ID: 403974
Cookbook: browseurl.jbs
Time: 15:38:45
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Analysis Report http://localcoronavirus.com

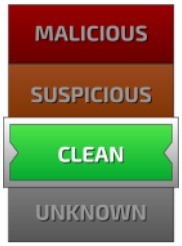
Overview

General Information

Sample URL:	http://localcoronavirus.com
Analysis ID:	403974
Infos:	

Most interesting Screenshot:

Detection

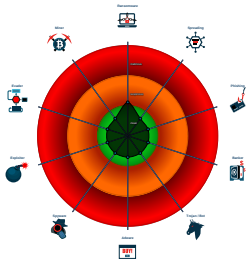


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4872 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5680 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4872 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- OpenWith.exe (PID: 7128 cmdline: C:\Windows\system32\OpenWith.exe -Embedding MD5: D179D03728E95E040A889F760C1FC402)
- **cleanup**

Malware Configuration

No configs have been found

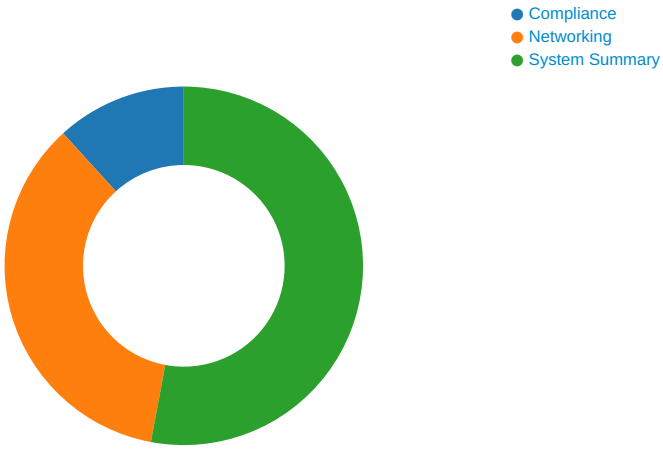
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



