGB colour space - sRGB.....desc.....,Reference Viewing Condition in IEC61966-2.1.....,Reference Viewing Condition in IEC61966-2.1.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\activeview[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	84
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEqjdfXPQE/xlEy:1QEoqh3QEoy
MD5:	6A3F2D147842187CD48B1546EDDD5BA0
SHA1:	AB278C31189DF2939428CF81A3850A2C6DBF5E2E
SHA-256:	D4990F907BCA02F02B3D41216EEA5461609D4BCBA07A3CBEE0D7CF28A6D0D864
SHA-512:	998F55BF5C3D4A71CB3C23782B788F71E7625DF83A37FE8A18F915AAA3BDE5420183A3C709816664E262069EE2FE245CA44799E3476B6DE507B5D68FC86F8960
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\appliedxlabs[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 434 x 94, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	5166
Entropy (8bit):	7.93670411135492
Encrypted:	false
SSDEEP:	96:lmoxOVqvqZEpVxMb+usZAjuN43ezhs45Y1xBrtdiYJ9GF0:UoMVp4ry9sOjuu3Whs4Y7rtAIo6
MD5:	A88F34C9DB3A05836B3333237CED76A0
SHA1:	18719E3278BED9697F31D9ECF4100A5C3EF9B12A
SHA-256:	898411BB4B36A617F31FB304C99BEE6FC8E43CB2E4EAF68DDDB536A092AA13AC
SHA-512:	72C666A00BBECFE69C7F1D3AE48EF4C1F8F8121F76A1262EB4DA9214E5CC22D1E4D6A941AFB4705DB2E40F1B5F265CA73CE99F385CDF91BFAC3EF09171EA1094
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19tracking.narrativa.com/img/appliedxlabs.png
Preview:	.PNG.....IHDR.....^.....Y.....bKGD.....pHYs.....B(.x....tIME.....1x.....IDATx..i`....5....L....(.\.Q.#.l"...A."n\.....!I.6.A...W/....@....v..P.z....[!.!...!.5.I.L.t'....KUu..e.t..:U. 0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0...a>+5..2rV.w.gj."..a.8oR..I8.#.).....jp.(..5Q;....{..m.+.fp.]A$D..O...P.l.o..P.9jka.'..U{.....|...s.....=.....j]9..v.xr.....N..=...W....< ..]..O...P.4(.;F.q....c....5xCl7!.....s.r....A5...b.s.A...:..4.\<.0..qE..W.C.a..#v*Yz..kD..!..%..==...*.....w...j0S....E.(...b.....~.|).q.....^.O...v.J..9.....D....$,.....a..Gu.....) RA..+f.4P..xSF..._.l3.z.T."A..G.Ea.mM.`R]..l6T1..{...JF..B.`.....E....j\"&~...w..F.q....!..J.}=,E.i....V.C.}.b1.6.pLI..<..[.V..}.....f..a.....w...t....v..Zh..d.XZ).3%..>.....3.uQ)C.>6L/ .A.Qd.....u.....v.:...m...K..@w..h..3...uJ.._.}.N.0.-....X\C...g..){.....)#.=.q.Y...S.C.. ..A';..>....0?.^'&.....6.....#u..a.nQ#/..s.)Y.x.....-1.c....j...!.B]8e.g+.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bootstrap[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	122474
Entropy (8bit):	5.093960028699236
Encrypted:	false
SSDEEP:	768:8sBGxw/wIHoS1LFN4vI6kHrviqbeoCk1NtFbdbHVO3+++vhuip3X22q0QmNaO:ww/nhOI6kHrviqIk3JVXB31V
MD5:	C5EC3E8CC0623722678112FAC229B8C8
SHA1:	AE1075BF5F15A8D794848FB974074227223A520D
SHA-256:	5F8DC136DA36D63CC6F9CAC536FDB5CB3B64B25C81269604B708E61A55FC8C6E
SHA-512:	CDB08C1EDC36C0C456D067FA6FBFBC5AC14D7FF85AE9BAA6D8A8E678D65AFD4B80BAC857C2553BEA63B691C0E018C220C179AD760E0C181A52E2CF9C7611C04
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/css/bootstrap.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bootstrap[1].css	
Preview:	/*!* Bootstrap v3.3.5 (http://getbootstrap.com).* Copyright 2011-2015 Twitter, Inc..* Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE) *//*!normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css*/html{font-family:sans-serif;-webkit-text-size-adjust:100%;-ms-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{margin:.67em 0;font-size:2em}mark{color:#000;background:#ff0}small{font-size:80%}sub,sup{position:relative;font-size:75%;line-height:0;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{height:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\box-5e3cec51ed8e99df6977c199d27812d7[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):	1514
Entropy (8bit):	5.492829226473901
Encrypted:	false
SSDEEP:	24:h+vFgj+AvQq9FkTqpNoVN96970UF2RS0GViso3RTsn4JRJ6MshCgrX4Nu:a1Ad8OpNgNAuUF2RtLR1Q4JRJChCgroU
MD5:	5E3CEC51ED8E99DF6977C199D27812D7
SHA1:	5547262C1169562043B7DC06A80FD832768726A1
SHA-256:	486762D56893F9B12FDFAD41C3A76F11FC745B5436E97E596A63C22EE13D2E33
SHA-512:	4ED903305DAA06CB822DC99636AF78E97A64A6339EE069C829F28DD1B77768FDA6783D3D46D91A97FDB30B4C3DFFB3C0704D17100ED38D28BF0F9255CDED56F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://vars.hotjar.com/box-5e3cec51ed8e99df6977c199d27812d7.html
Preview:	<!DOCTYPE html>..<html lang="en">.<head>.<meta charset="utf-8"/>.<script>(function(){function f(a){try{var b=JSON.parse(a.data);b.key&&g[b.key]&&g[b.key].parseCommand(b,a.origin)}catch(d){return null}}var p;try{p={cookie:{get:function(a){return(a=RegExp("(?:^|)"+a+"=([^;]*)").exec(document.cookie))?a[1]:void 0},set:function(a,b,d,h){a=[a+"="+b,"path=/","expires="+d.toUTCString()].concat(h||[]).join("; ");document.cookie=a},remove:function(a){document.cookie=a+"=; expires=Tue, 13 Mar 1979 00:00:00 UTC; path=/;"}}}catch(u){return}var g={_hjOptOut:new function(a,b,d,h,.f){this.parseCommand=function(c,g){function q(){var a=JSON.stringify({messageId:r,value:k||!1});window.parent.postMessage(a,"*")}var l=p[a],m=c.action,n=c.key,r=c.messageId,e=c.siteId,e=h?n:n+":"+e,k=c.value,s=c.expiresMinutes||1440*(c.expiresDays||365),t=function(){var a=new Date;a.setTime(a.getTime()+6E4*s);return a}();if(!function(){var a={_hjSet:d,_hjGet:b,_hjRemove:d}[m]||[];return 0<=a.indexOf("*")||0<=a.indexOf(g)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\carto[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 460 x 180, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	9343
Entropy (8bit):	7.928118421655706
Encrypted:	false
SSDEEP:	192:zOkNQuovYAn99BM9PTUAvbf2aXlj6GIe7V1q4kUbroHuJLNw+:zF6u69rkQAzOYmQq4kUc+i+
MD5:	DDECEE61C56ECBB4203EE6816923A764
SHA1:	CBE1C1306273B2B5B33F5B1A36CD0F2F7B87E7F0
SHA-256:	AA0736ECDFB7146FA6DB4D65A4104996D09F540018A1F0294AA7ED647F8E3CF3
SHA-512:	F5F6348DA0B5A9E0B59A32A13E77373B8FE1D3C5C949D546D9C714CCDE9F19BF240E55A608BAE625B4D364485110158EC6C9A90AE190BE12C6AA598A8568A05A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19tracking.narrativa.com/img/carto.png
Preview:	.PNG.....IHDR.....gAMA.....a...$6IDATx.....u.u.....H.8.)....)W8C0..s..`...v*$...|...I...Nc...qH.....!..I.A$..B'....f?.3..3.3.W...ov..{..7..3..D.D@.D....7n..g.G:.....ku.>...>.....u.l.t5.o..L..@...jW.....K.....@...L.[@.....7..=..*$R&VI..J.-.h.....&.....5.d..S.U....V..(a.....Q.....$9.A5Y.\.J..tE....f..Mu.....@t.qk.;....c7"...%\|-.u.5&.P"." ...@..H.I...2..j.8. q.(C.J.ehe.(.'`...$..0An...2...}.e...B..f!.UA...."..&..>.\%..8e.^.G.J...-" ."..D....w...U.....B..f!.QA...."..D.$..0Wu.....#.E.3..." ... I..8..D.....Bwi..w..]....fpM&.E@.\.@....;C5.t..#..H...3(Q.....+.H...d..hWu.n..E.o!.g0O.R.k?.#."PF.H..=d,..w.dG..]....9..%L.H....."..D...s.U+_]A.g.+i9M...{+J..6.....pE....>.K.E=:.....qQ....rQ.:J...." ...@...x.F.~.%G.s.4...1%L?;....p@..r+.e.....L.#..L1i~h..%%Ls.. ."..9.h...TI8.8E..x1E...N.." .).h.6.4..x3E...W.7" ... Y.:.....`-r....h.`...si.0shyU)."".....6.e<T.9.....4..Z.....M..r.....K.3..S.D...$K>.N.{....0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\casa-pedro-rabo-toro-madrid-kh8--1024x512@abc[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, baseline, precision 8, 1024x512, frames 3
Category:	downloaded
Size (bytes):	106982
Entropy (8bit):	7.962758453095419
Encrypted:	false
SSDEEP:	3072:W1jW+H+iFMxtSPzETymYdXLnwOdmOIoE3p4DeRNaIyCvidEo:4W+eiFMT3mHXLnwgmpyD/I1iqo
MD5:	87A60438469D8C57F22272E6978B8AC7
SHA1:	3B6DAC848988CB0C5D164027D3ABEFEC35A42D2B
SHA-256:	B73B6A1DC7E4D09B28868456E69D03D62B12BC52E3E2EB28D044F23A37702058
SHA-512:	7776596FAB375D904676874171B0E1414DEB046C022A999F816198A6023DEE32D9E7C110514F91E9A75B9A8EB5CFAF273D0327BF98BE7CD69C44FAA5C784180E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\casa-pedro-rabo-toro-madrid-kh8--1024x512@abc[1].jpg	
IE Cache URL:	http://https://static4.abc.es/media/gastronomia/2021/05/10/casa-pedro-rabo-toro-madrid-kh8--1024x512@abc.jpg
Preview:	......JFIF.....d.d.....,Photoshop 3.0.8BIM.....d.....d.....C.....C....."..... .....B.....!.1A."Q.2a#q..BR.3...$Cb..%...4Sr..&.....*.....!..1."A.Q2a..#.3Bq.....?...e.-..$.W.....W.$0....TF6f.Q"}....U... .Z.....OzW....]...2.....X.....'.!.;$.....:....Km.....k&.d6B..+.....y.....r)B.....I..u. a. sFC..1A.:..g....V..|.0RW....Q.[Z.R.;...Ym}9....|.....j...Bt..T.P...+&#dgp..CehB..>h....\. a.V.....& ..IXZ....Q..U.KDPq{d...j.....82.. ..|.i.<>#{e....r....5d6....j)....>..j../..T.yJ...}..iu.....IQmA' ...y....4.:.....M.V..UIr..[{.7."...I.....8rwy...i/ ...I...5..-..Z.<..'n...rVr.....R....R....*'.....,_H..n3.D .....nZ.T.;....BP.....X.Z....lw.LaZ$>..pi..d0.jV.U..U.7m.....VyF.....H.j.b.d.;]<U....[.Pe....C.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\chart.js@2.8[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	156721
Entropy (8bit):	5.3437462807874025
Encrypted:	false
SSDEEP:	3072:9IqGk57miKaxSUE879VE7CjWX1gLQmZ23M:9IqG67miKaxSUE879VEXO3
MD5:	B235B564DE9C2C1D61D7EF07FCF2B93B
SHA1:	2EBF900E0386749373E9887026590FE7DAFC30AE
SHA-256:	52FF41341B9CBC23E2A4A436352F706292668BC0D33847D303F9C7D9AA0900BC
SHA-512:	99FEFC2AE914FDAF2B8EBEDA051BC26B657083FAB4B548C984BB5C2B9DCF1C46C5C0212A43976EAE5CEF55381080AA6FF9FC8D313E99413D40ABAB6936A7F 9A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.jsdelivr.net/npm/chart.js@2.8.0
Preview:	/*!. * Chart.js v2.8.0. * https://www.chartjs.org. * (c) 2019 Chart.js Contributors. * Released under the MIT License. */.!function(t,e){"object"==typeof exports&&"undefi ned"!=typeof module?module.exports=e(function(){try{return require("moment")}catch(t){}}()):"function"==typeof define&&define.amd?define(["require"],function(t){return e(function(){try{return t("moment")}catch(t){}}())}):t.Chart=e(t.moment)}(this,function(t){"use strict";t=t&&t.hasOwnProperty("default")?t.default:t;var e={rgb2hsl:i,rgb2hs v:n,rgb2hwb:a,rgb2cmyk:o,rgb2keyword:s,rgb2xyz:l,rgb2lab:d,rgb2lch:function(t){return x(d(t))},hsl2rgb:u,hsl2hsv:function(t){var e=t[0],i=t[1]/100,n=t[2]/100;if(0===n)ret urn[0,0,0];return[e,100*(2*(i*=(n*=2)<=1?n:2-n)/(n+i)),100*((n+i)/2)]},hsl2hwb:function(t){return a(u(t))},hsl2cmyk:function(t){return o(u(t))},hsl2keyword:function(t){return s(u(t))},hsv2rgb:h,hsv2hsl:function(t){var e,i,n=t[0],a=t[1]/100,o=t[2]/100;return e=a*o,[n,100*(e=(e/=(i=(2-a)*o)<=1?i:2-i)||0),100*(i/=2)]},hsv