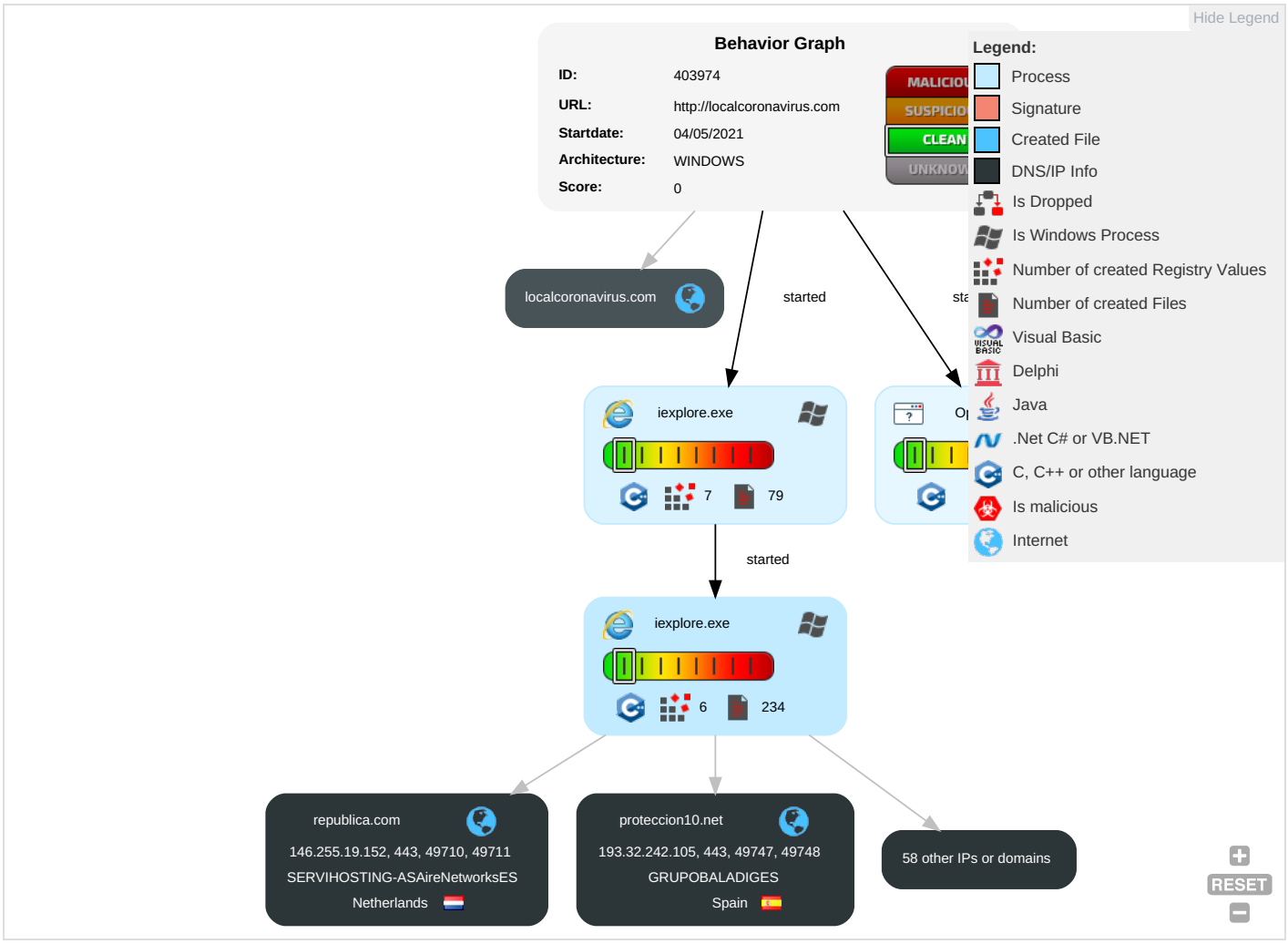
Click to jump to signature section

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

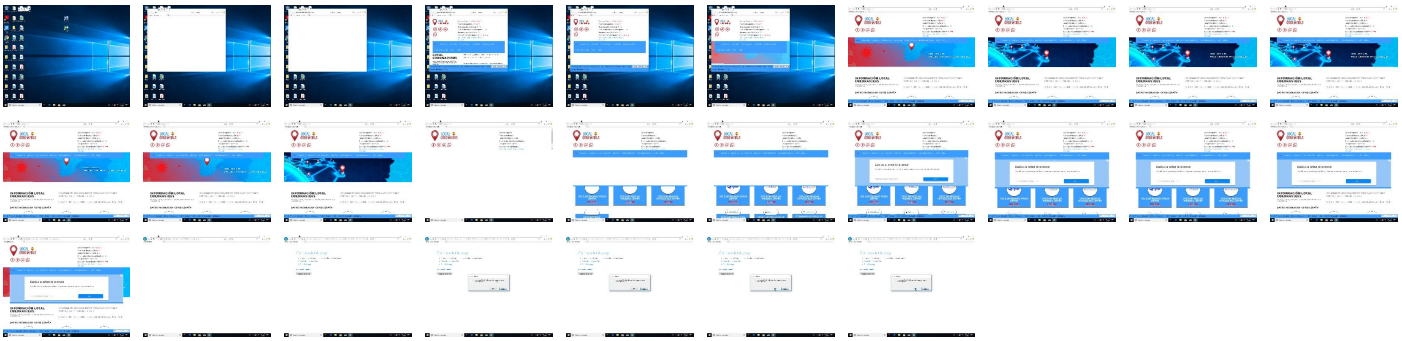
Behavior Graph

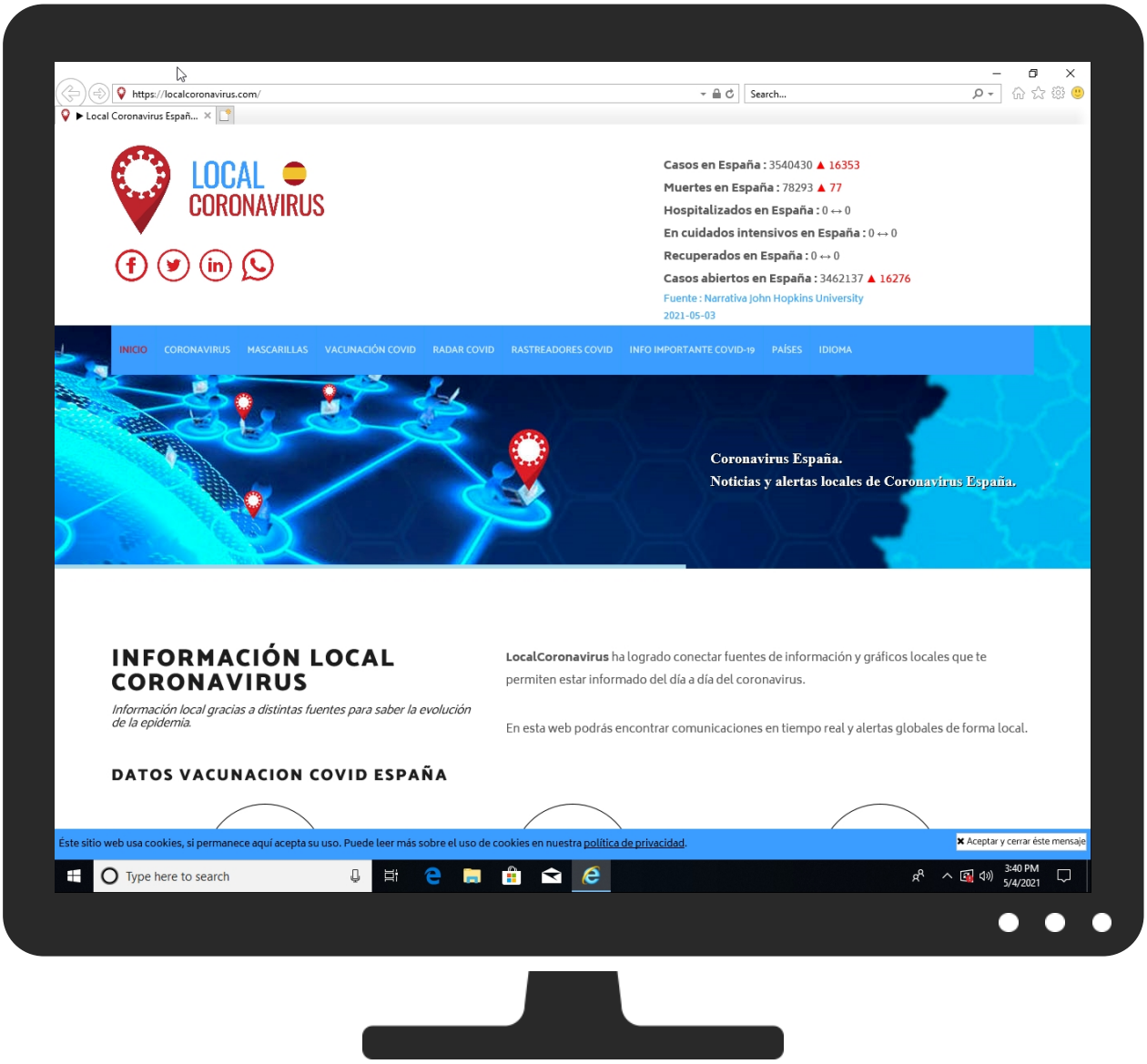


Screenshots

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

Source	Detection	Scanner	Label	Link
cc.adingo.jp	0%	Virustotal		Browse
prensaiberica.map.fastly.net	0%	Virustotal		Browse
localcoronavirus.com	5%	Virustotal		Browse
cni-digital.map.fastly.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.hotjarconsent.com/sv.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/sv.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/sv.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://www.hotjarconsent.com/pt.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://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://https://www.facebook.cus.com/	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/	0%	Avira URL Cloud	safe	
http://https://www.nwc10.com/politica-privacidad	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://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://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://www.eldiarioar.com/mundo/libertad-ayuso-coalicion-extrema-derecha-cambio-madrid-26-anos-desp	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://www.facebook.c	0%	URL Reputation	safe	
http://https://www.facebook.c	0%	URL Reputation	safe	
http://https://www.facebook.c	0%	URL Reputation	safe	
http://https://proteccion10.net/compras.html	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	
http://https://www.hotjarconsent.com/sq.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/sq.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/sq.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/it.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/it.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/it.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/pt_br.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/pt_br.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/pt_br.html	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.googletagservices.com	142.250.186.34	true	false		high
www.meneame.net	52.212.89.238	true	false		high
di7juyclzlgyp.cloudfront.net	13.225.74.99	true	false		high
cc.adingo.jp	18.179.240.58	true	false	• 0%, Virustotal, Browse	unknown
prensaiberica.map.fastly.net	199.232.194.133	true	false	• 0%, Virustotal, Browse	unknown
republica.com	146.255.19.152	true	false		high
scontent.xx.fbcdn.net	31.13.92.14	true	false		high
script.hotjar.com	13.224.193.31	true	false		high
tagr-gcp-odr-euw4.mookie1.com	34.98.67.61	true	false		high
d1j70itqjm2icu.cloudfront.net	13.225.74.97	true	false		high
cm.g.doubleclick.net	172.217.16.130	true	false		high
facebook.com	31.13.92.36	true	false		high
match-1943069928.eu-west-1.elb.amazonaws.com	54.76.6.247	true	false		high
localcoronavirus.com	104.21.18.245	true	false	• 5%, Virustotal, Browse	unknown
d2dzdx91mh5kpx.cloudfront.net	13.224.193.60	true	false		high
id.rlcdn.com	35.244.174.68	true	false		high
static-cdn.hotjar.com	13.225.74.20	true	false		high
www.google.de	142.250.185.227	true	false		high
star-mini.c10r.facebook.com	31.13.92.36	true	false		high
pagead46.l.doubleclick.net	142.250.186.98	true	false		high
pugm22000nf.pubmatic.com	185.64.189.115	true	false		high
us-u.openx.net	35.244.159.8	true	false		high
stats.l.doubleclick.net	74.125.140.155	true	false		high
s.libertaddigital.com	213.149.255.231	true	false		high
cni-digital.map.fastly.net	151.101.2.133	true	false	• 0%, Virustotal, Browse	unknown
akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com	52.211.67.210	true	false		high
cs491.wac.edgecastcdn.net	192.229.233.25	true	false		high
proteccion10.net	193.32.242.105	true	false		unknown
vars.hotjar.com	13.224.193.91	true	false		high
partnerad.l.doubleclick.net	142.250.185.194	true	false		high
aec01.esg.eldiario.edgetcdn.io	84.17.62.22	true	false		unknown
googleads.g.doubleclick.net	172.217.16.130	true	false		high
m.facebook.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high
img.europapress.es	unknown	unknown	false		high
image6.pubmatic.com	unknown	unknown	false		high
estaticos-cdn.elperiodico.com	unknown	unknown	false		high
adservice.google.de	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
token.rubiconproject.com	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
static1.abc.es	unknown	unknown	false		high
match.adsrvr.org	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
odr.mookie1.com	unknown	unknown	false		high
www.republica.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
imagenes.20minutos.es	unknown	unknown	false		high
static.eldiario.es	unknown	unknown	false		high
media.revistagq.com	unknown	unknown	false		high