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\cookie_push_onload[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	1174
Entropy (8bit):	5.74166936214599
Encrypted:	false
SSDEEP:	24:hY6t2eJJBewfHDdUg8EcvjHODQMJXeK+C6uS/MLmeK+C6uSGymWAuDSXeMzCUtVv:9V4goLHODS1CTXT1CTVyPyCM6Nu
MD5:	2FE2B1F17888E326B010A8CDA72D48D3
SHA1:	59CBBEEDE4C472024C482BAE8529144119BBBD27
SHA-256:	9A9B7FB32E01FD70747F32EFDBD0472FD681C85EEBB0C42D10C7A514820A0062
SHA-512:	30BE2E73020EB97A67709E47DED40E999D352DA9B94EDD946D1315BDA65AD616AAA3CDFCFA675D061E4ED4AE1BAE3F0D245908D44411B2425C49B4345D2F66 07
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>.<head>. <title></title>. <script type="text/javascript">(function(){var f=null,g=null;function l(a){var b="";n(a,function(a){b+=String.fromCharCo de(a)});return b}function n(a,b){function c(b){for(;e<a.length;){var c=a.charAt(e++),d=g[c];if(null!=d)return d;if(!/^[\s\xa0]*$/.test(c))throw Error("Unknown base64 encoding at char: "+c);}return b}p();for(var e=0;;){var d=c(-1),m=c(0),h=c(64),k=c(64);if(64===k&&-1===d)break;b(d<<2|m>>4);64!=h&&(b(m<<4&240|h>>2),64!=k&&b(h<<6&192|k))}}.f unction p(){if(!f){f={};g={};for(var a=0;65>a;a++)f[a]="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=".charAt(a),g[f[a]]=a,62<=a&& (g["ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_".charAt(a)]=a)}};function q(){for(var a=window.location.hash.substring(1).split(","),b=0;b<a.length;b++){var c=l(a[b]),e=window;e.google_image_requests||(e.google_image_requests=[]);var d=e.document.createElement("img");d.src=c;e.google_ima ge_requests.push(d)}}var r=!1;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\cookie_push_onload[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1174
Entropy (8bit):	5.74166936214599
Encrypted:	false
SSDEEP:	24:hY6t2eJJBewfHDdUg8EcvjHODQMJXeK+C6uS/MLmeK+C6uSGymWAuDSXeMzCUtVv:9V4goLHODS1CTXT1CTVyPyCM6Nu
MD5:	2FE2B1F17888E326B010A8CDA72D48D3
SHA1:	59CBBEEDE4C472024C482BAE8529144119BBBD27
SHA-256:	9A9B7FB32E01FD70747F32EFDBD0472FD681C85EEBB0C42D10C7A514820A0062
SHA-512:	30BE2E73020EB97A67709E47DED40E999D352DA9B94EDD946D1315BDA65AD616AAA3CDFCFA675D061E4ED4AE1BAE3F0D245908D44411B2425C49B4345D2F66 07
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\cookie_push_onload[2].htm	
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/pagead/s/cookie_push_onload.html
Preview:	<!DOCTYPE html>.<html>.<head>. <title></title>. <script type="text/javascript">(function(){var f=null,g=null;function l(a){var b="";n(a,function(a){b+=String.fromCharCode(a)});return b}function n(a,b){function c(b){for(;e<a.length;){var c=a.charAt(e++),d=g[c];if(null!=d)return d;if(!/^[\s\xa0]*$/.test(c))throw Error("Unknown base64 encoding at char: "+c);}return b}p();for(var e=0;;){var d=c(-1),m=c(0),h=c(64),k=c(64);if(64===k&&-1===d)break;b(d<<2|m>>4);64!=h&&(b(m<<4&240|h>>2),64!=k&&b(h<<6&192|k))}}.function p(){if(!f){f={};g={};for(var a=0;65>a;a++)f[a]="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=".charAt(a),g[f[a]]=a,62<=a&&(g["ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_".charAt(a)]=a)}};function q(){for(var a=window.location.hash.substring(1).split(",",),b=0;b<a.length;b++){var c=l(a[b]),e=window;e.google_image_requests||(e.google_image_requests=[]);var d=e.document.createElement("img");d.src=c;e.google_image_requests.push(d)}}var r=!1;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\coronavirus[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 2562 x 1000, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	128113
Entropy (8bit):	7.7442775097721555
Encrypted:	false
SSDEEP:	3072:NcxzVODHHr3+ujPZ6OJpKcBKoorWcwyKiwN/dU94EpuB:wVODHLJh6RWzoKcwl/y9luB
MD5:	E328FA60DEA2B70BD55DFE5DB19636A3
SHA1:	E712B92D0DC01607335824BA98AAAF05CDE8E616
SHA-256:	4DCC4A7825DA718D5DFB14AFC17368318274D708C4BCF66DBF5746869BC398E0
SHA-512:	61912F0C288FC7454BEDC843FC89DAA8D57253E211E5C063DB55DDB384F77C6B8F5718156BCA5150EF4D5A6AADAF8F5D6CFFE38DF90878728BAA0194029875E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://4i2g925ohj.execute-api.eu-west-3.amazonaws.com/pro/coronavirus?confirmed_num=158.339.218&actives_num=49.872.666&recovered_num=105.173.319&deaths_num=3.293.233®ion_confirmed_num=3.567.408®ion_confirmed_today_num=8.186®ion_deaths_today_num=66®ion_deaths_num=78.792&date=10%20de%20mayo%20del%202021&top_paises1=EE.UU.&top_paises2=India&top_paises3=Brasil&top_paises1_num=32.707.799&top_paises2_num=22.662.575&top_paises3_num=15.184.790&top_comunidades1=Madrid&top_comunidades2=Catalu%C3%B1a&top_comunidades3=Andaluc%C3%ADa&top_comunidades1_num=692.750&top_comunidades2_num=592.912&top_comunidades3_num=558.932&gen_date=2021/05/10&gen_time=10%3A00&client=default_web®ion=world
Preview:	.PNG.....IHDR.....L.....IDATx...w`.....MOh..K ...4..DP…bA.....{.*WQQ..(H...]@).A:..j..e.....l6[f.M.~.q8{.g..N.y..... ..... ..... .....MS:..UnX...-.=..-{.t.....7.m.l.....3Kg.....pC).2.Voj9..~.....4.....`J.....O.s.k.y.R.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\css2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	394
Entropy (8bit):	5.0763466687204755
Encrypted:	false
SSDEEP:	12:jF/iO6ZRoMqt6pixhnqF/iO6ZN0qt6pixQZJY:5/iOY7aNxh+/iOYN0aNxMK
MD5:	8ECA5BE5716C9A67A4255EB483070A84
SHA1:	CAA5346B3ACD1BBD6244E84A7B3EBD8E04D57564
SHA-256:	8D403531AC59D06314856C7A97B32BF2896E26E8E84F1E10D515EE2B5BA31E40
SHA-512:	D94CF5CCEB3EB5D2EC5CF37FA83B190FB9DCB77F99C7B2AE0E66C4E4150954C2C35DD4023B050461E55A152EA59B6D31F1A502F4791D1A76A4EE0E5AF8B4FCB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css2?family=Roboto:wght@400;700&display=swap
Preview:	@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Me5g.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 700;. font-display: swap;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlvAA.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	175
Entropy (8bit):	5.0522421646209255
Encrypted:	false
SSDEEP:	3:0SYWFFWIIYCzHRiRI5XwDKLRIHDfFRWdFTfqzrZqcdAqsKTCEIoENRgVoYARNin:0IFFli+56ZRWHTizlpdAxInVuNin
MD5:	C9B33444138B8312C889B87B157D7830
SHA1:	60CF82CB0DEF72CD46143D1BD562BE26BA874802
SHA-256:	8EB72810C473A7DBEAB9EA57FDBFAA004741DFFE2070CACCAC318052AF3B81A1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\css[1].css	
SHA-512:	93655BE7DE9E3EC1116810D442396C69456FB7EFE746003BE23A23BE5EBB927246EF3EBC9A68B7E11DF392714870D570F3C733CE2B7D73D895094FFAF7D680B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Roboto
Preview:	@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	196
Entropy (8bit):	5.216636356333161
Encrypted:	false
SSDEEP:	3:0SYWFFWlIYCQWb6MRI5XwDKLRIHDfFRWdFTfqzrZqcdfbwTTu7lQzoIcH9MSQUYn:0IFFQC+56ZRWHTizlpdfOuxHHhFNin
MD5:	EA2BA08328DAAE44F54FEEE41724FE99
SHA1:	C1CC6020B57B6CDAE4115CB4572FB92DF7A4B652
SHA-256:	AC00B42673BF10B10E44CF70FBD2D5B85B2DE19D314561BCB2C0AFA1607FBCA0
SHA-512:	247846B4910A71028BAE75DDC3C306C8C2E1D97F65509E8878087684DBC3EEF63636056539A5AE348F9312FFA0DECEEF20E24E7A91D1F25D27A9270030DC615
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=IBM+Plex+Mono
Preview:	@font-face {. font-family: 'IBM Plex Mono';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/ibmplexmono/v6/-F63fjptAgt5VM-kVkqdyU8n1i8q0 Q.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\email-decode.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1239
Entropy (8bit):	5.068464054671174
Encrypted:	false
SSDEEP:	24:ch63Cf5W8QPIHRZ3hwVFS39bYGwNef1yTZsNUkQ1sZmSuLqNWRco5Jcn5IKM6cuY:C6SQnw/x+SR8ZZkQbp1RZ5JwiKMm7Zc
MD5:	9E8F56E8E1806253BA01A95CFC3D392C
SHA1:	A8AF90D7482E1E99D03DE6BF88FED2315C5DD728
SHA-256:	2595496FE48DF6FCF9B1BC57C29A744C121EB4DD11566466BC13D2E52E6BBCC8
SHA-512:	63F0F6F94FBABADC3F774CCAA6A401696E8A7651A074BC077D214F91DA080B36714FD799EB40FED64154972008E34FC733D6EE314AC675727B37B58FFBEBEBE E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\email-decode.min[1].js	
Preview:	!function(){"use strict";function e(e){try{if("undefined"==typeof console)return;"error"in console?console.error(e):console.log(e)}catch(e){}}function t(e){return d.innerHTML='',d.childNodes[0].getAttribute("href")||""}function r(e,t){var r=e.substr(t,2);return parseInt(r,16)}function n(n,c){for(var o="",a=r(n,c),i=c+2;i<n.length;i+=2){var l=r(n,i)^a;o+=String.fromCharCode(l)}try{o=decodeURIComponent(escape(o))}catch(u){e(u)}return t(o)}function c(t){for(var r=t.querySelectorAll("a"),c=0;c<r.length;c++)try{var o=r[c],a=o.href.indexOf(l);a>-1&&(o.href="mailto:"+n(o.href,a+l.length))}catch(i){e(i)}}function o(t){for(var r=t.querySelectorAll(u),c=0;c<r.length;c++)try{var o=r[c],a=o.parentNode,i=o.getAttribute(f);if(i){var l=n(i,0),d=document.createTextNode(l);a.replaceChild(d,o)}}catch(h){e(h)}}function a(t){for(var r=t.querySelectorAll("template"),n=0;n<r.length;n++)try{i(r[n].content)}catch(c){e(c)}}function i(t){try{c(t),o(t),a(t)}catch(r){e(r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	135340
Entropy (8bit):	5.5593152421892285
Encrypted:	false
SSDEEP:	1536:M8FNc2MxgK0jWFZDJQlqtEf9NsF9Ptd47FDYSGsX9Ufak+p+w7a/cHu9WXbeLrEl:HSNQlq6K9PbmnbLmm0WXbJ7lVtRZTR
MD5:	7F56F23F672C565EC595375EA033CCC6
SHA1:	63791F235EADBDD7F7B49559B4B56D70C7A9DB6C
SHA-256:	15ABAD0EB398F2BF11D4B4DCE00F402F63A9C1C03D233989508B0E295281B546
SHA-512:	25DF81AE848C839E6EECA2800ED32A07FF9CCA44429D45392965C157DBBA49FCB580C3AE63340F2FC2A54863073DF42D4FE653C3AF6B110226B9246633DF42A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js
Preview:	(function(sttc){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .var n,aa;function ba(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var ca="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 ea(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&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 fa=ea(this),ha="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),p={},ia={};function r(a,b){var c=ia[b];if(null==c)return a[b];c=a[c];return void 0!==c?c:a[b]} .function u(a,b,c){if(b)a:{var d=a.split(".");a=1===d.length;var e=d[0],f;!a&&e in p?f=p:f=fa;for(e=0;e<d.length-1;e++){var g=d[e];if(!(g in f))break a;f=f[g]}d=d[d.length-1];c=ha&&"es6"===c?f[d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\f[2].txt	
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):	11600
Entropy (8bit):	6.016017964621134
Encrypted:	false
SSDEEP:	192:XvUhIgVpiwniHiJDGFIpeWpUY3fTndA59wOT1vAJ4lO6dJh+gkAyHCWu6JRMIqyj:HgVpixiprHpbbdAfwOT1vAmlOz7iYUwj
MD5:	D64363C85CD2BD59C4A18B360E06C675
SHA1:	5EABC2C4924BD15F1FB4A47B702FAFB1DBAFAFCC
SHA-256:	EFD6A8D34EBD0842419D3DF15BE9C3558BC459F53ABA96B8924EE7E3ECC4D1C9
SHA-512:	017091012764033FFB3C1467D1049A4F00C8100CD911E4FDDD2B3BE9B757BF19BD97BF7CF99A89C8DB0C652748D17C31B3FD7919B8249C3E795C149C1D6131F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/getconfig/sodar?sv=200&tid=gda&tv=r20210505&st=env

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\f[2].txt	
Preview:	{"sodar_query_id":"a-qYYMPQI_6V7_UPz_eJ8Ag","injector_basename":"sodar2","bg_hash_basename":"HpwNkB4r-iltD3wVs4tNs86Vb9pM92Oc366-IABnofE","bg_binary":"vaDJ2f7Dyj8rcnnV+oABVPDAlWwuz7Y9IApIPMoNY0h9LBnH0z53JCoKBrNz4CK4CCbaG/0sFcHAr6tKd9cA1giINf9uWTrS/wp115073CHYKHLOdZxvb384P0AJ/DPeTrFoq2dpNjA6RPIBgqpPApHr7y5CZVTV53LsXNENyDMrze+IQoIBT4/1VjrWNR+snZ7nCz6eAmNPNiDzaYl+7ZH1SJhhHoVKojDDR460sw5frZsnayaLqg4n3tvEKHlY8j6ARzsxPcFdHV31r7GM8gvpuqPrfBg5ZvFBAI81BtuZ9huJETKPBCJTJ2mBroXFo2Q1zrhshoETuNrAbosOMiIuRHSDgK8wYsti8f3HjzCdMtTnkD5n5hq0XYdztTQ79fN3q/9OtC11bQpDk3kAx4zrGZRKelTlqVci8HCPoZihEvNotV3hVnEE8SmW08nMtYS1jhoMLkpyL7sQT3JtMT9Mxu1nq+FaiWKoNntx6ZnmYzRd9Udzo93f3fapjQ7OSCENOIxd79TwqK30K2FPR6O9PFgz66wWmlG7WAFH5v5dSmCePKF54QC/mDnkDTA+IWnR1Cw6js6dhYo1DiI1K3yIFh4Cq1M6lXDCRZ5KlUKkozM9DLT20KYKt46AIHdONIrZDDFty5AysKsvWzgbKbr8xIF4XP2N0sqTBAiIFBteoY/C4vPzgEic6Tt4mvRyfE8gT950vUI7wOkzY28SokLEj82FOgu22bQJ0tYmwvjliJoeMi4wXb2CN1d/gteec4EaxYs8o8q+ylgmsmbEm4mN9hXHYkdcBQensDWu105QbfNKY4JiJpUx0PREYWLQoXMAYAXBXV5DLshLB

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\f[3].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	6716
Entropy (8bit):	5.434549771102314
Encrypted:	false
SSDEEP:	96:LScH4yqXEwjsNgD4ZqRPe83bwgc3j3T9f2hgEpUrEaI5hKU9fdr3jEI:LScH4ycEbNgDv20V0+hgEpUgaIt9FrgI
MD5:	E76687FCCC7D4223217B796C10F4334C
SHA1:	B7314FB59141C98E96F440B7B9C43245DBB49479
SHA-256:	580175BBF792F751911D37F6B000167E51A768B9F9EC4532EE7B2E52B7316E8A
SHA-512:	F8E153E01A482EBF515778B07A27B452295975CB830AFA7E9AF57C493B196C786C11655D880BB572AABD2DB544C5DC44A9B1A9C0E6A3E90A4126794D5CEB56D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/pagead/js/r20210505/r20110914/elements/html/spam_signals/spam_signals_bundle.js
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .var e=this||self;var h=Array.prototype.indexOf?function(a,b){return Array.prototype.indexOf.call(a,b,void 0)}:function(a,b){if("string"===typeof a)return"string"!==typeof b||1!=b.length?-1:a.indexOf(b,0);for(var c=0;c<a.length;c++)if(c in a&&a[c]===b)return c;return-1},m=Array.prototype.forEach?function(a,b){Array.prototype.forEach.call(a,b,void 0)}:function(a,b){for(var c=a.length,d="string"===typeof a?a.split(""):a,f=0;f<c;f++)f in d&&b.call(void 0,d[f],f,a)};function n(a){var b=!1,c;return function(){b||(c=a(),b=!0);return c}};function p(a){p[" "](a);return a}p[" "]=function(){};var q={Event:{l:"click",J:"dblclick",j:"mousedown",ca:"mouseup",ba:"mouseover",aa:"mouseout",$:"mousemove",Y:"mouseenter",Z:"mouseleave",ya:"touchstart",xa:"touchmove",wa:"touchend",va:"touchcancel",S:"keypress",o:"keydown",T:"keyup",L:"deviceorientation",da:"MozOrientation",K:"devicemotion",ka:"orientationch

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\f[4].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:tDKn:tDK
MD5:	124D3918819AB4C349A7F9FA979BEF07
SHA1:	6AD167D76A8768130783CD19AA6D8143C0B1BF37
SHA-256:	DAA795332E5DBCF893ADF2D5F3349F02B8C1CB957FF3B5F4C11B742E33C3376F
SHA-512:	4F7F15B28C6B38FC66002DBEE29688B801A689B716093BA63ADBE23FFFE144621198973A8AC4981FF2D20881BD4C84E45130A631E5B9A5EAE3A5FE26C106F7D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://partner.googleadservices.com/gampad/cookie.js?domain=localcoronavirus.com&callback=_gfp_s_&client=ca-pub-4607443575710795&cookie=ID%3D246690374f7834b9-22e1539e0cc8007f%3AT%3D1620634217%3ART%3D1620634217%3AS%3DALNI_MaaSjGCWhXUyvXhhwrCEe0XJNKY9A
Preview:	_gfp_s_({});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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):	26711
Entropy (8bit):	4.753681219070429
Encrypted:	false
SSDEEP:	384:/i5yWeTUKW+KlkJ5de2UYmydfwYUas8l8yQ/7:klr+Klk3YlKfwYUf8l8yQ/7
MD5:	0831CBA6A670E405168B84AA20798347
SHA1:	05EA25BC9B3AC48993E1FEE322D3BC94B49A6E22
SHA-256:	936FFCCDC35BC55221E669D0E76034AF76BA8C080C1B1149144DBBD3B5311829
SHA-512:	655F4A6B01B62DE824C29DE7025C4B21516E7536AE5AE0690B5D2E11A7CC1D82F449AAEBCF903B1BBF645E1E7EE7EC28C50E47339E7D5D7D94663309DFA5A996
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/css/font-awesome.min.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\font-awesome.min[1].css	
Preview:	/*!. * Font Awesome 4.4.0 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=4.4.0');src:url('../fonts/fontawesome-webfont.eot?#iefix&v=4.4.0') format('embedded-opentype'),url('../fonts/fontawesome-webfont.woff2?v=4.4.0') format('woff2'),url('../fonts/fontawesome-webfont.woff?v=4.4.0') format('woff'),url('../fonts/fontawesome-webfont.ttf?v=4.4.0') format('truetype'),url('../fonts/fontawesome-webfont.svg?v=4.4.0#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\MEEXW4H4\hotjar-2075733[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3502
Entropy (8bit):	5.250106220561627
Encrypted:	false
SSDEEP:	48:Z1f+Bmr4DDilr/CpDuMY6wRQAQl07k5G8r4U4R5UETledeHtwWNxsTnOf3DZ:ORPi6/snIQg24U4bU4qO0qTZ
MD5:	0B42C46D0511566FB0AA2DDC34D6F585
SHA1:	09F69BFBB93271C43307D1EFEEFC547CF368E15E
SHA-256:	AC77F7A971CDA919D497BD657C41D77F3F342D49155D8936788B580481EF5A5F
SHA-512:	15062A19963273FEFFF9BD279581ABCCEB085C5EC68BC12AB334EFA05774CF854EA5EC68E1CDC466E866627CCDCCF22671021645FBE78B65A0D15D4836D123B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.hotjar.com/c/hotjar-2075733.js?sv=6
Preview:	window.hjSiteSettings = window.hjSiteSettings || {"site_id":2075733,"r":0.493100070271164,"rec_value":0.0,"state_change_listen_mode":"automatic","record":false,"continuous_capture_enabled":false,"recording_capture_keystrokes":false,"anonymize_digits":true,"anonymize_emails":true,"suppress_all":false,"suppress_text":false,"suppress_location":false,"user_attributes_enabled":false,"legal_name":null,"privacy_policy_url":null,"deferred_page_contents":[],"record_targeting_rules":[],"feedback_widgets":[],"heatmaps":[],"polls":[],"integrations":{"optimizely":{"tag_recordings":false}},"features":["heatmap.continuous_capture","recordings.filter_new_user","survey.impressions","feedback.widgetV2","feedback.full_screen_survey","settings.billing_v2","feedback.widget_telemetry"]};..!function(e){var t={};function n(o){if(t[o])return t[o].exports;var r=t[o]={i:o,l:!1,exports:{}};return e[o].call(r.exports,r,r.exports,n),r.l=!0,r.exports}n.m=e,n.c=t,n.d=function(e,t,o){n.o(e,t)||Object.defineProperty(e,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	low
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\hv-TlzNxIFoO84YddYQyKTdYVA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17436, version 1.1
Category:	downloaded
Size (bytes):	17436
Entropy (8bit):	7.965352471070945
Encrypted:	false
SSDEEP:	384:ChlDcp5BWeKjusp5cqGp6sbnmBrzqlUToVYH1/jY:wAxWeeuHqGpjbmB3qmoGY
MD5:	FAE921830A5CD9C547291C01A4CC69FC
SHA1:	67A6D64EC90969D7F2B5ED5EAF00B75DB66BC2F2
SHA-256:	5DD422BF3BA941E0CD33C3F16ACDB0442727B3419668930F9C97B814CD2E051E
SHA-512:	B647D1456FC3A8CD48D19CB80F302EF17D52E0156D6EC7A307ABBA313F918128E249F99398C2B932F393056815014A9B7DC9B955B377AB9C37BEAF911AEAABF9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/biryani/v6/hv-TlzNxIFoO84YddYQyKTdYVA.woff

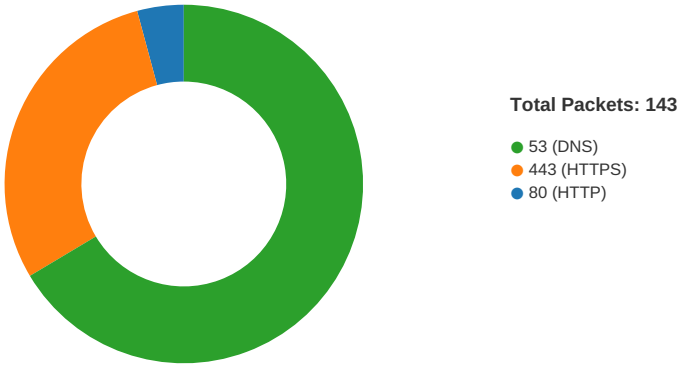
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\hv-TlzNxIFoO84YddYQyKTdYVA[1].woff	
Preview:	wOFF.....D.....z.....GDEF..... ..."...xGPOS..... ... DvLuGSUB...../.....eOS/2.....N...`y...cmap...@.....V.. .cvt .....F...d....fpgm.....g...a.._.gasp..... ...glyf.....2(..\.d..head..<....6...6...Thhea..<.....$....hmtx..=.....;Fnloca..>.....i/maxp..@.... ... .K.wname..@.....T.RKKpost..A.....}}d..prep..C....~.....la.x.....\}M.f.D0 .e.%..\O>.....DFLT.....x..3Cpa.....k...F.m.....e755555...t.3w.{n<..N.a.b.....<...kiVm9.....0...../39.s._.....\|.....+.>.;.....X.Qdas..(...WP..y...c\...9.E....\..7.r.?. .E.Y....R..\.kr]n...<&....!Miq..$...,...&'y...2o1<..vHA.n.z.....)..8.Ec..^k....g..b...5.....l'..7wF.<M.&.z.....:.2..N.R..".{.l.7.ru.x.c`fRd.f`e``.b.```...q.F...@.....H.$?-....WI.%.o...K(..... 9&%.o@J.....&....x.].3.\....Y.c;?{.m.m.nc.m...i.*6..A.....B..py...J".<..m..n{...j.>...~.....X._P<..l...%{.....*n..v..^...,..i...E.o..s...m.7.^.}.....lz.M..Q.uO...&4.....6