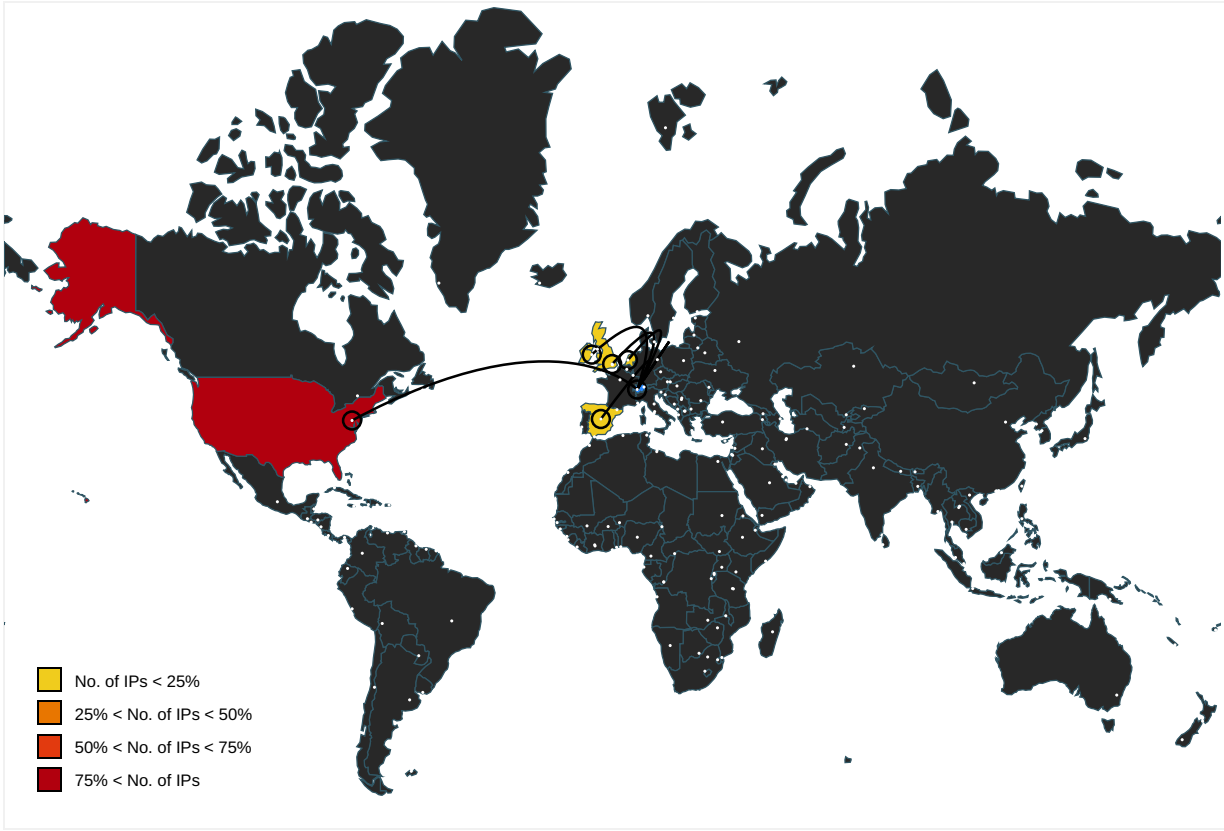
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.infosalus.com/asistencia/noticia-gobierno-asegura-espana-condiciones-vacunar-70-poblacio	1PTSF1WK.htm.2.dr	false		high
http://fontawesome.io	font-awesome.min[1].css.2.dr	false		high
http://https://stats.g.doubleclick.net/g/collect	js[1].js0.2.dr	false		high
http://https://www.hotjarconsent.com/sv.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.genbeta.com/actualidad/esta-web-puedes-comprobar-saturacion-aforo-tu-colegio-electoral-t	1PTSF1WK.htm.2.dr	false		high
http://https://www.elperiodico.com/es/sociedad/20210504/vacunacion-covid-cataluna-datos-ultima-hora-1164434	1PTSF1WK.htm.2.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/interaction/%3Fai%3DCjCerpU6RYLPwEY-a-waU7LqwAezmuqNi5b2x	{9DDE2F11-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr, ads[1].htm.2.dr	false		high
http://https://www.hotjarconsent.com/pt.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.20minutos.es/noticia/4684721/0/las-farmacias-malaguenas-comenzaran-un-programa-de-seguim	1PTSF1WK.htm.2.dr	false		high
http://https://static1.abc.es/media/espana/2021/05/04/teruel_buj-k0zG--1024x512	1PTSF1WK.htm.2.dr	false		high
http://https://www.youtube.com/iframe_api	js[1].js0.2.dr	false		high
http://https://www.hotjarconsent.com/de.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	widgets[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.meneame.net/m/actualidad/dispara-precio-vivienda-europa-medio-crisis-economica	1PTSF1WK.htm.2.dr	false		high
http://https://www.facebook.cus.com/	{9DDE2F11-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://connect.facebook.net/en_US/fbevents.js	1PTSF1WK.htm.2.dr	false		high
http://getbootstrap.com)	bootstrap[1].js.2.dr, bootstrap[1].css.2.dr	false	• Avira URL Cloud: safe	low
http://https://www.abc.es/espana/aragon/abci-teruel-regala-115000-euros-bonos-para-gastar-comercios-bares-y	1PTSF1WK.htm.2.dr	false		high
http://https://script.hotjar.com/	hotjar-2075733[1].js.2.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.2.dr	false		high
http://https://cdn.ampproject.org/amp4ads-host-v0.js	f[1].txt0.2.dr	false		high
http://https://www.mscbs.gob.es/profesionales/saludPublica/ccayes/alertasActual/nCov/vacunaCovid19.htm	1PTSF1WK.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://greensock.com	jquery.themepunch.tools.min[1].js.2.dr	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://https://covid19tracking.narrativa.com/	1PTSF1WK.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://insights-staging.hotjar.com	box-5e3cec51ed8e99df6977c199d27812d7[1].htm.2.dr	false		high
http://https://www.nwc10.com/politica-privacidad	1PTSF1WK.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.lavozdegalicia.es/noticia/sociedad/2021/05/04/gobierno-aprobara-decreto-comunidades-pued	1PTSF1WK.htm.2.dr	false		high
http://https://vars.hotjar.com/box-5e3cec51ed8e99df6977c199d27812d7.html	{9DDE2F11-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false		high
http://https://cdn.jsdelivr.net/npm/chart.js	1PTSF1WK.htm.2.dr	false		high
http://https://www.hotjarconsent.com/pl.html	modules.7225c79fe4e29708c611[1].js.2.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[2].htm.2.dr, ads[1].htm1.2.dr	false		high
http://https://www.hotjarconsent.com/fr.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.hotjarconsent.com/ru.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.libertaddigital.com/ciencia-tecnologia/salud/2021-05-04/portugal-suma-un-dia-mas-sin-mue	1PTSF1WK.htm.2.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/images/mtad/x_blue.png	{9DDE2F11-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr, ads[1].htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://labs.skinkers.com/touchSwipe/	jquery.themepunch.tools.min[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/images/adchoices/iconx2-000000.png	ads[2].htm.2.dr, ads[1].htm1.2.dr, {9DDE2F11-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false		high
http://https://www.motorpasion.com/industria/ventas-coches-espana-abril-cierra-desplome-34-2-respecto-a-niv	1PTSF1WK.htm.2.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&h=280&adk=	{9DDE2F11-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false		high
http://https://www.googletagservices.com/activeview/js/current/osd.js	f[1].txt0.2.dr	false		high
http://https://cct.google/taggy/agent.js	js[2].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/interaction/%3Fai%3DCovBFqU6RYKrdIdKD-waG9qSoAfL766Jijb6x	ads[1].htm0.2.dr	false		high
http://https://i.blogs.es/9fbb30/aforo-ios/840_560.jpg	1PTSF1WK.htm.2.dr	false		high
http://https://imagenes.20minutos.es/files/og_thumbnail/uploads/imagenes/2021/05/04/la-consejeria-de-turism	1PTSF1WK.htm.2.dr	false		high
http://https://www.eldiario.es/madrid/participacion-sube-puntos-comunidad-madrid-respecto-13-00-horas_1_789	1PTSF1WK.htm.2.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/drt/si	{9DDE2F11-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false		high
http://https://www.eldiarioar.com/mundo/libertad-ayuso-coalicion-extrema-derecha-cambio-madrid-26-anos-desp	1PTSF1WK.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.hotjarconsent.com/el.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.google.%/ads/ga-audiences	analytics[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.facebook.c	{9DDE2F11-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.youtube.com/	msapplication.xml7.1.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/html/r20210429/r20190131/zrt_lookup.html#RS-0-&adk=181227	{9DDE2F11-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false		high
http://https://proteccion10.net/compras.html	1PTSF1WK.htm.2.dr, {9DDE2F11-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://stats.g.doubleclick.net/g/collect?v=2&	js[1].js0.2.dr	false		high
http://https://www.republica.com/wp-content/uploads/2021/05/bill-gates-y-melinda-gates.jpg	1PTSF1WK.htm.2.dr	false		high
http://https://www.lavozdegalicia.es/default/2021/04/14/00121618431541670624319/Foto/sdasdasd.jpg	1PTSF1WK.htm.2.dr	false		high
http://googleads.g.doubleclick.net	f[3].txt.2.dr, f[1].txt0.2.dr	false		high
http://https://twitter.com/in	{9DDE2F11-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false		high
http://https://www.europapress.es/murcia/noticia-consejeria-turismo-grupo-fuertes-hotel-puerto-juan-montiel	1PTSF1WK.htm.2.dr	false		high
http://https://www.hotjarconsent.com/zh.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nwc10.com/condiciones-del-servicio	1PTSF1WK.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.nwc10.com/politica-privacidad	1PTSF1WK.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://twitter.com/SaludPublicaEs	1PTSF1WK.htm.2.dr	false		high
http://https://www.hotjar.com	box-5e3cec51ed8e99df6977c199d27812d7[1].htm.2.dr	false		high
http://https://www.hotjarconsent.com/fi.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://plugins.jquery.com/project/touchSwipe	jquery.themepunch.tools.min[1].js.2.dr	false		high
http://www.greensock.com/club/	jquery.themepunch.tools.min[1].js.2.dr	false		high
http://https://github.com/mattbryson/TouchSwipe-Jquery-Plugin	jquery.themepunch.tools.min[1].js.2.dr	false		high
http://greensock.com/standard-license	jquery.themepunch.tools.min[1].js.2.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/images/mtad/ad_choices_blue.png	{9DDE2F11-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr, ads[1].htm.2.dr	false		high
http://www.amazon.com/	msapplication.xml.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://https://www.hotjarconsent.com/sq.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://media.revistagq.com/photos/60910fb6235a5910299c90f7/16:9/w_1920	1PTSF1WK.htm.2.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/interaction/%3Fai%3DCy_Eyv06RYP7RAcSV1wach5fICdHl885i_K3g	ads[1].htm1.2.dr	false		high
http://https://static.eldiario.es/clip/b4ea4bde-ea9d-4a45-9776-0c96ca06f282_facebook-eldiarioar-watermarked	1PTSF1WK.htm.2.dr	false		high