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2021 10:10:13.245945930 CEST	49714	80	192.168.2.3	172.67.183.244
May 10, 2021 10:10:13.245999098 CEST	49715	80	192.168.2.3	172.67.183.244
May 10, 2021 10:10:13.286693096 CEST	80	49714	172.67.183.244	192.168.2.3
May 10, 2021 10:10:13.286780119 CEST	49714	80	192.168.2.3	172.67.183.244
May 10, 2021 10:10:13.287583113 CEST	49714	80	192.168.2.3	172.67.183.244
May 10, 2021 10:10:13.287650108 CEST	80	49715	172.67.183.244	192.168.2.3
May 10, 2021 10:10:13.287731886 CEST	49715	80	192.168.2.3	172.67.183.244
May 10, 2021 10:10:13.328294992 CEST	80	49714	172.67.183.244	192.168.2.3
May 10, 2021 10:10:13.342283964 CEST	80	49714	172.67.183.244	192.168.2.3
May 10, 2021 10:10:13.342339993 CEST	49714	80	192.168.2.3	172.67.183.244
May 10, 2021 10:10:13.382330894 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:13.423221111 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:13.423361063 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:13.465759039 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:13.508804083 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:13.518620014 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:13.518646002 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:13.518712044 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:13.518752098 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:13.574532032 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:13.582077980 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:13.582390070 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:13.615398884 CEST	443	49716	172.67.183.244	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2021 10:10:13.615684986 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:13.615701914 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:13.615765095 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:13.615900040 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:13.617927074 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:13.623027086 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:13.623050928 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:13.623105049 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:13.656651974 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:13.703417063 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:13.997133970 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:13.997214079 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.001161098 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.001177073 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.001193047 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.001204967 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.001218081 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.001244068 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.001610041 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.001627922 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.001658916 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.001693010 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.002623081 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.002639055 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.002681017 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.002722979 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.034748077 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.034773111 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.034893990 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.034893036 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.034910917 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.034955025 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.035476923 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.035505056 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.035526037 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.035566092 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.036458015 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.036484957 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.036521912 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.036562920 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.037451982 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.037477970 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.037508011 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.037525892 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.038381100 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.038435936 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.099291086 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.099962950 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.100600958 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.101228952 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.102847099 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.103508949 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.104146957 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.104775906 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.105412006 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.107353926 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.140151024 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.140733004 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.141360044 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.142004967 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.145962000 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.145977020 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.145982981 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.146409988 CEST	443	49716	172.67.183.244	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2021 10:10:14.147186041 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.149128914 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.152242899 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.152257919 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.152273893 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.152319908 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.152343988 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.152404070 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.152908087 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.152966022 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.153003931 CEST	443	49716	172.67.183.244	192.168.2.3
May 10, 2021 10:10:14.153043032 CEST	49716	443	192.168.2.3	172.67.183.244
May 10, 2021 10:10:14.153378963 CEST	443	49716	172.67.183.244	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2021 10:10:03.946178913 CEST	57544	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:03.999682903 CEST	53	57544	8.8.8.8	192.168.2.3
May 10, 2021 10:10:05.571794033 CEST	55984	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:05.625400066 CEST	53	55984	8.8.8.8	192.168.2.3
May 10, 2021 10:10:06.441524029 CEST	64185	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:06.490377903 CEST	53	64185	8.8.8.8	192.168.2.3
May 10, 2021 10:10:07.628489971 CEST	65110	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:07.678795099 CEST	53	65110	8.8.8.8	192.168.2.3
May 10, 2021 10:10:08.678534985 CEST	58361	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:08.730055094 CEST	53	58361	8.8.8.8	192.168.2.3
May 10, 2021 10:10:10.534929991 CEST	63492	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:10.583492041 CEST	53	63492	8.8.8.8	192.168.2.3
May 10, 2021 10:10:11.524022102 CEST	60831	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:11.589056969 CEST	53	60831	8.8.8.8	192.168.2.3
May 10, 2021 10:10:11.911669970 CEST	60100	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:11.960264921 CEST	53	60100	8.8.8.8	192.168.2.3
May 10, 2021 10:10:13.155260086 CEST	53195	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:13.223541021 CEST	53	53195	8.8.8.8	192.168.2.3
May 10, 2021 10:10:14.113147020 CEST	50141	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:14.124916077 CEST	53023	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:14.170272112 CEST	53	50141	8.8.8.8	192.168.2.3
May 10, 2021 10:10:14.173480988 CEST	53	53023	8.8.8.8	192.168.2.3
May 10, 2021 10:10:14.631124973 CEST	49563	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:14.666594028 CEST	51352	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:14.679932117 CEST	53	49563	8.8.8.8	192.168.2.3
May 10, 2021 10:10:14.731324911 CEST	53	51352	8.8.8.8	192.168.2.3
May 10, 2021 10:10:14.969357014 CEST	59349	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.057516098 CEST	53	59349	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.323745012 CEST	57084	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.383980989 CEST	53	57084	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.404093981 CEST	58823	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.430960894 CEST	57568	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.454746962 CEST	50540	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.465584040 CEST	53	58823	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.493063927 CEST	53	57568	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.513704062 CEST	54366	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.520025015 CEST	53034	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.535191059 CEST	57762	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.542586088 CEST	55435	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.548643112 CEST	53	50540	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.553714037 CEST	50713	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.565409899 CEST	56132	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.587017059 CEST	53	53034	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.594146967 CEST	53	57762	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.602931976 CEST	58987	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.616774082 CEST	53	55435	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.616800070 CEST	53	50713	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2021 10:10:15.624723911 CEST	53	56132	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.642855883 CEST	56579	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.658587933 CEST	60633	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.658613920 CEST	61292	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.660589933 CEST	63619	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.663733959 CEST	53	58987	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.674156904 CEST	64938	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.705456018 CEST	53	56579	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.712335110 CEST	61946	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.718332052 CEST	53	63619	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.719470978 CEST	64910	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.719856977 CEST	52123	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.722278118 CEST	53	60633	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.722882986 CEST	56130	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:15.725678921 CEST	53	61292	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.733328104 CEST	53	54366	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.734384060 CEST	53	64938	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.776252985 CEST	53	61946	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.788624048 CEST	53	52123	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.797442913 CEST	53	64910	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.801578999 CEST	53	56130	8.8.8.8	192.168.2.3
May 10, 2021 10:10:15.977479935 CEST	56338	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:16.026253939 CEST	53	56338	8.8.8.8	192.168.2.3
May 10, 2021 10:10:16.344170094 CEST	59420	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:16.410202980 CEST	53	59420	8.8.8.8	192.168.2.3
May 10, 2021 10:10:16.424503088 CEST	58784	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:16.483540058 CEST	63978	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:16.489568949 CEST	53	58784	8.8.8.8	192.168.2.3
May 10, 2021 10:10:16.511981964 CEST	62938	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:16.542710066 CEST	55708	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:16.550755978 CEST	53	63978	8.8.8.8	192.168.2.3
May 10, 2021 10:10:16.560633898 CEST	53	62938	8.8.8.8	192.168.2.3
May 10, 2021 10:10:16.603355885 CEST	53	55708	8.8.8.8	192.168.2.3
May 10, 2021 10:10:17.471801996 CEST	56803	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:17.495307922 CEST	57145	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:17.498796940 CEST	55359	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:17.516526937 CEST	58306	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:17.540241003 CEST	53	56803	8.8.8.8	192.168.2.3
May 10, 2021 10:10:17.541526079 CEST	64124	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:17.547173023 CEST	49361	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:17.562201023 CEST	53	55359	8.8.8.8	192.168.2.3
May 10, 2021 10:10:17.574480057 CEST	53	57145	8.8.8.8	192.168.2.3
May 10, 2021 10:10:17.577469110 CEST	53	58306	8.8.8.8	192.168.2.3
May 10, 2021 10:10:17.607004881 CEST	53	64124	8.8.8.8	192.168.2.3
May 10, 2021 10:10:17.612548113 CEST	53	49361	8.8.8.8	192.168.2.3
May 10, 2021 10:10:17.622539997 CEST	63150	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:17.626418114 CEST	53279	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:17.687529087 CEST	53	53279	8.8.8.8	192.168.2.3
May 10, 2021 10:10:17.687551975 CEST	53	63150	8.8.8.8	192.168.2.3
May 10, 2021 10:10:17.974255085 CEST	56881	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:18.034049034 CEST	53	56881	8.8.8.8	192.168.2.3
May 10, 2021 10:10:21.840981960 CEST	53642	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:21.884216070 CEST	55667	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:21.892529011 CEST	53	53642	8.8.8.8	192.168.2.3
May 10, 2021 10:10:21.941531897 CEST	53	55667	8.8.8.8	192.168.2.3
May 10, 2021 10:10:22.585586071 CEST	54833	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:22.654129982 CEST	53	54833	8.8.8.8	192.168.2.3
May 10, 2021 10:10:25.650511026 CEST	62476	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:25.710621119 CEST	53	62476	8.8.8.8	192.168.2.3
May 10, 2021 10:10:29.976681948 CEST	49705	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:29.980170012 CEST	61477	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:29.983831882 CEST	61633	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:30.015604973 CEST	55949	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:30.023507118 CEST	57601	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2021 10:10:30.032537937 CEST	53	61633	8.8.8.8	192.168.2.3
May 10, 2021 10:10:30.032566071 CEST	49342	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:30.039772987 CEST	53	61477	8.8.8.8	192.168.2.3
May 10, 2021 10:10:30.054897070 CEST	53	49705	8.8.8.8	192.168.2.3
May 10, 2021 10:10:30.060630083 CEST	56253	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:30.064357042 CEST	53	55949	8.8.8.8	192.168.2.3
May 10, 2021 10:10:30.069701910 CEST	49667	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:30.073438883 CEST	55439	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:30.099116087 CEST	53	49342	8.8.8.8	192.168.2.3
May 10, 2021 10:10:30.099313974 CEST	53	57601	8.8.8.8	192.168.2.3
May 10, 2021 10:10:30.125963926 CEST	53	56253	8.8.8.8	192.168.2.3
May 10, 2021 10:10:30.135770082 CEST	53	49667	8.8.8.8	192.168.2.3
May 10, 2021 10:10:30.149425983 CEST	53	55439	8.8.8.8	192.168.2.3
May 10, 2021 10:10:30.437156916 CEST	57069	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:30.485790968 CEST	53	57069	8.8.8.8	192.168.2.3
May 10, 2021 10:10:30.965559959 CEST	57659	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:31.014225960 CEST	53	57659	8.8.8.8	192.168.2.3
May 10, 2021 10:10:35.967201948 CEST	54717	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:36.037822008 CEST	53	54717	8.8.8.8	192.168.2.3
May 10, 2021 10:10:36.972377062 CEST	63975	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:37.037971973 CEST	53	63975	8.8.8.8	192.168.2.3
May 10, 2021 10:10:37.166699886 CEST	56639	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:37.229310989 CEST	53	56639	8.8.8.8	192.168.2.3
May 10, 2021 10:10:39.201261997 CEST	51856	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:39.262589931 CEST	53	51856	8.8.8.8	192.168.2.3
May 10, 2021 10:10:41.548145056 CEST	56546	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:41.599739075 CEST	53	56546	8.8.8.8	192.168.2.3
May 10, 2021 10:10:41.718528986 CEST	62152	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:41.766992092 CEST	53	62152	8.8.8.8	192.168.2.3
May 10, 2021 10:10:42.823112011 CEST	56546	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:42.875878096 CEST	53	56546	8.8.8.8	192.168.2.3
May 10, 2021 10:10:42.961105108 CEST	53470	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:43.013643980 CEST	53	53470	8.8.8.8	192.168.2.3
May 10, 2021 10:10:43.843993902 CEST	56546	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:43.896836042 CEST	53	56546	8.8.8.8	192.168.2.3
May 10, 2021 10:10:43.962263107 CEST	53470	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:44.010916948 CEST	53	53470	8.8.8.8	192.168.2.3
May 10, 2021 10:10:45.117361069 CEST	53470	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:45.166043043 CEST	53	53470	8.8.8.8	192.168.2.3
May 10, 2021 10:10:47.118021965 CEST	53470	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:47.166822910 CEST	53	53470	8.8.8.8	192.168.2.3
May 10, 2021 10:10:49.494261980 CEST	56546	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:49.547791004 CEST	53	56546	8.8.8.8	192.168.2.3
May 10, 2021 10:10:51.130395889 CEST	53470	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:51.178997040 CEST	53	53470	8.8.8.8	192.168.2.3
May 10, 2021 10:10:52.776953936 CEST	56446	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:52.778426886 CEST	59631	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:52.781933069 CEST	55515	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:52.788147926 CEST	64547	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:52.829216003 CEST	53	59631	8.8.8.8	192.168.2.3
May 10, 2021 10:10:52.832382917 CEST	53	55515	8.8.8.8	192.168.2.3
May 10, 2021 10:10:53.022502899 CEST	53	56446	8.8.8.8	192.168.2.3
May 10, 2021 10:10:53.030716896 CEST	53	64547	8.8.8.8	192.168.2.3
May 10, 2021 10:10:53.499546051 CEST	56546	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:53.550986052 CEST	53	56546	8.8.8.8	192.168.2.3
May 10, 2021 10:10:53.597755909 CEST	51759	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:53.651134014 CEST	53	51759	8.8.8.8	192.168.2.3
May 10, 2021 10:10:58.494772911 CEST	59207	53	192.168.2.3	8.8.8.8
May 10, 2021 10:10:58.854151964 CEST	53	59207	8.8.8.8	192.168.2.3
May 10, 2021 10:11:06.241933107 CEST	54269	53	192.168.2.3	8.8.8.8
May 10, 2021 10:11:06.290740013 CEST	53	54269	8.8.8.8	192.168.2.3
May 10, 2021 10:11:10.872987032 CEST	54856	53	192.168.2.3	8.8.8.8
May 10, 2021 10:11:10.921495914 CEST	53	54856	8.8.8.8	192.168.2.3
May 10, 2021 10:11:11.761985064 CEST	64140	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2021 10:11:11.810688019 CEST	53	64140	8.8.8.8	192.168.2.3
May 10, 2021 10:11:12.762579918 CEST	62271	53	192.168.2.3	8.8.8.8
May 10, 2021 10:11:12.827199936 CEST	53	62271	8.8.8.8	192.168.2.3
May 10, 2021 10:11:12.827261925 CEST	57404	53	192.168.2.3	8.8.8.8
May 10, 2021 10:11:12.876971006 CEST	53	57404	8.8.8.8	192.168.2.3
May 10, 2021 10:11:15.728897095 CEST	62997	53	192.168.2.3	8.8.8.8
May 10, 2021 10:11:15.804438114 CEST	53	62997	8.8.8.8	192.168.2.3
May 10, 2021 10:11:28.474235058 CEST	57712	53	192.168.2.3	8.8.8.8
May 10, 2021 10:11:28.541677952 CEST	53	57712	8.8.8.8	192.168.2.3
May 10, 2021 10:11:28.983304977 CEST	60065	53	192.168.2.3	8.8.8.8
May 10, 2021 10:11:29.042402029 CEST	53	60065	8.8.8.8	192.168.2.3
May 10, 2021 10:11:29.398386002 CEST	55068	53	192.168.2.3	8.8.8.8
May 10, 2021 10:11:29.467797041 CEST	53	55068	8.8.8.8	192.168.2.3
May 10, 2021 10:11:29.941911936 CEST	64700	53	192.168.2.3	8.8.8.8
May 10, 2021 10:11:29.994971991 CEST	53	64700	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 10, 2021 10:10:13.155260086 CEST	192.168.2.3	8.8.8.8	0xe0bd	Standard query (0)	localcoronavirus.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:14.969357014 CEST	192.168.2.3	8.8.8.8	0x14bb	Standard query (0)	phantom-expansion.unidadeditorial.es	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.323745012 CEST	192.168.2.3	8.8.8.8	0x6d0d	Standard query (0)	cdn2.excelsior.com.mx	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.404093981 CEST	192.168.2.3	8.8.8.8	0x9	Standard query (0)	static4.abc.es	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.430960894 CEST	192.168.2.3	8.8.8.8	0xafa	Standard query (0)	www.lavozdegalicia.es	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.454746962 CEST	192.168.2.3	8.8.8.8	0xfec3	Standard query (0)	cronicaglobal.elespanol.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.513704062 CEST	192.168.2.3	8.8.8.8	0x3d75	Standard query (0)	www.republica.com.uy	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.520025015 CEST	192.168.2.3	8.8.8.8	0x4f44	Standard query (0)	imagenes.20minutos.es	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.535191059 CEST	192.168.2.3	8.8.8.8	0x7003	Standard query (0)	ep00.epimg.net	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.542586088 CEST	192.168.2.3	8.8.8.8	0x912b	Standard query (0)	d3cra5ec8gdi8w.cloudfront.net	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.553714037 CEST	192.168.2.3	8.8.8.8	0xa68d	Standard query (0)	i.blogs.es	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.565409899 CEST	192.168.2.3	8.8.8.8	0x5798	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.602931976 CEST	192.168.2.3	8.8.8.8	0x9693	Standard query (0)	as01.epimg.net	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.642855883 CEST	192.168.2.3	8.8.8.8	0x91f6	Standard query (0)	img.huffingtonpost.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.658587933 CEST	192.168.2.3	8.8.8.8	0xfee2	Standard query (0)	img2.rtve.es	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.658613920 CEST	192.168.2.3	8.8.8.8	0xf2	Standard query (0)	static.hotjar.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.660589933 CEST	192.168.2.3	8.8.8.8	0x9f26	Standard query (0)	www.puntodebreak.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.674156904 CEST	192.168.2.3	8.8.8.8	0x244a	Standard query (0)	phantom-elmundo.unidadeditorial.es	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.712335110 CEST	192.168.2.3	8.8.8.8	0x3370	Standard query (0)	static2.abc.es	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.719470978 CEST	192.168.2.3	8.8.8.8	0xf7ca	Standard query (0)	platform.twitter.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.719856977 CEST	192.168.2.3	8.8.8.8	0x742f	Standard query (0)	www.elconfidencialdigital.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.722882986 CEST	192.168.2.3	8.8.8.8	0x250f	Standard query (0)	s1.eestatic.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.977479935 CEST	192.168.2.3	8.8.8.8	0xa3d2	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)
May 10, 2021 10:10:16.344170094 CEST	192.168.2.3	8.8.8.8	0x8746	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 10, 2021 10:10:16.483540058 CEST	192.168.2.3	8.8.8.8	0xc13d	Standard query (0)	proteccion10.net	A (IP address)	IN (0x0001)
May 10, 2021 10:10:16.542710066 CEST	192.168.2.3	8.8.8.8	0x16d0	Standard query (0)	script.hotjar.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:17.495307922 CEST	192.168.2.3	8.8.8.8	0xe4c3	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
May 10, 2021 10:10:17.498796940 CEST	192.168.2.3	8.8.8.8	0x1d7c	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
May 10, 2021 10:10:17.541526079 CEST	192.168.2.3	8.8.8.8	0x81c0	Standard query (0)	adservice.google.ch	A (IP address)	IN (0x0001)
May 10, 2021 10:10:17.622539997 CEST	192.168.2.3	8.8.8.8	0xd2fe	Standard query (0)	www.googletagservices.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:17.626418114 CEST	192.168.2.3	8.8.8.8	0xa56a	Standard query (0)	vars.hotjar.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:21.884216070 CEST	192.168.2.3	8.8.8.8	0x7d2a	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
May 10, 2021 10:10:29.976681948 CEST	192.168.2.3	8.8.8.8	0xd722	Standard query (0)	cms.quantserve.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:29.980170012 CEST	192.168.2.3	8.8.8.8	0x58fe	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:29.983831882 CEST	192.168.2.3	8.8.8.8	0x6400	Standard query (0)	rtb.openx.net	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.015604973 CEST	192.168.2.3	8.8.8.8	0xd57a	Standard query (0)	image6.pubmatic.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.023507118 CEST	192.168.2.3	8.8.8.8	0x66c	Standard query (0)	pixel.rubiconproject.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.032566071 CEST	192.168.2.3	8.8.8.8	0x8f58	Standard query (0)	ssum-sec.casalemedia.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.060630083 CEST	192.168.2.3	8.8.8.8	0x652f	Standard query (0)	cc.adingo.jp	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.069701910 CEST	192.168.2.3	8.8.8.8	0x4de6	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.073438883 CEST	192.168.2.3	8.8.8.8	0xe0d3	Standard query (0)	pixel.everesttech.net	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.437156916 CEST	192.168.2.3	8.8.8.8	0x7f	Standard query (0)	d.agkn.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.965559959 CEST	192.168.2.3	8.8.8.8	0x14c	Standard query (0)	odr.mookie1.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:37.166699886 CEST	192.168.2.3	8.8.8.8	0x75c3	Standard query (0)	localcoronavirus.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:52.776953936 CEST	192.168.2.3	8.8.8.8	0x8480	Standard query (0)	beacon.walmart.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:52.778426886 CEST	192.168.2.3	8.8.8.8	0x296a	Standard query (0)	e.dlx.addthis.com	A (IP address)	IN (0x0001)
May 10, 2021 10:10:52.781933069 CEST	192.168.2.3	8.8.8.8	0xbb4e	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