http://https://www.hotjarconsent.com/it.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://platform.twitter.com/widgets.js	1PTSF1WK.htm.2.dr	false		high
http://https://attestation.android.com	f[1].txt.2.dr	false		high
http://https://www.hotjarconsent.com	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.20minutos.es/noticia/4684770/0/la-consejeria-de-turismo-grupo-fuertes-y-hotel-puerto-jua	1PTSF1WK.htm.2.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/interaction/%3Fai%3DC2NR3vU6RYLepNo7Y1gbn8rOIC-zmuqNi5b2x	ads[2].htm.2.dr, {9DDE2F11-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false		high
http://https://www.republica.com/2021/05/04/bill-y-melinda-gates-se-divorcian-tras-27-anos-de-matrimonio/	1PTSF1WK.htm.2.dr	false		high
http://https://www.hotjarconsent.com/pt_br.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.primevideo.com/?&tag=nwc10-21	compras[1].htm.2.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&adk=181227	{9DDE2F11-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0	rx_lidar[1].js.2.dr, f[3].txt.2.dr	false		high
http://https://amzn.to/2PG3o3c	compras[1].htm.2.dr	false		high
http://https://i.blogs.es/3d0f69/peugeot-concesionario-/840_560.jpeg	1PTSF1WK.htm.2.dr	false		high
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://https://amzn.to/31GOUWE	compras[1].htm.2.dr	false		high
http://https://img.europapress.es/fotoweb/fotonoticia_20210504124210_1024.jpg	1PTSF1WK.htm.2.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/html/r20210429/r20190131/zrt_lookup.html	{9DDE2F11-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false		high
http://fontello.com	revicons[1].eot.2.dr	false		high
http://https://www.meneame.net//mnmstatic.net/img/mnm/logo-350x350.png	1PTSF1WK.htm.2.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/html/r20210429/r20190131/zrt_lookup.html#	{9DDE2F11-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr, f[1].txt.2.dr	false		high
http://https://img.europapress.es/fotoweb/fotonoticia_20210504113316_1024.jpg	1PTSF1WK.htm.2.dr	false		high
http://https://cdn.ampproject.org/rtv/%	f[1].txt0.2.dr	false		high
http://https://googleads.g.doubleclick.net	f[3].txt.2.dr, f[1].txt0.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
84.17.62.22	aec01.esg.eldiario.edgetcdn.io	United Kingdom		60068	CDN77GB	false
192.229.233.25	cs491.wac.edgecastcdn.net	United States		15133	EDGECASTUS	false
213.149.255.231	s.libertaddigital.com	Spain		16371	ACENS_ASSpainHostinghousingandVPNservicesES	false
146.255.19.152	republica.com	Netherlands		29119	SERVIHOSTING-ASAireNetworksES	false
31.13.92.14	scontent.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false
31.13.92.36	facebook.com	Ireland		32934	FACEBOOKUS	false
13.225.74.20	static-cdn.hotjar.com	United States		16509	AMAZON-02US	false
142.250.185.227	www.google.de	United States		15169	GOOGLEUS	false
35.244.159.8	us-u.openx.net	United States		15169	GOOGLEUS	false
54.76.6.247	match-1943069928.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
199.232.194.133	prensaiberica.map.fastly.net	United States		54113	FASTLYUS	false
18.179.240.58	cc.adingo.jp	United States		16509	AMAZON-02US	false
185.64.189.115	pugm22000nf.pubmatic.com	United Kingdom		62713	AS-PUBMATICUS	false
13.224.193.91	vars.hotjar.com	United States		16509	AMAZON-02US	false
13.224.193.31	script.hotjar.com	United States		16509	AMAZON-02US	false
142.250.186.98	pagead46.l.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.186.34	www.googletagservices.com	United States		15169	GOOGLEUS	false
52.211.67.210	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
13.225.74.97	d1j70itqjm2icu.cloudfront.net	United States		16509	AMAZON-02US	false
104.21.18.245	localcoronavirus.com	United States		13335	CLOUDFLARENETUS	false
52.212.89.238	www.meneame.net	United States		16509	AMAZON-02US	false
13.225.74.99	di7juyclzlgyp.cloudfront.net	United States		16509	AMAZON-02US	false
74.125.140.155	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
151.101.2.133	cni-digital.map.fastly.net	United States		54113	FASTLYUS	false
142.250.185.194	partnerad.l.doubleclick.net	United States		15169	GOOGLEUS	false
193.32.242.105	proteccion10.net	Spain		41705	GRUPOBALADIGES	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.224.193.60	d2dzdx91mh5kpx.cloudfront.net	United States		16509	AMAZON-02US	false
35.244.174.68	id.rlcdn.com	United States		15169	GOOGLEUS	false
172.217.16.130	cm.g.doubleclick.net	United States		15169	GOOGLEUS	false
34.98.67.61	tagr-gcp-odr-euw4.mookie1.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403974
Start date:	04.05.2021
Start time:	15:38:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 13s
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:	19
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@4/190@36/30
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): 131.253.33.200, 13.107.22.200, 52.147.198.201, 104.43.139.144, 20.82.210.154, 88.221.62.148, 142.250.185.72, 142.250.184.234, 142.250.185.110, 142.250.186.162, 92.122.213.162, 92.122.213.154, 151.101.2.109, 151.101.66.109, 151.101.130.109, 151.101.194.109, 142.250.185.67, 142.250.185.142, 172.217.18.98, 142.250.184.196, 142.250.186.161, 69.173.144.165, 69.173.144.138, 69.173.144.139, 184.30.24.56, 13.64.90.137, 152.199.19.161, 2.20.142.210, 2.20.142.209, 92.122.145.220 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, arc.msn.com.nsatc.net, partner.googleadservices.com, fs-wildcard.microsoft.com.edgekey.net, e11290.dspg.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, www.google-analytics.com, www.bing.com, fonts.googleapis.com, fs.microsoft.com, skypedataprdcolcus16.cloudapp.net, pagead2.googlesyndication.com, dual-a-0001.dc-msedge.net, www3.l.google.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, wac.apr-8315.edgecastdns.net, cs9.wpc.v0cdn.net, a1972.g2.akamai.net, au.download.windowsupdate.com.edgesuite.net, pixel.rubiconproject.net.akadns.net, store-images.s-microsoft.com-c.edgekey.net, adservice.google.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, www.googletagmanager.com, arc.trafficmanager.net, prod.fs.microsoft.com.akadns.net, dualstack.f3.shared.global.fastly.net, static-abc.akamaized.net, skypedataprdcolwus17.cloudapp.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, skypedataprdcoleus16.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, tpc.googlesyndication.com, go.microsoft.com.edgekey.net, analytics.google.com • 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
15:41:10	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\IUHEMSR9\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\T8DRMTJ1\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):	226123
Entropy (8bit):	5.355341736734998
Encrypted:	false
SSDEEP:	768:0gQ3em9O5kTgQ3em9O5kTgQ3em9O5kDDBgQ3em9O5kDDBgQ3em9O5kDDxgQ3em9k:yXXP7b11ngggaJR11llk
MD5:	510EC31AA4633205D18F60BD6193E058
SHA1:	B585D47FA014035824436E02BBE841B62771DE89
SHA-256:	BD0F379AEC7128D2CBC5958D57B02DFE9A9C6864B70878710F496F7CDA9D8AC9
SHA-512:	49D5C01DA8243FEFE81973FD109A495C0FDA628F858FCA887D2FBB4E3B8D12A179AB49C04FE6C6E73E8771C582F6565E8A7DDA1964D25AFCA4376D184B085D E
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="goog_pem_mod" value="804" ltime="1665891600" htime="30884150" /><item name="google_experiment_mod34" value="13" ltime="1666201600" htime="30884150" /><item name="google_experiment_mod53" value="950" ltime="1666201600" htime="30884150" /><item name="google_experiment_mod36" value="821" ltime="1666361600" htime="30884150" /><item name="google_experiment_mod37" value="487" ltime="1666361600" htime="30884150" /></root><root><item name="goog_pem_mod" value="804" ltime="1665891600" htime="30884150" /><item name="google_experiment_mod34" value="13" ltime="1666201600" htime="30884150" /><item name="google_experiment_mod53" value="950" ltime="1666201600" htime="30884150" /><item name="google_experiment_mod36" value="821" ltime="1666361600" htime="30884150" /><item name="google_experiment_mod37" value="487" ltime="1666361600" htime="30884150" /><item name="google_experiment_mod44" value="205" ltime="1666361600" htime="30884150" /></root><root><item name="goog_pem_m

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9DDE2F0F-AD29-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.882793420260734

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9DDE2F0F-AD29-11EB-90E6-ECF4BB82F7E0}.dat	
Encrypted:	false
SSDEEP:	192:r6ZpZj2kW1tHifwlbzMHzBIZDasfGlSjrjql:rm/azfg5tEJXY
MD5:	9456EBF306BBE04787ADCD4F2CA1907F
SHA1:	3576789837121ECA7255B54735D7E3B232296918
SHA-256:	BA8862DAA63BADC37DE01A1D993084CE8C66483D7E519CE7ACB97280091DBA34
SHA-512:	65EAD9BE91C4084D2B7045E97FBD74E43AF58FBF8E459325B331DCC143EF633B0ACCA199730AF701BE6DACD67E3DE86A302DD2BBD7A0BF531C12E6B14D157 14
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\{9DDE2F11-AD29-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	1121308
Entropy (8bit):	4.044495001400963
Encrypted:	false
SSDEEP:	6144:JXrKefZ4XrKefZ1WBDqefS7RLBDqefS7R2k:JnZ4nZ45S7RL5S7R7
MD5:	4667B841B0900FEC546FF407F016DC30
SHA1:	1E5EFEFBDA80490A1FEAFE43D9CA513B6E586C03
SHA-256:	04AA4CE0E9190C62AC3DB362588DABD709FE7ABA7AFA109967AA0429CDDE61A3
SHA-512:	3DB59FA741AA62CD51DA7E671B0B6F6D79E0E44CDAE1B84710BAB8C5DDD4F24F0060E62634B65E8B138377E8A54296C4C8F2A6CA1F35D6971C9B02C0B2968B D
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\{A67B91EC-AD29-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5661644543434754
Encrypted:	false
SSDEEP:	48:IwoGcprNGwpaSG4pQhGrapbSFZGQpKgG7HpRmQaTGIpG:rcZXQi6xBSFzA7TmQeA
MD5:	CB0A925FC6C864BD32C8FF243BEADA14
SHA1:	3CE29AFC4A534A8A4AB7C9CFAC117375A76AE4DE
SHA-256:	F2B06F7697D492C744F8BB01E21E973D1633904DD0C5EC69DFD3E29A7D240277
SHA-512:	70E1A6A090768F4DD5FF0835164FB040AB951BD4C8C067AAC1BB9734547E99DCFD39A484B40949866E11FAF4489FB4B7C1F42C8E37474362BCB436B045521323
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):	660
Entropy (8bit):	5.118241716613301
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEtBkeBkanWimI002EtM3MHdNMNxOEtBkeBkanWimI00OYVbkEtMb:2d6NxOCueuaSZHKd6NxOCueuaSZ7xb
MD5:	DAB80B9824F91C04D870D6A1E7CC8D5D
SHA1:	42ABF597AB8173A810B673A35F30B591FFF2435F
SHA-256:	F07FC640DB6C201966BD5F10E4E74B00C4299623260A65DF960E6BCD0DA2CA0C
SHA-512:	57A5682F756984660D216D280C20554A5676B65B0DEBC1F8453B39174756F5A775274B59FD3DBB947B4235ACC2692928F9CE252F0CBB636BB90EA822832467B6