May 10, 2021 10:10:52.788147926 CEST	192.168.2.3	8.8.8.8	0xce2e	Standard query (0)	ag.innovid.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:28.474235058 CEST	192.168.2.3	8.8.8.8	0x65c0	Standard query (0)	covid19tracking.narrativa.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:28.983304977 CEST	192.168.2.3	8.8.8.8	0x1d2b	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:29.398386002 CEST	192.168.2.3	8.8.8.8	0xf5fa	Standard query (0)	4i2g925ohj.execute-api.eu-west-3.amazonaws.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:29.941911936 CEST	192.168.2.3	8.8.8.8	0x354e	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:10:13.223541021 CEST	8.8.8.8	192.168.2.3	0xe0bd	No error (0)	localcoronavirus.com		172.67.183.244	A (IP address)	IN (0x0001)
May 10, 2021 10:10:13.223541021 CEST	8.8.8.8	192.168.2.3	0xe0bd	No error (0)	localcoronavirus.com		104.21.18.245	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.057516098 CEST	8.8.8.8	192.168.2.3	0x14bb	No error (0)	phantom-expansion.unidadeditorial.es	dbpabf0off7y1.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.057516098 CEST	8.8.8.8	192.168.2.3	0x14bb	No error (0)	dbpabf0off7y1.cloudfront.net		65.9.66.65	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:10:15.057516098 CEST	8.8.8.8	192.168.2.3	0x14bb	No error (0)	dbpabf0off7y1.cloudfront.net		65.9.66.100	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.057516098 CEST	8.8.8.8	192.168.2.3	0x14bb	No error (0)	dbpabf0off7y1.cloudfront.net		65.9.66.80	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.057516098 CEST	8.8.8.8	192.168.2.3	0x14bb	No error (0)	dbpabf0off7y1.cloudfront.net		65.9.66.34	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.383980989 CEST	8.8.8.8	192.168.2.3	0x6d0d	No error (0)	cdn2.excelsior.com.mx	d37ub18b7ivraq.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.383980989 CEST	8.8.8.8	192.168.2.3	0x6d0d	No error (0)	d37ub18b7ivraq.cloudfront.net		99.86.2.109	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.383980989 CEST	8.8.8.8	192.168.2.3	0x6d0d	No error (0)	d37ub18b7ivraq.cloudfront.net		99.86.2.114	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.383980989 CEST	8.8.8.8	192.168.2.3	0x6d0d	No error (0)	d37ub18b7ivraq.cloudfront.net		99.86.2.100	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.383980989 CEST	8.8.8.8	192.168.2.3	0x6d0d	No error (0)	d37ub18b7ivraq.cloudfront.net		99.86.2.5	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.465584040 CEST	8.8.8.8	192.168.2.3	0x9	No error (0)	static4.abc.es	static.abc.es		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.465584040 CEST	8.8.8.8	192.168.2.3	0x9	No error (0)	static.abc.es	static-abc.akamaized.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.493063927 CEST	8.8.8.8	192.168.2.3	0xafa	No error (0)	www.lavozdegalicia.es	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.493063927 CEST	8.8.8.8	192.168.2.3	0xafa	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		54.194.190.147	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.493063927 CEST	8.8.8.8	192.168.2.3	0xafa	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		54.194.71.119	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.493063927 CEST	8.8.8.8	192.168.2.3	0xafa	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		52.211.217.51	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.493063927 CEST	8.8.8.8	192.168.2.3	0xafa	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		52.210.129.255	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.493063927 CEST	8.8.8.8	192.168.2.3	0xafa	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		34.249.141.22	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.493063927 CEST	8.8.8.8	192.168.2.3	0xafa	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		52.211.67.210	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.548643112 CEST	8.8.8.8	192.168.2.3	0xfec3	No error (0)	cronicaglobal.elespanol.com	caching.elespanol.edge2befaster.io		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.548643112 CEST	8.8.8.8	192.168.2.3	0xfec3	No error (0)	caching.elespanol.edge2befaster.io	caching.meta-cluster-03.edge2befaster.io		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.548643112 CEST	8.8.8.8	192.168.2.3	0xfec3	No error (0)	caching.meta-cluster-03.edge2befaster.io	cec01.eug.edgetcdn.io		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.548643112 CEST	8.8.8.8	192.168.2.3	0xfec3	No error (0)	cec01.eug.edgetcdn.io		51.68.35.185	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.548643112 CEST	8.8.8.8	192.168.2.3	0xfec3	No error (0)	cec01.eug.edgetcdn.io		51.255.81.138	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:10:15.587017059 CEST	8.8.8.8	192.168.2.3	0x4f44	No error (0)	imagenes.20minutos.es	di7juyclzlgyp.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.587017059 CEST	8.8.8.8	192.168.2.3	0x4f44	No error (0)	di7juyclzlgyp.cloudfront.net		13.32.25.93	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.587017059 CEST	8.8.8.8	192.168.2.3	0x4f44	No error (0)	di7juyclzlgyp.cloudfront.net		13.32.25.102	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.587017059 CEST	8.8.8.8	192.168.2.3	0x4f44	No error (0)	di7juyclzlgyp.cloudfront.net		13.32.25.43	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.587017059 CEST	8.8.8.8	192.168.2.3	0x4f44	No error (0)	di7juyclzlgyp.cloudfront.net		13.32.25.126	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.594146967 CEST	8.8.8.8	192.168.2.3	0x7003	No error (0)	ep00.epimg.net	prisa-us-eu.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.594146967 CEST	8.8.8.8	192.168.2.3	0x7003	No error (0)	prisa-us-eu.map.fastly.net		199.232.194.133	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.594146967 CEST	8.8.8.8	192.168.2.3	0x7003	No error (0)	prisa-us-eu.map.fastly.net		199.232.198.133	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.616774082 CEST	8.8.8.8	192.168.2.3	0x912b	No error (0)	d3cra5ec8gdi8w.cloudfront.net		13.35.253.104	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.616774082 CEST	8.8.8.8	192.168.2.3	0x912b	No error (0)	d3cra5ec8gdi8w.cloudfront.net		13.35.253.186	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.616774082 CEST	8.8.8.8	192.168.2.3	0x912b	No error (0)	d3cra5ec8gdi8w.cloudfront.net		13.35.253.12	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.616774082 CEST	8.8.8.8	192.168.2.3	0x912b	No error (0)	d3cra5ec8gdi8w.cloudfront.net		13.35.253.176	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.616800070 CEST	8.8.8.8	192.168.2.3	0xa68d	No error (0)	i.blogs.es	d1j70itqjm2icu.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.616800070 CEST	8.8.8.8	192.168.2.3	0xa68d	No error (0)	d1j70itqjm2icu.cloudfront.net		13.32.25.35	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.616800070 CEST	8.8.8.8	192.168.2.3	0xa68d	No error (0)	d1j70itqjm2icu.cloudfront.net		13.32.25.109	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.616800070 CEST	8.8.8.8	192.168.2.3	0xa68d	No error (0)	d1j70itqjm2icu.cloudfront.net		13.32.25.9	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.616800070 CEST	8.8.8.8	192.168.2.3	0xa68d	No error (0)	d1j70itqjm2icu.cloudfront.net		13.32.25.47	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.624723911 CEST	8.8.8.8	192.168.2.3	0x5798	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.624723911 CEST	8.8.8.8	192.168.2.3	0x5798	No error (0)	scontent.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.663733959 CEST	8.8.8.8	192.168.2.3	0x9693	No error (0)	as01.epimg.net	prisa-us-eu.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.663733959 CEST	8.8.8.8	192.168.2.3	0x9693	No error (0)	prisa-us-eu.map.fastly.net		199.232.194.133	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.663733959 CEST	8.8.8.8	192.168.2.3	0x9693	No error (0)	prisa-us-eu.map.fastly.net		199.232.198.133	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.705456018 CEST	8.8.8.8	192.168.2.3	0x91f6	No error (0)	img.huffingtonpost.com	cs491300.wpc.mucdn.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.705456018 CEST	8.8.8.8	192.168.2.3	0x91f6	No error (0)	cs491300.wpc.mucdn.net		192.229.220.196	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.718332052 CEST	8.8.8.8	192.168.2.3	0x9f26	No error (0)	www.puntodebreak.com	puntodebreak.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.718332052 CEST	8.8.8.8	192.168.2.3	0x9f26	No error (0)	puntodebreak.com		185.125.78.79	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:10:15.722278118 CEST	8.8.8.8	192.168.2.3	0xfee2	No error (0)	img2.rtve.es	caching.c251.edge2befaster.io		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.722278118 CEST	8.8.8.8	192.168.2.3	0xfee2	No error (0)	caching.c251.edge2befaster.io	aec01.esg.rtve.edgetcdn.io		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.722278118 CEST	8.8.8.8	192.168.2.3	0xfee2	No error (0)	aec01.esg.rtve.edgetcdn.io		51.210.220.45	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.722278118 CEST	8.8.8.8	192.168.2.3	0xfee2	No error (0)	aec01.esg.rtve.edgetcdn.io		185.103.37.61	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.722278118 CEST	8.8.8.8	192.168.2.3	0xfee2	No error (0)	aec01.esg.rtve.edgetcdn.io		185.103.37.62	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.722278118 CEST	8.8.8.8	192.168.2.3	0xfee2	No error (0)	aec01.esg.rtve.edgetcdn.io		51.89.172.162	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.722278118 CEST	8.8.8.8	192.168.2.3	0xfee2	No error (0)	aec01.esg.rtve.edgetcdn.io		185.103.37.59	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.722278118 CEST	8.8.8.8	192.168.2.3	0xfee2	No error (0)	aec01.esg.rtve.edgetcdn.io		51.89.235.116	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.722278118 CEST	8.8.8.8	192.168.2.3	0xfee2	No error (0)	aec01.esg.rtve.edgetcdn.io		51.195.63.235	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.722278118 CEST	8.8.8.8	192.168.2.3	0xfee2	No error (0)	aec01.esg.rtve.edgetcdn.io		51.195.63.237	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.722278118 CEST	8.8.8.8	192.168.2.3	0xfee2	No error (0)	aec01.esg.rtve.edgetcdn.io		51.210.220.43	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.725678921 CEST	8.8.8.8	192.168.2.3	0xf2	No error (0)	static.hotjar.com	static-cdn.hotjar.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.725678921 CEST	8.8.8.8	192.168.2.3	0xf2	No error (0)	static-cdn.hotjar.com		13.32.25.105	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.725678921 CEST	8.8.8.8	192.168.2.3	0xf2	No error (0)	static-cdn.hotjar.com		13.32.25.2	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.725678921 CEST	8.8.8.8	192.168.2.3	0xf2	No error (0)	static-cdn.hotjar.com		13.32.25.20	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.725678921 CEST	8.8.8.8	192.168.2.3	0xf2	No error (0)	static-cdn.hotjar.com		13.32.25.35	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.733328104 CEST	8.8.8.8	192.168.2.3	0x3d75	No error (0)	www.republica.com.uy	republica.com.uy		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.733328104 CEST	8.8.8.8	192.168.2.3	0x3d75	No error (0)	republica.com.uy		108.170.35.187	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.734384060 CEST	8.8.8.8	192.168.2.3	0x244a	No error (0)	phantom-elmundo.unidadeditorial.es	dbpabf0off7y1.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.734384060 CEST	8.8.8.8	192.168.2.3	0x244a	No error (0)	dbpabf0off7y1.cloudfront.net		65.9.66.65	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.734384060 CEST	8.8.8.8	192.168.2.3	0x244a	No error (0)	dbpabf0off7y1.cloudfront.net		65.9.66.100	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.734384060 CEST	8.8.8.8	192.168.2.3	0x244a	No error (0)	dbpabf0off7y1.cloudfront.net		65.9.66.34	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.734384060 CEST	8.8.8.8	192.168.2.3	0x244a	No error (0)	dbpabf0off7y1.cloudfront.net		65.9.66.80	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.776252985 CEST	8.8.8.8	192.168.2.3	0x3370	No error (0)	static2.abc.es	static.abc.es		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.776252985 CEST	8.8.8.8	192.168.2.3	0x3370	No error (0)	static.abc.es	static-abc.akamaized.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.788624048 CEST	8.8.8.8	192.168.2.3	0x742f	No error (0)	www.elconfidencialdigital.com		104.25.56.34	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:10:15.788624048 CEST	8.8.8.8	192.168.2.3	0x742f	No error (0)	www.elconfidencialdigital.com		104.25.57.34	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.788624048 CEST	8.8.8.8	192.168.2.3	0x742f	No error (0)	www.elconfidencialdigital.com		172.67.82.88	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.797442913 CEST	8.8.8.8	192.168.2.3	0xf7ca	No error (0)	platform.twitter.com	cs472.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.797442913 CEST	8.8.8.8	192.168.2.3	0xf7ca	No error (0)	cs472.wac.edgecastcdn.net	cs1-apr-8315.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.797442913 CEST	8.8.8.8	192.168.2.3	0xf7ca	No error (0)	cs1-apr-8315.wac.edgecastcdn.net	wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.797442913 CEST	8.8.8.8	192.168.2.3	0xf7ca	No error (0)	cs1-lb-eu.8315.ecdns.net	cs491.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.797442913 CEST	8.8.8.8	192.168.2.3	0xf7ca	No error (0)	cs491.wac.edgecastcdn.net		192.229.233.25	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.801578999 CEST	8.8.8.8	192.168.2.3	0x250f	No error (0)	s1.eestatic.com	caching.elespanol.edge2befaster.io		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.801578999 CEST	8.8.8.8	192.168.2.3	0x250f	No error (0)	caching.elespanol.edge2befaster.io	caching.meta-cluster-03.edge2befaster.io		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.801578999 CEST	8.8.8.8	192.168.2.3	0x250f	No error (0)	caching.meta-cluster-03.edge2befaster.io	cec01.eug.edgetcdn.io		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:15.801578999 CEST	8.8.8.8	192.168.2.3	0x250f	No error (0)	cec01.eug.edgetcdn.io		51.68.35.185	A (IP address)	IN (0x0001)
May 10, 2021 10:10:15.801578999 CEST	8.8.8.8	192.168.2.3	0x250f	No error (0)	cec01.eug.edgetcdn.io		51.255.81.138	A (IP address)	IN (0x0001)
May 10, 2021 10:10:16.026253939 CEST	8.8.8.8	192.168.2.3	0xa3d2	No error (0)	cdn.jsdelivr.net	dualstack.f3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:16.410202980 CEST	8.8.8.8	192.168.2.3	0x8746	No error (0)	googleads.g.doubleclick.net		216.58.214.194	A (IP address)	IN (0x0001)
May 10, 2021 10:10:16.550755978 CEST	8.8.8.8	192.168.2.3	0xc13d	No error (0)	proteccion10.net		193.32.242.105	A (IP address)	IN (0x0001)
May 10, 2021 10:10:16.603355885 CEST	8.8.8.8	192.168.2.3	0x16d0	No error (0)	script.hotjar.com		13.32.25.86	A (IP address)	IN (0x0001)
May 10, 2021 10:10:16.603355885 CEST	8.8.8.8	192.168.2.3	0x16d0	No error (0)	script.hotjar.com		13.32.25.17	A (IP address)	IN (0x0001)
May 10, 2021 10:10:16.603355885 CEST	8.8.8.8	192.168.2.3	0x16d0	No error (0)	script.hotjar.com		13.32.25.19	A (IP address)	IN (0x0001)
May 10, 2021 10:10:16.603355885 CEST	8.8.8.8	192.168.2.3	0x16d0	No error (0)	script.hotjar.com		13.32.25.118	A (IP address)	IN (0x0001)
May 10, 2021 10:10:17.562201023 CEST	8.8.8.8	192.168.2.3	0x1d7c	No error (0)	www.google.ch		172.217.19.99	A (IP address)	IN (0x0001)
May 10, 2021 10:10:17.574480057 CEST	8.8.8.8	192.168.2.3	0xe4c3	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:17.574480057 CEST	8.8.8.8	192.168.2.3	0xe4c3	No error (0)	stats.l.doubleclick.net		74.125.140.154	A (IP address)	IN (0x0001)
May 10, 2021 10:10:17.574480057 CEST	8.8.8.8	192.168.2.3	0xe4c3	No error (0)	stats.l.doubleclick.net		74.125.140.157	A (IP address)	IN (0x0001)
May 10, 2021 10:10:17.574480057 CEST	8.8.8.8	192.168.2.3	0xe4c3	No error (0)	stats.l.doubleclick.net		74.125.140.156	A (IP address)	IN (0x0001)
May 10, 2021 10:10:17.574480057 CEST	8.8.8.8	192.168.2.3	0xe4c3	No error (0)	stats.l.doubleclick.net		74.125.140.155	A (IP address)	IN (0x0001)
May 10, 2021 10:10:17.577469110 CEST	8.8.8.8	192.168.2.3	0xa78f	No error (0)	partnerad.l.doubleclick.net		216.58.214.226	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:10:17.607004881 CEST	8.8.8.8	192.168.2.3	0x81c0	No error (0)	adservice.google.ch	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:17.607004881 CEST	8.8.8.8	192.168.2.3	0x81c0	No error (0)	pagead46.l.doubleclick.net		172.217.19.98	A (IP address)	IN (0x0001)
May 10, 2021 10:10:17.687529087 CEST	8.8.8.8	192.168.2.3	0xa56a	No error (0)	vars.hotjar.com		99.86.2.129	A (IP address)	IN (0x0001)
May 10, 2021 10:10:17.687529087 CEST	8.8.8.8	192.168.2.3	0xa56a	No error (0)	vars.hotjar.com		99.86.2.91	A (IP address)	IN (0x0001)
May 10, 2021 10:10:17.687529087 CEST	8.8.8.8	192.168.2.3	0xa56a	No error (0)	vars.hotjar.com		99.86.2.113	A (IP address)	IN (0x0001)
May 10, 2021 10:10:17.687529087 CEST	8.8.8.8	192.168.2.3	0xa56a	No error (0)	vars.hotjar.com		99.86.2.115	A (IP address)	IN (0x0001)
May 10, 2021 10:10:17.687551975 CEST	8.8.8.8	192.168.2.3	0xd2fe	No error (0)	www.googletagservices.com		216.58.214.226	A (IP address)	IN (0x0001)
May 10, 2021 10:10:21.941531897 CEST	8.8.8.8	192.168.2.3	0x7d2a	No error (0)	www.google.de		172.217.16.99	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.032537937 CEST	8.8.8.8	192.168.2.3	0x6400	No error (0)	rtb.openx.net		35.186.253.211	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.032537937 CEST	8.8.8.8	192.168.2.3	0x6400	No error (0)	rtb.openx.net		35.227.252.103	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.039772987 CEST	8.8.8.8	192.168.2.3	0x58fe	No error (0)	id.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.054897070 CEST	8.8.8.8	192.168.2.3	0xd722	No error (0)	cms.quantserve.com	2kpixel.quantserve.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:30.054897070 CEST	8.8.8.8	192.168.2.3	0xd722	No error (0)	2kpixel.quantserve.com	global.px.quantserve.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:30.054897070 CEST	8.8.8.8	192.168.2.3	0xd722	No error (0)	global.px.quantserve.com		91.228.74.189	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.054897070 CEST	8.8.8.8	192.168.2.3	0xd722	No error (0)	global.px.quantserve.com		91.228.74.134	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.054897070 CEST	8.8.8.8	192.168.2.3	0xd722	No error (0)	global.px.quantserve.com		91.228.74.226	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.054897070 CEST	8.8.8.8	192.168.2.3	0xd722	No error (0)	global.px.quantserve.com		91.228.74.198	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.054897070 CEST	8.8.8.8	192.168.2.3	0xd722	No error (0)	global.px.quantserve.com		91.228.74.133	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.064357042 CEST	8.8.8.8	192.168.2.3	0xd57a	No error (0)	image6.pubmatic.com	pugm22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:30.064357042 CEST	8.8.8.8	192.168.2.3	0xd57a	No error (0)	pugm22000nfc.pubmatic.com	pugm22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:30.064357042 CEST	8.8.8.8	192.168.2.3	0xd57a	No error (0)	pugm22000nf.pubmatic.com		185.64.189.115	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.099116087 CEST	8.8.8.8	192.168.2.3	0x8f58	No error (0)	ssum-sec.casalemedia.com	ssum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:30.099313974 CEST	8.8.8.8	192.168.2.3	0x66c	No error (0)	pixel.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:30.125963926 CEST	8.8.8.8	192.168.2.3	0x652f	No error (0)	cc.adingo.jp		54.64.53.220	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.125963926 CEST	8.8.8.8	192.168.2.3	0x652f	No error (0)	cc.adingo.jp		54.178.254.210	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.125963926 CEST	8.8.8.8	192.168.2.3	0x652f	No error (0)	cc.adingo.jp		54.250.196.226	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:10:30.125963926 CEST	8.8.8.8	192.168.2.3	0x652f	No error (0)	cc.adingo.jp		18.180.1.224	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.125963926 CEST	8.8.8.8	192.168.2.3	0x652f	No error (0)	cc.adingo.jp		52.69.69.122	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.125963926 CEST	8.8.8.8	192.168.2.3	0x652f	No error (0)	cc.adingo.jp		52.68.53.67	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.125963926 CEST	8.8.8.8	192.168.2.3	0x652f	No error (0)	cc.adingo.jp		54.178.184.38	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.125963926 CEST	8.8.8.8	192.168.2.3	0x652f	No error (0)	cc.adingo.jp		18.179.240.58	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.135770082 CEST	8.8.8.8	192.168.2.3	0x4de6	No error (0)	cm.g.doubleclick.net		172.217.16.98	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.149425983 CEST	8.8.8.8	192.168.2.3	0xe0d3	No error (0)	pixel.everesttech.net	tp00.everesttech.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:30.485790968 CEST	8.8.8.8	192.168.2.3	0x7f	No error (0)	d.agkn.com	data.agkn.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:30.485790968 CEST	8.8.8.8	192.168.2.3	0x7f	No error (0)	data.agkn.com	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:30.485790968 CEST	8.8.8.8	192.168.2.3	0x7f	No error (0)	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		52.29.48.214	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.485790968 CEST	8.8.8.8	192.168.2.3	0x7f	No error (0)	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		18.195.77.77	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.485790968 CEST	8.8.8.8	192.168.2.3	0x7f	No error (0)	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		18.194.113.221	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.485790968 CEST	8.8.8.8	192.168.2.3	0x7f	No error (0)	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		18.196.98.222	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.485790968 CEST	8.8.8.8	192.168.2.3	0x7f	No error (0)	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		52.28.108.245	A (IP address)	IN (0x0001)
May 10, 2021 10:10:30.485790968 CEST	8.8.8.8	192.168.2.3	0x7f	No error (0)	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		18.195.194.125	A (IP address)	IN (0x0001)
May 10, 2021 10:10:31.014225960 CEST	8.8.8.8	192.168.2.3	0x14c	No error (0)	odr.mookie1.com	tagr-gcp-odr-euw4.mookie1.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:31.014225960 CEST	8.8.8.8	192.168.2.3	0x14c	No error (0)	tagr-gcp-odr-euw4.mookie1.com		34.98.67.61	A (IP address)	IN (0x0001)
May 10, 2021 10:10:37.229310989 CEST	8.8.8.8	192.168.2.3	0x75c3	No error (0)	localcoronavirus.com		172.67.183.244	A (IP address)	IN (0x0001)
May 10, 2021 10:10:37.229310989 CEST	8.8.8.8	192.168.2.3	0x75c3	No error (0)	localcoronavirus.com		104.21.18.245	A (IP address)	IN (0x0001)
May 10, 2021 10:10:52.829216003 CEST	8.8.8.8	192.168.2.3	0x296a	No error (0)	e.dlx.addthis.com	gtm08.nexac.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:10:52.829216003 CEST	8.8.8.8	192.168.2.3	0x296a	No error (0)	gtm08.nexac.com	a7cb1ba23276f4b358d8fca4e8cdf9ab-1165437553.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:52.829216003 CEST	8.8.8.8	192.168.2.3	0x296a	No error (0)	a7cb1ba23276f4b358d8fca4e8cdf9ab-1165437553.us-east-1.elb.amazonaws.com		184.73.211.96	A (IP address)	IN (0x0001)
May 10, 2021 10:10:52.829216003 CEST	8.8.8.8	192.168.2.3	0x296a	No error (0)	a7cb1ba23276f4b358d8fca4e8cdf9ab-1165437553.us-east-1.elb.amazonaws.com		107.23.233.216	A (IP address)	IN (0x0001)
May 10, 2021 10:10:52.832382917 CEST	8.8.8.8	192.168.2.3	0xbb4e	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
May 10, 2021 10:10:52.832382917 CEST	8.8.8.8	192.168.2.3	0xbb4e	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
May 10, 2021 10:10:53.022502899 CEST	8.8.8.8	192.168.2.3	0x8480	No error (0)	beacon.walmart.com	beacon-cdn-custom.walmart.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:53.030716896 CEST	8.8.8.8	192.168.2.3	0xce2e	No error (0)	ag.innovid.com	ag-5-split.ag.innovid.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:53.030716896 CEST	8.8.8.8	192.168.2.3	0xce2e	No error (0)	aragorn-uk-prod.inbake.com	aragornapp-v2-prod-uk-lbj.inbake.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:10:53.030716896 CEST	8.8.8.8	192.168.2.3	0xce2e	No error (0)	aragornapp-v2-prod-uk-lbj.inbake.com		18.135.148.201	A (IP address)	IN (0x0001)
May 10, 2021 10:10:53.030716896 CEST	8.8.8.8	192.168.2.3	0xce2e	No error (0)	aragornapp-v2-prod-uk-lbj.inbake.com		3.8.240.220	A (IP address)	IN (0x0001)
May 10, 2021 10:10:53.030716896 CEST	8.8.8.8	192.168.2.3	0xce2e	No error (0)	aragornapp-v2-prod-uk-lbj.inbake.com		52.56.157.170	A (IP address)	IN (0x0001)
May 10, 2021 10:11:12.827199936 CEST	8.8.8.8	192.168.2.3	0x3662	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:28.541677952 CEST	8.8.8.8	192.168.2.3	0x65c0	No error (0)	covid19tracking.narrativa.com	d2jcax5o6gwtn6.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:28.541677952 CEST	8.8.8.8	192.168.2.3	0x65c0	No error (0)	d2jcax5o6gwtn6.cloudfront.net		13.32.25.3	A (IP address)	IN (0x0001)
May 10, 2021 10:11:28.541677952 CEST	8.8.8.8	192.168.2.3	0x65c0	No error (0)	d2jcax5o6gwtn6.cloudfront.net		13.32.25.81	A (IP address)	IN (0x0001)
May 10, 2021 10:11:28.541677952 CEST	8.8.8.8	192.168.2.3	0x65c0	No error (0)	d2jcax5o6gwtn6.cloudfront.net		13.32.25.54	A (IP address)	IN (0x0001)
May 10, 2021 10:11:28.541677952 CEST	8.8.8.8	192.168.2.3	0x65c0	No error (0)	d2jcax5o6gwtn6.cloudfront.net		13.32.25.68	A (IP address)	IN (0x0001)
May 10, 2021 10:11:29.042402029 CEST	8.8.8.8	192.168.2.3	0x1d2b	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:29.467797041 CEST	8.8.8.8	192.168.2.3	0xf5fa	No error (0)	4i2g925ohj.execute-api.eu-west-3.amazonaws.com		65.9.66.121	A (IP address)	IN (0x0001)
May 10, 2021 10:11:29.467797041 CEST	8.8.8.8	192.168.2.3	0xf5fa	No error (0)	4i2g925ohj.execute-api.eu-west-3.amazonaws.com		65.9.66.68	A (IP address)	IN (0x0001)
May 10, 2021 10:11:29.467797041 CEST	8.8.8.8	192.168.2.3	0xf5fa	No error (0)	4i2g925ohj.execute-api.eu-west-3.amazonaws.com		65.9.66.127	A (IP address)	IN (0x0001)
May 10, 2021 10:11:29.467797041 CEST	8.8.8.8	192.168.2.3	0xf5fa	No error (0)	4i2g925ohj.execute-api.eu-west-3.amazonaws.com		65.9.66.103	A (IP address)	IN (0x0001)
May 10, 2021 10:11:29.994971991 CEST	8.8.8.8	192.168.2.3	0x354e	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- localcoronavirus.com
- www.puntodebreak.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49714	172.67.183.244	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 10, 2021 10:10:13.287583113 CEST	1052	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: localcoronavirus.com Connection: Keep-Alive
May 10, 2021 10:10:13.342283964 CEST	1053	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 10 May 2021 08:10:13 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Mon, 10 May 2021 09:10:13 GMT Location: https://localcoronavirus.com/ cf-request-id: 09f6ecb3c500002fa505238000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=a%2FREAcqTSC0p78nKkNCt9lmw9EXU7tQIwp4gYNHkfiEoYiwYh2G44K6ZWAgj4%2BU%2BU6Wz3HEC7r8P2d3EbZQgiDguCLbmWjK4KdowF9hT5s6N%2FvbUog%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Vary: Accept-Encoding Server: cloudflare CF-RAY: 64d1b0993c982fa5-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49769	185.125.78.79	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 10, 2021 10:10:16.416304111 CEST	5195	OUT	GET /files/alexander-zverev-conclusiones-mutua-madrid-open-2021.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.puntodebreak.com