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x76e9496f,0x01d74136</date><accdate>0x76e9496f,0x01d74136</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>0x76e9496f,0x01d74136</date><accdate>0x76e9496f,0x01d74136</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):	657
Entropy (8bit):	5.141192704798259
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kobanWimI002EtM3MHdNMNxe2koOjanWimI00OYkak6EtMb:2d6NxrvbaSZHKd6NxrvwaSZ7Ja7b
MD5:	7D8AC00156F8F23B35DDC715DF2CF33D
SHA1:	F455A89561453088ADFFAF9B183427CC2862659C
SHA-256:	D0D2CA22451AB31CE2D35890EABB1664E4A3199CBED9B3C929A0792C7013E6DD
SHA-512:	D4D70342425C276B846E0017B945DBA7B8DA5E6303FB5FA29F1FFF933A48D7DA7419884954281488 8D05F522E8C1D0C4DF85F17D5E0EDFC0C123A453ED80F7A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x76e15a21,0x01d74136</date><accdate>0x76e15a21,0x01d74136</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>0x76e15a21,0x01d74136</date><accdate>0x76e292a9,0x01d74136</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):	666
Entropy (8bit):	5.125495718333674
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLnXYXanWimI002EtM3MHdNMNxvLnXmanWimI00OYmZEtMb:2d6NxvbXYXaSZHKd6NxvbXmaSZ7Zb
MD5:	DA758372407D74DD10ECD26FDFC9AA92
SHA1:	32F0C44D92B144551622E421574353C74282B81D
SHA-256:	3B1E8A0FCE7A9F4F58A9B8A515A2C6453E4F357000CC56D4384CDA50D5CEAF24
SHA-512:	84045EA8050FDBC616CFC27C6EEE507CFBEF13A0F6CD66E6E38F1E4EC379A2EBCD43414476457FC2EB34AA7E5582B69F88B57CD128F18E7A69FE8139F0E96A07
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x76e9e595,0x01d74136</date><accdate>0x76e9e595,0x01d74136</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>0x76e9e595,0x01d74136</date><accdate>0x76ea81e0,0x01d74136</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):	651
Entropy (8bit):	5.101732777871384
Encrypted:	false
SSDEEP:	12:TMHdNMNxihianWimI002EtM3MHdNMNxihianWimI00OYd5EtMb:2d6NxQiaSZHKd6NxQiaSZ7qjb
MD5:	8E2D679F38C80E5F9DA7A625677FC562
SHA1:	745F8822980B2B73F0749919088F6ADAFD27034D
SHA-256:	444899DB1982127C3D4F8878710D18980B4DADA492F0E133F00555654FBF6B77
SHA-512:	5232E06AB1E702AC040D1ABF145CEF73900B39CC351D06650D961896ACBB27B620263C9B63467F4D772329B34B443E248A93E8EF1BD11F408DDE73E6674C719E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x76e6d86c,0x01d74136</date><acc date>0x76e6d86c,0x01d74136</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>0x76e6d86c,0x01d74136</date><accdate>0x76e6d 86c,0x01d74136</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):	660
Entropy (8bit):	5.126903398843315
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwYnPnanWimI002EtM3MHdNMNxhGwYnPnanWimI00OY8K075EtMb:2d6NxQvvaSZHKd6NxQvvaSZ7RKajb
MD5:	D91081A1BC05B307C124BF143B63F323
SHA1:	D27C928E3ED4452B0DD2C42E73B63D38CC322055
SHA-256:	43BFA633807C11CBAE680377EA95157FCBA7B2D5AB1652F52E5246CFE853D203
SHA-512:	199348B3752D58F1EC811305E666184F4991A4309E459686BB14D13B1182F57A5D6F2DF73EBCEE4C9B0C7E8B4AFBCD3E82360BBE8EAE002FA1BDBE5D0789DFI 4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x76eb1e2b,0x01d74136</date>< accdate>0x76eb1e2b,0x01d74136</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>0x76eb1e2b,0x01d74136</date><accdate>0 x76eb1e2b,0x01d74136</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):	657
Entropy (8bit):	5.091608926763934
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nDganWimI002EtM3MHdNMNx0nDHkanWimI00OYxEtMb:2d6Nx0DgaSZHKd6Nx0DHkaSZ7+b
MD5:	399E9BE7703D10A51DB73E9B50458CF7
SHA1:	C66D58B840ED8EED2D21CB6D06BCCC7AD9E513D1
SHA-256:	31B958AD541A20024CB6DBF663BBBCCD5AECA21144EEE5C2108214813D683924
SHA-512:	014603A6E6D74CA12C726063C11BDB8D2E217F52345E511B0145A6005C54E87D9A77FF0B61A0496B1D50ED081B912B4E257435AE70B179323E19FA74D670D98B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x76e810f0,0x01d74136</date><a ccdate>0x76e810f0,0x01d74136</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>0x76e810f0,0x01d74136</date><accdate>0x7 6e8ad24,0x01d74136</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\pin20259167780\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):	660
Entropy (8bit):	5.139223142721226
Encrypted:	false
SSDEEP:	12:TMHdNMNxx21anWimI002EtM3MHdNMNxx21anWimI00OY6Kq5EtMb:2d6NxE1aSZHKd6NxE1aSZ7Xb
MD5:	AD2698D60AFF3D1F6542CB0264D99014
SHA1:	38DDF7AF32A38DC3A9B5FD29186B510A20C977BC
SHA-256:	F21AF3B0A3F85D4F36F47A37707C1D7F7125DAE758571439373B620EB118A795
SHA-512:	1856EF40D4111969F8EAF7DCD904CD3231523C194C7DC66E55700477A843FC653BEFD0757F47410BD298A1AC0D6F656DCC0D8A2F968D1655B3E6020CF124BCF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x76e7749c,0x01d74136</date>< accdate>0x76e7749c,0x01d74136</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>0x76e7749c,0x01d74136</date><accdate>0 x76e7749c,0x01d74136</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):	663
Entropy (8bit):	5.1141619909618505
Encrypted:	false
SSDEEP:	12:TMHdNMNxcZkAkanWimI002EtM3MHdNMNxcZkj9anWimI00OYVEtMb:2d6NxckAkaSZHKd6NxckJaSZ7Gb
MD5:	4FF9A65C26CFECE4B5977CDAFF27E088
SHA1:	FCA66A99A38924B7E18E99F69C4DDCF3F41A2BB9
SHA-256:	A39FD656C1A8CD62B3C614F90F216C652B80D176B0DFA4CBB431CDE5CEF32184
SHA-512:	9D736DE8BE903090CA32AFE412BC5BDCEDDC68AB8FC49CBF54DF5C7D6A6F09031364D13D18A02F5EC5F32269DF7B94F2E8618A6DEEED0FCA48DAA1B28F26EAA
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x76e46765,0x01d74136</date><accdate>0x76e46765,0x01d74136</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>0x76e46765,0x01d74136</date><accdate>0x76e503ac,0x01d74136</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):	657
Entropy (8bit):	5.117958477581544
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnKtanWimI002EtM3MHdNMNxfnKdvokanWimI00OYe5EtMb:2d6NxitaSZHKd6NxivaSZ7Fjb
MD5:	71725C0464D19D1BDBE788E6F62F70E0
SHA1:	5859A2033E7DABE2812035E8F3A7F82D542A08BA
SHA-256:	6631500CD0395D8920A46D17660773D344BCEED60D5C1BC19714188430638385
SHA-512:	A574E6077A240F4F29F9F114F75293B882C7200D653B7EDB51491D38C34FA000DB5E812CA952839FCAD1F8D3060513B8483977E77BFC8577D2421CA67B3E020D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x76e59fe9,0x01d74136</date><accdate>0x76e59fe9,0x01d74136</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>0x76e59fe9,0x01d74136</date><accdate>0x76e63c26,0x01d74136</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\po60zt0\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	5893
Entropy (8bit):	7.724903479387729
Encrypted:	false
SSDEEP:	96:ohuQ5Vo7FhknmWpYOxYbOLMHfmH0mgzdtsfNFeC933ktunIOys60yiiLEgY4yJVB:oEQ07FhknOuM/muPs1Fqmd9nyiiZqr
MD5:	19707E47DA1A453BCB19061DCA0E16EA
SHA1:	05189A5A1BFB9E22C642EBDEAD7ABC7F3298A785
SHA-256:	9EDDDC2A5B5901A9160D237CA410DE882D6138F8C2BDC27122BB5C256C2EB845
SHA-512:	C128A3CD77454C1A83A913AC23CB9A9F148FAC6A3DEAC84264752B9B58134434500047247B819AD43D2E9AD1163D58FB3B3AB5F6CD1BD326B15D8B19C9FC82B
Malicious:	false
Reputation:	low
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...I[. 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.@,=.YAx...U.;..b.p...azTd.7p....E.Z...<.....O..S?.....pHYs...#...#.x.?v....iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns: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\0MX4YUS9\1PTSF1WK.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\1PTSF1WK.htm	
Size (bytes):	122780
Entropy (8bit):	5.194075014117802
Encrypted:	false
SSDEEP:	1536:fL83LI+7/nygBnN2/SrkYt/hILtbt2C+XavXy3Qqa0MH1w0SB:fY35yg9N2/StKvXy3QqaJOB
MD5:	805FF9BC0DCCDCBFCE5E3B2B1CF65178
SHA1:	8CE983E7ED3BFF6B437FDD3C5B6DF88397F4BC08
SHA-256:	66EBEBBC8EB80235E7116FD077BBA1A0F14A4A5BBA620C031A3B4F0B99F7497F
SHA-512:	0941533F28CAE20CD8D88E8AEE64D42941800247CDF12D4FB280231C8F6821B5A2303497196FC7DABB267CBCFE087E8C849FE8E8DF22F638BE2273EEE868AC7D
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\0MX4YUS9\863871680303623[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	260504
Entropy (8bit):	5.470099146172389
Encrypted:	false
SSDEEP:	6144:Rk1HgCSntDV/HaK3V/Ha8NEPjQHguH3HpQrwzzmy:dNESj
MD5:	87753B8262278E0166E7F1E7F92C49E0
SHA1:	6C9E6E058A8C5846B2085117D823BF53B1FA3AAD
SHA-256:	F1D6A7834E0748B811B80D759DF150551D95091910B5A847B6BF0B7118C98190
SHA-512:	903601B90E616B51EFD69CAB7CE54626142F053101F118AD07B92E78C4463CEA3EB2F752E0DE02BFD1FEBF97E529F8B104416DF0D8EF010E1CE1B9541D95618
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\NYFVR9XC.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):	122780
Entropy (8bit):	5.193693112234917
Encrypted:	false
SSDEEP:	1536:fL83LI+7/nygB7DmzSrkYt/hILtbt2C+yQvXy3Qqa0MH1w0SB:fY35ygNDmzStHvXy3QqaJOB
MD5:	35AFB46CE76DD7857B51D69B3D29405A
SHA1:	E0E97DB7E8F5B9121C694D24CBE6AB2EE89BD646
SHA-256:	1A0272BFD0FFA43E3CB2A1675A9B1EB794ECB796752CB7D5A753F3C601196E50
SHA-512:	A645AEDD8C00C3BBCFC0E6A53BD92D6AD060FFF9F7A4DCF711558DD7C8D58EAB093F635EEAC9FF4170702C7559E718C915ABCE26A3AF91B10C1CD1FE53DED8B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/
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\0MX4YUS9\WhatsApp_local_coronavirus[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 240 x 240, 8-bit/color RGBA, non-interlaced
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\WhatsApp_local_coronavirus[1].png	
Size (bytes):	9229
Entropy (8bit):	7.8482709074172465
Encrypted:	false
SSDEEP:	192:4dgy7F8kn2Uhol9II9+A5yCJbPtndSUywePu7iyg7WeV3Ey8UY2A4tsSQhG:uvNn6Z+A5yolnEU1H+Cm37NLJQ0
MD5:	5796710287A4401FB4BFB44777440A3B
SHA1:	CA27C3240BA83E5A69C1F27EB27EFF335CBE5637
SHA-256:	DC02DDC4760348E5A4B3BE31785318618F4D1D8E49EF01C2BDBD342C805C402E
SHA-512:	DC8066DB03F018F0C38F2D9E89A811324CE1DBE904A64B6A51AC6C98B0A4DB5938B89B833AC9CA1C0C1C31165732D259B860E64E90C2447EF71E12117CD302C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/images/WhatsApp_local_coronavirus.png
Preview:	.PNG.....IHDR.....>U....&iCCPAdobe RGB (1998)..(.c``2ptqre.``..+).rwR...R`?.....> v^~^*...v...D_....@..J.(*.....(%.8...../)..3...E..... vQH.3.}...K.....I..... ..H}:....6....KR+@.28..T.e.g.(.ZZZ*8..'.*.W.....+x.%.....%.....B.....j..d.2.....9....bg.b..\ZT.e22...#.#.....B...a.....T...!...>..9...O..:6\....pHYs.....+.....iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns: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:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#" xmp:CreatorTool="Adobe Photoshop CC 2018 (Windows)" xmp:CreateDate="2020-08-24T14:35:41+02:00" xmp:Modi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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):	84738
Entropy (8bit):	6.087981855893732
Encrypted:	false
SSDEEP:	768:ZuNxaucrhUZA/MpxRoDGvYm96WURjdZVMZViZVyZVJZVJZVAZV5ZVYrcKClBVge7:McrhOpRoDGvt96nRjkGVuxeksCsd
MD5:	07BC9D2C365AC56E2A6080D367770855
SHA1:	D48885BF8002BD73AE2F396F17232C9C651E5EC4
SHA-256:	F1621C7D9EF7CCEC04AF4BE560BD57869FAAE8B53708C9239A80BF5CC550883D
SHA-512:	4C7C3CF26AB142F78A8D38FC03A1F6FEF1885715154A06BE3253C4FD356AADC8AF50620EBECA5221F67FE2694BB1147FD0E7A6AC7DFF19F0930B9BF02416B30C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&h=280&adk=2834291916&adf=1839787983&pi=t.aa~a.2825320467~rp.1&w=784&fwrn=4&fwrnh=100&lmt=1620167993&rafmt=1&to=qs&pwprc=4903144676&psa=0&format=784x280&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=1620167992228&bpp=256&bdt=7021&idt=258&shv=r20210429&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3De56d315663ea3c76-22b0e249c5c700e2%3AT%3D1620135589%3ART%3D1620135589%3AS%3DALNI_Mb3HA_1ETEXdPtDGNNg329xlt86Cw&prev_fmts=0x0&nras=2&correlator=4940367878114&frm=20&pv=1&ga_vid=1292693962.1620167988&ga_sid=1620167989&ga_hid=2138563339&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=0&ady=9447&biw=784&bih=554&scr_x=0&scr_y=0&oid=3&pvsid=1833982228483054&pem=804&eae=0&fc=1920&docm=11&brdim=44%2C114%2C36%2C36%2C1280%2C%2C800%2C640%2C784%2C554&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=128&bc=1&ifi=2&uci=a!2&btvi=1&xpc=5nHLSvG1Ju&p=https%3A//localcoronavirus.com&dtd=1075
Preview:	<!DOCTYPE html><html lang=fr><head><meta charset="UTF-8"><link rel="preload" href="https://www.gstatic.com/mysidia/a204a622610ec42c29322584ae03f5a9.js?tag=client_fast_engine" as="script"><script>var jscVersion = 'r20210429';</script><script>var google_casm=[];</script><script src="https://www.gstatic.com/mysidia/f27a2327937451811f326a3c5359709a.js?tag=pingback"></script><script>mys.pingback.init("COrVqrSTsPACFdLB3godBjsJFQ", [4,1],"scream/throne_image_logo_och", {2:"server",1:"bannerB",4:"mysidia_upscale,mysidia_analytics"},17);</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-overlay{height:100%;width:100%;overflow:hidden;position:absolute;top:0;left:0;box-sizing:border-box;pointer-events:none;z-index:1;border:1px solid #E5E5E5;}.mys-wrapper A,.mys-wrapper A:visited,.mys-wrapper A:hover,.m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\ads[2].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):	145627