Timestamp	kBytes transferred	Direction	Data
May 10, 2021 10:10:16.484019041 CEST	5225	IN	HTTP/1.1 200 OK Connection: Keep-Alive Cache-Control: public, max-age=604800 Expires: Mon, 17 May 2021 08:10:16 GMT Content-Type: image/png Last-Modified: Sun, 09 May 2021 08:35:54 GMT Accept-Ranges: bytes Content-Length: 261128 Date: Mon, 10 May 2021 08:10:16 GMT Server: LiteSpeed Access-Control-Allow-Origin: * Access-Control-Allow-Headers: origin, x-requested-with, content-type Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 c1 00 00 01 1a 08 02 00 00 00 e6 20 7b 53 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 0e c3 00 00 0e c3 01 c7 6f a8 64 00 00 ff a5 49 44 41 54 78 5e ec fd 87 97 24 cb 75 de 8b 62 91 38 e3 7a da 7b ef bd f7 de 7b 6f a6 bb a7 a7 bd 77 e5 bd f7 ae bd ef 1e ef e7 f8 03 ef 41 18 92 20 29 01 24 45 8a 94 44 91 a2 ae a4 ab cb 27 dd f7 96 de ba ef 3f 78 df 8e a8 ee e9 39 e7 00 04 49 00 3c a0 b0 d7 37 39 91 51 59 59 d9 55 59 bf fa 76 44 64 e4 e7 7e eb 9f 29 7e fb b7 7f fb a2 f0 b1 f2 c7 e2 f2 43 97 cb ff 52 e3 f3 9f ff bc b7 c4 02 ab 17 35 ac f4 e6 a3 4c 17 c1 b6 a5 f8 d8 ea 95 ab 57 6e dc f4 09 0c 0a 89 8c 8e 4d 48 49 cf ca 2b 2a 2a ab aa 6e 68 6e e9 ec ed bb 35 36 3a 31 3f b9 20 58 58 97 af ca b4 22 b5 49 66 b0 ab ac 6e 85 d5 2d b7 ba 45 46 c7 9a d6 b2 a4 34 cc 08 95 63 cb e2 c1 e9 95 ce d1 99 86 be db 65 6d fd b9 b5 2d 69 25 55 71 59 05 91 89 69 81 91 d1 d8 fb 35 9f 9b 57 11 6f 5d 79 8b 85 f7 b5 59 f0 e3 b9 1c 1f ab ff 19 db 7c 6a 78 b7 78 73 9b 4f d6 fc 8c e0 5b f2 a7 20 3e 56 e6 f1 b1 f2 a7 c6 27 1f e2 db ff 42 e2 f2 0e 7f f6 9e f9 96 08 ef fa 2f 33 ae 5c b9 72 ed da b5 9b 37 6f 06 07 07 47 47 47 a7 a4 a4 e4 e4 e6 96 55 54 34 34 36 77 76 f7 de 1a 9b 98 5c 58 5a 10 8a d7 95 6a 89 ce a0 34 5b 75 0e a7 c1 ed 31 7a 36 8d 9e 1d 13 69 d3 e8 de d0 bb 3c 5a 87 4b 65 b5 4b 0d 16 a1 c6 24 50 eb d6 94 9a 35 a5 1a c b 15 b9 7a 49 aa 5c 94 28 a0 65 89 72 45 aa 5a 66 ab 73 12 d9 bc 44 b6 20 95 2d ca e4 10 15 c4 d2 45 89 6c 49 2a 5f 91 2b 21 14 e6 65 b4 c1 92 8c 6a 96 65 d8 03 6d b3 24 91 2d 63 1b 99 02 1b 2c 88 a5 0b 62 2c e5 6c ff b4 3a 2f 16 cf 8b 25 f 3 12 da 15 b4 20 91 cd 8a c4 73 62 f1 82 44 b2 28 95 2e 4a 65 d8 66 56 28 86 e6 44 e2 05 91 64 01 4b 81 68 6e 4d 38 b7 2e 9c 17 8a 7f 15 0c f5 7e b6 8c 80 de d2 af 43 f0 d3 c5 bb 72 e9 d4 f4 ae ff 94 f8 e4 36 bc 06 ec 7b 23 50 7f 69 9f 97 e3 63 f4 41 5c d4 30 34 bd f1 30 ca a4 bf 2f 70 c6 fb f8 fa 86 84 86 c7 c4 25 a6 64 64 e7 15 96 95 55 d6 d5 35 b7 b5 f7 0c f4 0f df 19 9d 5c 98 5a 14 2c 08 bc 0c 95 1b 89 a1 4a eb 86 c2 ba 21 31 b9 04 3a 2b 31 54 ac 1a 5b 96 0c ce ac 76 dd 9e 6d 1a b8 53 d9 31 58 50 df 96 59 56 93 9c 5b 1c 9b 9e 19 16 97 10 10 16 e6 e3 ef 7f dd e7 c6 75 bc 18 0b e2 e9 d5 ab f8 be 21 70 0c de 23 66 f1 fa 6d 39 7f af 2e 97 2f 82 57 fe b4 f8 79 b6 f9 69 71 f1 dc 8b c2 a7 c6 e5 87 2e ca ec 19 af e3 53 6b fe e9 e1 dd 17 8b 8b 1a 5e f8 69 71 79 e3 5f 6a 7c 92 a1 b9 60 68 39 31 b4 ab a7 7f 78 6c 62 7a 61 79 51 20 5e 57 a8 a4 3a 83 ca 62 7b 83 a1 ee 6d a3 7b 13 18 05 43 35 76 a7 c2 6c 93 e8 cd 42 8d 71 5d a5 65 00 25 ad 2a d4 cb 32 15 30 8a e5 8a 4c bd 2a 53 2f 4b 55 1c 79 1f 23 26 00 87 25 58 b9 4a cf 52 a1 72 51 2a e7 00 05 c1 21 70 13 f4 e4 00 bd a0 2a 67 28 db 3f c3 2e 61 51 02 d4 2e 4b e4 a0 ed a2 48 Data Ascii: PNGIHDR {SsRGBgAMAapHYsodIDATx^$ub8z{{owA)$ED'?x9I<79QYYUYvDd~)~CR5LWnMHI+**nhn56:1?XX"Ifn-EF4cem-i%UqYi5Wo]yY|jxxsO[>V'B/3\r7oGGGUT446wv\XZj4[u1z6i<ZKeK$P5zI\(erEZfsD -EII*_+!ejem$-c,b,I:/%sbD(.JefV(DdKhnM8.~Cr6{#PicA\040/p%ddU5\Z,J!1:+1T[vmS1XPYV[u!p#fm9./Wyiq.Sk^iqy_j|`h91xlbzayQ ^W:b{m{C5vlBq]e%*20L*S/KUy#&%XJRrQ*!p*g(?.aQ.KH

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
May 10, 2021 10:10:13.518646002 CEST	172.67.183.244	443	192.168.2.3	49716	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	Mon Oct 26 01:00:00 CET 2020 Mon Jan 27 13:48:08 CET 2020	Tue Oct 26 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		
May 10, 2021 10:10:15.197468996 CEST	65.9.66.65	443	192.168.2.3	49725	CN=*.unidadeditorial.es CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Jun 19 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jul 19 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 10, 2021 10:10:15.197669983 CEST	65.9.66.65	443	192.168.2.3	49726	CN=*.unidadeditorial.es CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Jun 19 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jul 19 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 10, 2021 10:10:15.488854885 CEST	99.86.2.109	443	192.168.2.3	49727	CN=excelsior.com.mx CN=excelsior.com.mx CN=R3, O=Let's Encrypt, C=US	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.	Sat Apr 24 15:00:02 CEST 2021 Sat Apr 24 15:00:02 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jul 23 15:00:02 CEST 2021 Fri Jul 23 15:00:02 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=excelsior.com.mx	CN=R3, O=Let's Encrypt, C=US	Sat Apr 24 15:00:02 CEST 2021	Fri Jul 23 15:00:02 CEST 2021		
					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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:10:15.490546942 CEST	99.86.2.109	443	192.168.2.3	49728	CN=excelsior.com.mx CN=excelsior.com.mx CN=R3, O=Let's Encrypt, C=US	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.	Sat Apr 24 15:00:02 CEST 2021 Sat Apr 24 15:00:02 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jul 23 15:00:02 CEST 2021 Fri Jul 23 15:00:02 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=excelsior.com.mx	CN=R3, O=Let's Encrypt, C=US	Sat Apr 24 15:00:02 CEST 2021	Fri Jul 23 15:00:02 CEST 2021		
					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		
May 10, 2021 10:10:15.667494059 CEST	54.194.190.147	443	192.168.2.3	49732	CN=*.lavozdegalicia.es, OU=PremiumSSL Legacy Wildcard, O=LA VOZ DE GALICIA S.A., STREET="RONDA DE OUTEIRO, 1 - 3 BAJO", L=A CORUNA, ST=La Corua, OID.2.5.4.17=15006, C=ES CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Thu Oct 17 02:00:00 CEST 2019 Fri Nov 02 01:00:00 CET 2018	Tue Jan 18 01:00:00 CET 2022 Wed Jan 01 00:59:59 CET 2031	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=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
May 10, 2021 10:10:15.698672056 CEST	51.68.35.185	443	192.168.2.3	49734	CN=cronicaglobal.elespanol.com 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.	Sun Mar 28 11:00:43 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Sat Jun 26 11:00:43 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		
May 10, 2021 10:10:15.698734045 CEST	51.68.35.185	443	192.168.2.3	49733	CN=cronicaglobal.elespanol.com 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.	Sun Mar 28 11:00:43 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Sat Jun 26 11:00:43 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:10:15.704582930 CEST	54.194.190.147	443	192.168.2.3	49731	CN=*.lavozdegalicia.es, OU=PremiumSSL Legacy Wildcard, O=LA VOZ DE GALICIA S.A., STREET="RONDA DE OUTEIRO, 1 - 3 BAJO", L=A CORUNA, ST=La Corua, OID.2.5.4.17=15006, C=ES CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Thu Oct 17 02:00:00 CEST 2019 Fri Nov 02 01:00:00 CET 2018	Tue Jan 18 01:00:00 CET 2022 Wed Jan 01 00:59:59 CET 2031	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=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
May 10, 2021 10:10:15.714168072 CEST	13.32.25.93	443	192.168.2.3	49738	CN=*.20minutos.es CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Apr 05 02:00:00 CEST 2021 Mon Nov 06 13:23:52 CET 2017	Mon Apr 25 01:59:59 CEST 2022 Sat Nov 06 13:23:52 CET 2027	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=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:52 CET 2017	Sat Nov 06 13:23:52 CET 2027		
May 10, 2021 10:10:15.714521885 CEST	13.32.25.93	443	192.168.2.3	49737	CN=*.20minutos.es CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Apr 05 02:00:00 CEST 2021 Mon Nov 06 13:23:52 CET 2017	Mon Apr 25 01:59:59 CEST 2022 Sat Nov 06 13:23:52 CET 2027	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=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:52 CET 2017	Sat Nov 06 13:23:52 CET 2027		
May 10, 2021 10:10:15.716280937 CEST	199.232.194.133	443	192.168.2.3	49735	CN=*.epimg.net 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.	Mon May 03 13:44:46 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Sun Aug 01 13:44:46 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		
May 10, 2021 10:10:15.719518900 CEST	199.232.194.133	443	192.168.2.3	49736	CN=*.epimg.net 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.	Mon May 03 13:44:46 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Sun Aug 01 13:44:46 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:10:15.744858027 CEST	13.32.25.35	443	192.168.2.3	49740	CN=*.blogs.es CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Feb 05 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Mar 07 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 10, 2021 10:10:15.778208971 CEST	13.32.25.35	443	192.168.2.3	49739	CN=*.blogs.es CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Feb 05 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Mar 07 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:10:15.781671047 CEST	31.13.92.14	443	192.168.2.3	49743	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Apr 06 02:00:00 CEST 2021	Sun Jul 04 01:59:59 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
							Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 10, 2021 10:10:15.783023119 CEST	13.35.253.104	443	192.168.2.3	49744	CN=*.cloudfront.net CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Feb 22 01:00:00 CET 2021	Tue Feb 22 00:59:59 CET 2022	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
							Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
							Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
					CN=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
May 10, 2021 10:10:15.818428993 CEST	31.13.92.14	443	192.168.2.3	49741	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Apr 06 02:00:00 CEST 2021	Sun Jul 04 01:59:59 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
							Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 10, 2021 10:10:15.820354939 CEST	13.35.253.104	443	192.168.2.3	49742	CN=*.cloudfront.net CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Feb 22 01:00:00 CET 2021	Tue Feb 22 00:59:59 CET 2022	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
							Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
							Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
					CN=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
May 10, 2021 10:10:15.821768045 CEST	199.232.194.133	443	192.168.2.3	49746	CN=*.epimg.net 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.	Mon May 03 13:44:46 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Sun Aug 01 13:44:46 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		
May 10, 2021 10:10:15.822391033 CEST	199.232.194.133	443	192.168.2.3	49745	CN=*.epimg.net 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.	Mon May 03 13:44:46 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Sun Aug 01 13:44:46 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		
May 10, 2021 10:10:15.848443031 CEST	192.229.220.196	443	192.168.2.3	49748	CN=img.huffingtonpost.com, O="Verizon Digital Media Services, Inc.", L=Los Angeles, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon May 04 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Wed Jun 08 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 10, 2021 10:10:15.864749908 CEST	192.229.220.196	443	192.168.2.3	49747	CN=img.huffingtonpost.com, O="Verizon Digital Media Services, Inc.", L=Los Angeles, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon May 04 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Wed Jun 08 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 10, 2021 10:10:15.868005991 CEST	13.32.25.105	443	192.168.2.3	49752	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 10, 2021 10:10:15.870609999 CEST	13.32.25.105	443	192.168.2.3	49751	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:10:15.878607988 CEST	65.9.66.65	443	192.168.2.3	49754	CN=*.unidadeditorial.es CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Jun 19 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jul 19 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 10, 2021 10:10:15.935400009 CEST	65.9.66.65	443	192.168.2.3	49753	CN=*.unidadeditorial.es CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Jun 19 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jul 19 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:10:15.944212914 CEST	51.210.220.45	443	192.168.2.3	49749	CN=*.rtve.es, O=Corporacion de Radio y Television Espanola SA SME, OU=Digital, L=Madrid, ST=Madrid, C=ES CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Thu Feb 20 15:36:50 CET 2020 Wed Nov 21 01:00:00 CET 2018	Sun Apr 17 10:58:42 CEST 2022 Tue Nov 21 01:00:00 CET 2028	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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
May 10, 2021 10:10:15.949856043 CEST	51.210.220.45	443	192.168.2.3	49750	CN=*.rtve.es, O=Corporacion de Radio y Television Espanola SA SME, OU=Digital, L=Madrid, ST=Madrid, C=ES CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Thu Feb 20 15:36:50 CET 2020 Wed Nov 21 01:00:00 CET 2018	Sun Apr 17 10:58:42 CEST 2022 Tue Nov 21 01:00:00 CET 2028	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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
May 10, 2021 10:10:16.005702972 CEST	185.125.78.79	443	192.168.2.3	49756	CN=puntodebreak.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun May 02 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Aug 01 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 10, 2021 10:10:16.023221016 CEST	185.125.78.79	443	192.168.2.3	49755	CN=puntodebreak.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun May 02 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Aug 01 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:10:16.035535097 CEST	104.25.56.34	443	192.168.2.3	49763	CN=elconfidencialdigital.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	Thu Jul 30 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Jul 30 14:00:00 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		
May 10, 2021 10:10:16.035784960 CEST	192.229.233.25	443	192.168.2.3	49765	CN=*.twimg.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 05 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Wed Nov 10 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	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=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 10, 2021 10:10:16.041541100 CEST	104.25.56.34	443	192.168.2.3	49764	CN=elconfidencialdigital.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	Thu Jul 30 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Jul 30 14:00:00 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		
May 10, 2021 10:10:16.043505907 CEST	192.229.233.25	443	192.168.2.3	49766	CN=*.twimg.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 05 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Wed Nov 10 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	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=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 10, 2021 10:10:16.043550968 CEST	51.68.35.185	443	192.168.2.3	49762	CN=*.elespanol.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Nov 18 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Sun Dec 19 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 10, 2021 10:10:16.044823885 CEST	51.68.35.185	443	192.168.2.3	49761	CN=*.elespanol.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Nov 18 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Sun Dec 19 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 10, 2021 10:10:16.265893936 CEST	108.170.35.187	443	192.168.2.3	49757	CN=republica.com.uy CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Mar 29 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Jun 28 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:10:16.276505947 CEST	108.170.35.187	443	192.168.2.3	49758	CN=republica.com.uy CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Mar 29 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Jun 28 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 10, 2021 10:10:16.550328016 CEST	216.58.214.194	443	192.168.2.3	49770	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 Apr 13 12:11:12 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:11:11 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		
May 10, 2021 10:10:16.552556992 CEST	216.58.214.194	443	192.168.2.3	49771	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 Apr 13 12:11:12 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:11:11 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		
May 10, 2021 10:10:16.702656031 CEST	13.32.25.86	443	192.168.2.3	49781	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 10, 2021 10:10:16.702934027 CEST	13.32.25.86	443	192.168.2.3	49780	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 10, 2021 10:10:16.758529902 CEST	193.32.242.105	443	192.168.2.3	49778	CN=proteccion10.net 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 Mar 24 02:05:17 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 22 03:05:17 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		
May 10, 2021 10:10:16.763375998 CEST	193.32.242.105	443	192.168.2.3	49779	CN=proteccion10.net 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 Mar 24 02:05:17 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 22 03:05:17 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:10:17.683732033 CEST	74.125.140.154	443	192.168.2.3	49788	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 Apr 13 12:11:12 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:11:11 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		
May 10, 2021 10:10:17.683830023 CEST	74.125.140.154	443	192.168.2.3	49787	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 Apr 13 12:11:12 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:11:11 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		
May 10, 2021 10:10:17.691665888 CEST	172.217.19.99	443	192.168.2.3	49785	CN=*.google.ch, 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 Apr 13 12:18:39 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:18:38 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		
May 10, 2021 10:10:17.691797018 CEST	172.217.19.99	443	192.168.2.3	49786	CN=*.google.ch, 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 Apr 13 12:18:39 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:18:38 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		
May 10, 2021 10:10:17.705712080 CEST	216.58.214.226	443	192.168.2.3	49789	CN=*.googleadservices.com, 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 Apr 13 12:15:09 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:15:08 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:10:17.709002018 CEST	216.58.214.226	443	192.168.2.3	49790	CN=*.googleadservices.com, 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 Apr 13 12:15:09 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:15:08 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		
May 10, 2021 10:10:17.776906967 CEST	99.86.2.129	443	192.168.2.3	49795	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 10, 2021 10:10:17.781625986 CEST	99.86.2.129	443	192.168.2.3	49797	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 10, 2021 10:10:17.823359013 CEST	216.58.214.226	443	192.168.2.3	49796	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 Apr 13 12:11:12 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:11:11 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		
May 10, 2021 10:10:17.824928999 CEST	216.58.214.226	443	192.168.2.3	49798	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 Apr 13 12:11:12 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:11:11 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		
May 10, 2021 10:10:30.374216080 CEST	185.64.189.115	443	192.168.2.3	49816	CN=*.pubmatic.com, O="PubMatic, Inc.", L=Redwood City, ST=California, C=US CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Dec 07 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri May 12 20:46:00 CEST 2000	Wed Dec 15 00:59:59 CET 2021 Mon May 12 01:59:59 CEST 2025 Tue May 13 01:59:00 CEST 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=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Sep 24 02:00:00 CEST 2020	Mon May 12 01:59:59 CEST 2025		
					CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri May 12 20:46:00 CEST 2000	Tue May 13 01:59:00 CEST 2025		
May 10, 2021 10:10:30.375473022 CEST	91.228.74.189	443	192.168.2.3	49813	CN=*.quantserve.com, O=Quantcast Corporation, L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 02 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Thu Oct 07 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:10:30.425828934 CEST	185.64.189.115	443	192.168.2.3	49815	CN=*.pubmatic.com, O="PubMatic, Inc.", L=Redwood City, ST=California, C=US CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Dec 07 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri May 12 20:46:00 CEST 2000	Wed Dec 15 00:59:59 CET 2021 Mon May 12 01:59:59 CEST 2025 Tue May 13 01:59:00 CEST 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=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Sep 24 02:00:00 CEST 2020	Mon May 12 01:59:59 CEST 2025		
					CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri May 12 20:46:00 CEST 2000	Tue May 13 01:59:00 CEST 2025		
May 10, 2021 10:10:30.436244011 CEST	35.186.253.211	443	192.168.2.3	49810	CN=*.openx.net, O=OpenX Technologies inc., L=Pasadena, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jun 18 02:00:00 CEST 2020 Mon Nov 06 13:23:45 CET 2017 Fri Nov 10 01:00:00 CET 2006	Tue Aug 17 14:00:00 CEST 2021 Sat Nov 06 13:23:45 CET 2027 Mon Nov 10 01:00:00 CET 2031	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=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 10, 2021 10:10:30.439369917 CEST	35.186.253.211	443	192.168.2.3	49809	CN=*.openx.net, O=OpenX Technologies inc., L=Pasadena, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jun 18 02:00:00 CEST 2020 Mon Nov 06 13:23:45 CET 2017 Fri Nov 10 01:00:00 CET 2006	Tue Aug 17 14:00:00 CEST 2021 Sat Nov 06 13:23:45 CET 2027 Mon Nov 10 01:00:00 CET 2031	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=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:10:30.440596104 CEST	35.244.174.68	443	192.168.2.3	49811	CN=*.rlcdn.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Feb 25 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Tue Mar 29 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 10, 2021 10:10:30.440606117 CEST	91.228.74.189	443	192.168.2.3	49814	CN=*.quantserve.com, O=Quantcast Corporation, L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 02 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Thu Oct 07 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 10, 2021 10:10:30.466553926 CEST	172.217.16.98	443	192.168.2.3	49823	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 Apr 13 12:11:12 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:11:11 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		
May 10, 2021 10:10:30.466598988 CEST	172.217.16.98	443	192.168.2.3	49821	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 Apr 13 12:11:12 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:11:11 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:10:30.468331099 CEST	35.244.174.68	443	192.168.2.3	49812	CN=*.rlcdn.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Feb 25 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Tue Mar 29 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 10, 2021 10:10:30.574637890 CEST	52.29.48.214	443	192.168.2.3	49828	CN=*.agkn.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Jul 25 02:00:00 CEST 2020 Mon Nov 06 13:23:33 CET 2017 Fri Nov 10 01:00:00 CET 2006	Sun Sep 18 14:00:00 CEST 2022 Sat Nov 06 13:23:33 CET 2027 Mon Nov 10 01:00:00 CET 2031	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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 10, 2021 10:10:30.588778973 CEST	52.29.48.214	443	192.168.2.3	49827	CN=*.agkn.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Jul 25 02:00:00 CEST 2020 Mon Nov 06 13:23:33 CET 2017 Fri Nov 10 01:00:00 CET 2006	Sun Sep 18 14:00:00 CEST 2022 Sat Nov 06 13:23:33 CET 2027 Mon Nov 10 01:00:00 CET 2031	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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 10, 2021 10:10:30.994359970 CEST	54.64.53.220	443	192.168.2.3	49822	CN=*.adingo.jp, O="fluct,Inc.", L=Shibuya-ku, ST=Tokyo, C=JP CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 26 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Fri Apr 15 01:59:59 CEST 2022 Tue Sep 24 01:59:59 CEST 2030	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=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 10, 2021 10:10:31.003604889 CEST	54.64.53.220	443	192.168.2.3	49824	CN=*.adingo.jp, O="fluct,Inc.", L=Shibuya-ku, ST=Tokyo, C=JP CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 26 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Fri Apr 15 01:59:59 CEST 2022 Tue Sep 24 01:59:59 CEST 2030	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=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 10, 2021 10:10:31.532646894 CEST	34.98.67.61	443	192.168.2.3	49831	CN=*.mookie1.com, O=Xaxis LLC, L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Feb 22 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Mar 26 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	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=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 10, 2021 10:10:31.547080040 CEST	34.98.67.61	443	192.168.2.3	49830	CN=*.mookie1.com, O=Xaxis LLC, L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Feb 22 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Mar 26 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	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=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 10, 2021 10:10:31.767860889 CEST	54.64.53.220	443	192.168.2.3	49829	CN=*.adingo.jp, O="fluct,Inc.", L=Shibuya-ku, ST=Tokyo, C=JP CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 26 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Fri Apr 15 01:59:59 CEST 2022 Tue Sep 24 01:59:59 CEST 2030	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=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:10:37.327020884 CEST	172.67.183.244	443	192.168.2.3	49836	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	Mon Oct 26 01:00:00 CET 2020 Mon Jan 27 13:48:08 CET 2020	Tue Oct 26 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					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		
May 10, 2021 10:10:52.986335039 CEST	35.244.159.8	443	192.168.2.3	49843	CN=*.openx.net, O=OpenX Technologies inc., L=Pasadena, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jun 18 02:00:00 CEST 2020 Mon Nov 06 13:23:45 CET 2017 Fri Nov 10 01:00:00 CET 2006	Tue Aug 17 14:00:00 CEST 2021 Sat Nov 06 13:23:45 CET 2027 Mon Nov 10 01:00:00 CET 2031	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=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 10, 2021 10:10:52.986393929 CEST	35.244.159.8	443	192.168.2.3	49844	CN=*.openx.net, O=OpenX Technologies inc., L=Pasadena, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jun 18 02:00:00 CEST 2020 Mon Nov 06 13:23:45 CET 2017 Fri Nov 10 01:00:00 CET 2006	Tue Aug 17 14:00:00 CEST 2021 Sat Nov 06 13:23:45 CET 2027 Mon Nov 10 01:00:00 CET 2031	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=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 10, 2021 10:10:53.145221949 CEST	18.135.148.201	443	192.168.2.3	49847	CN=*.innovid.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 07 01:00:00 CET 2020 Mon Nov 06 13:23:33 CET 2017	Thu Apr 07 14:00:00 CEST 2022 Sat Nov 06 13:23:33 CET 2027	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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:10:53.145685911 CEST	18.135.148.201	443	192.168.2.3	49848	CN=*.innovid.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 07 01:00:00 CET 2020 Mon Nov 06 13:23:33 CET 2017	Thu Apr 07 14:00:00 CEST 2022 Sat Nov 06 13:23:33 CET 2027	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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
May 10, 2021 10:10:53.159667015 CEST	184.73.211.96	443	192.168.2.3	49842	CN=*.dlx.addthis.com, OU=Oracle ODC BROOMFIELD, O=Oracle Corporation, L=Redwood City, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Apr 22 02:00:00 CEST 2021 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Tue May 24 01:59:59 CEST 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	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=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 10, 2021 10:10:53.163759947 CEST	184.73.211.96	443	192.168.2.3	49841	CN=*.dlx.addthis.com, OU=Oracle ODC BROOMFIELD, O=Oracle Corporation, L=Redwood City, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Apr 22 02:00:00 CEST 2021 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Tue May 24 01:59:59 CEST 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	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=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 10, 2021 10:11:28.633550882 CEST	13.32.25.3	443	192.168.2.3	49859	CN=covid19tracking.narrativa.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue Apr 06 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Fri May 06 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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