Entropy (8bit):	5.694381972350085
Encrypted:	false
SSDEEP:	1536:7adBHXs+cHhy52nSNwru5BjJJy49HgYEXa28AOQjJ+tG1dmvxW7gWRE:7ad1s3SNwrubN9W/gG0WRE
MD5:	91193E28746A852D9AE8AC338B467224
SHA1:	4B05F4A57FF0B33651067735F704A26D5C844C5F
SHA-256:	30F782771CA2D6B87D8713C5AD8D62314492C82C6B31F8656CDAC7D83454AF0E
SHA-512:	BB67EFDD743DD4E95B74551718C5C5B4EEE49953322FB039A26A4DB7C5EE31D276977281E7CFC62C1DEEB3AD13C9D694DA9F814021672C93AF37791DD03EA2E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\ads[2].htm	
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&adk=1812271804&adf=3025194257&lmt=1620168013&plat=1%3A32776%2C2%3A32776%2C9%3A32776%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1081344%2C32%3A32&format=0x0&url=https%3A%2F%2Flocalcoronavirus.com%2F&ea=0&flash=29.0.0&pra=5&wgl=1&dt=1620168012023&bpp=288&bdt=1402&idt=805&shv=r20210429&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3De56d315663ea3c76-22b0e249c5c700e2%3AT%3D1620135589%3ART%3D1620135589%3AS%3DALNI_Mb3HA_1ETEXdPtDGNNg329xlt86Cw&nras=1&correlator=2836834130781&frm=20&pv=2&ga_vid=1292693962.1620167988&ga_sid=1620168014&ga_hid=1641196723&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=-12245933&ady=-12245933&biw=1280&bih=906&scr_x=0&scr_y=0&eid=31060932&oid=3&pvsid=96816254938719&pem=804&eae=2&fc=1920&docm=11&brdim=0%2C86%2C0%2C86%2C1280%2C%2C1280%2C906%2C1280%2C906&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=0&bc=1&ifi=1&uci=a!1&dtd=1610
Preview:	<script>window.sra_later_blocks = [];</script><script>window.sra_later_blocks.push({creative:'\x3c!doctype html\x3e\x3chtml \x3e\x3chead\x3e\x3clink href\x3d\x27//fonts.googleapis.com/css2?family\x3dRoboto:wght@400;700\x26display\x3dswap\x27 rel\x3d\x27stylesheet\x27 type\x3d\x27text/css\x27\x3e\x3cstyle\x3e* {margin: 0;padding: 0;outline: none;}body {background: rgba(52, 58, 65, 0.600000);backdrop-filter: blur(15px); /*potential issue: minimal browser support*/-webkit-backdrop-filter: blur(15px); /*for safari*/height: 100%;}#ad_iframe {box-shadow: 0 !important;display: block;left: auto;margin: 0 auto;position: relative;top: auto;}.creative {transition: opacity 1s;-webkit-transition: opacity 1s;position: relative;}#card {background-color: #fff;border-radius: 6px;padding: 0 6px 1px;position: relative;box-shadow: 0px 8px 12px rgba(60, 64, 67, 0.15), 0px 4px 4px rgba(60, 64, 67, 0.3);}html {height: 100%;}.toprow {width: 100%;display: table;height: 24px;background-color: #fff;}.btn {displa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\bill-gates-y-melinda-gates[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, 1000x521, frames 3
Category:	downloaded
Size (bytes):	35827
Entropy (8bit):	7.961951457004857
Encrypted:	false
SSDEEP:	768:NZNAKQ0d9nU68FCO8jUS8yBiGQI/LmzxhWpNnB2MihV3UhFGAg:PNAKj7nvc5VyBiGQATpKMY35D
MD5:	4F403C148A3CF19851DAD37195532F03
SHA1:	B357A5D2FB0A22486ED416B2CFAB2E449B7D9E6A
SHA-256:	ED832F3B5A404A926DF28263FDFDA98799A65D0A1E18C64492374476AF5A99CF
SHA-512:	93D2FDA6EEFF48F9BFC2DD396949FD5138BB08FDFA277AF94170A241B60007B6054D7462F7114A7F0E7C7A1096CA2817534A6BB587B2A01B956BD8E95A261204
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.republica.com/wp-content/uploads/2021/05/bill-gates-y-melinda-gates.jpg
Preview:	.....JFIF.....`.`.....C.....".....)..."1+320+/.6<MB69I:./C\DIPRWWW4A_f^TeMUWS...C.....'..'S7/7SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS....."....F.....!1.A."2Qaq..3...#B..R....$br.45s..%6cCS...t.....(.....1.!.AQ.."2#a.B.3.....?....Dv.).Q..~":...b.:.~...R.ur@.....1Z..V.(..*rB.s..}.Q&.,"*.....H.j.f.#H.. Y..2.a... .I..v.$4.....D.....c....S.... .p7..,9....X...dQ.r4EC.,....r0pQ..26..c.2l.P\.....A....|.5.....9..Q...0..B..l.....m_....+_J...p;..{.f.c:...#....Rob.T.b...e..A&1..n...c.,. .Y.&_....rf.N..F.c.....G;.....x.d..$...!..d.!..... vG!.z.Ab.n.J%..A`..4(.@.. .\..k. .j.....bBe. .....!..0....@..9.r...=.B\..A[.2.[.6.*..Y.m.1..!.m.:.....A"....Y."`..c.H.grD..O...F.....z.f.O...d.n....O.b.....I`.#.,.....Y<.d.m#....`.HAHE.}...oI.....GW._.....R..zP..\..... |..D.9#$....M..9.....d=. ...R.pKK..A.."8..&..D.[....l6'LM.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\compras[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text
Category:	downloaded
Size (bytes):	1127
Entropy (8bit):	4.673598119786123
Encrypted:	false
SSDEEP:	24:hYJpLm8t0ieVF1osUt6RPj9e0OUEiJXEdYjUAAFqOyLCm:2eVS0BQiJXPjZA7wf
MD5:	56DB3B2D0D375442DECCDF74B4A7BB3B
SHA1:	54EAF367D6737497D9257D72A0558A15C0D3C325
SHA-256:	FF44A9D345DED7E7372A580DC4E030CC2A9CE5BFF12959AE0F264D3F65469FB7
SHA-512:	09C503F9545C7FB5CFB8B8095E738026D33FFF1707D605878230A383DD4A061EF813A48E4AC8646AB6DA240FAD364CFA69DDF8B52DE0A5F985890BDA55593F4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://proteccion10.net/compras.html
Preview:	<!DOCTYPE html>.<html lang="es">. <head>. <meta charset="utf-8" />. <title>Localcoronavirus</title>. <meta name="viewport" content="width=device-width, initial-scale=1.0" />. <style>. a.btn {. text-decoration: none;. background: #3b9dff;. color: #fff;. font-weight: 600;. font-family: Arial;. width: 45%;. display: inline-grid;. text-align: center;. margin: 5px 1%;. padding: 5px 0px;. border: 1px solid #3b9dff;. }. a.btn:hover {. backgr ound: #fff;. color: #3b9dff;. }. </style>. </head>. <body>. . <a. href="https://www.primevideo.com/?&tag=nwc10-21". class="btn". target="_blank". >Entretenimiento</a. >.. <a href="https://amzn.to/31GOUWE" target="_blank" class="btn". >Mascarillas</a. >.. <a href="h ttps://amzn.to/2XQwbGR" target="_blank" class="btn". >Gel Hidroalc.holico</a. >..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\coronavirus_mapa_localcoronavirus_slide_1[1].jpg	
MD5:	2AC5010CB1563099923B56C3476EA347
SHA1:	C56091141290A054F57C52FAE3C18C56F967F0A6
SHA-256:	D21E2127BFF9C55CFE6ED2EE9C702C506938210341D3719C6601961745F1C2B0
SHA-512:	D1BB0351916F52A47F08B5B