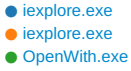
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 10, 2021 10:11:28.637671947 CEST	13.32.25.3	443	192.168.2.3	49860	CN=covid19tracking.narrativa.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue Apr 06 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Fri May 06 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 10, 2021 10:11:29.747221947 CEST	65.9.66.121	443	192.168.2.3	49864	CN=*.execute-api.eu-west-3.amazonaws.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sun Jul 12 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Aug 12 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 10, 2021 10:11:29.784437895 CEST	65.9.66.121	443	192.168.2.3	49863	CN=*.execute-api.eu-west-3.amazonaws.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sun Jul 12 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Aug 12 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5660 Parent PID: 792

General

Start time:	10:10:10
Start date:	10/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7ac580000
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: 5656 Parent PID: 5660

General

Start time:	10:10:11
Start date:	10/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5660 CREDAT:17410 /prefetch:2
Imagebase:	0x810000
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

Analysis Process: OpenWith.exe PID: 6460 Parent PID: 792

General

Start time:	10:11:24
Start date:	10/05/2021
Path:	C:\Windows\System32\OpenWith.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\OpenWith.exe -Embedding
Imagebase:	0x7ff7fa720000
File size:	111120 bytes
MD5 hash:	D179D03728E95E040A889F760C1FC402
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis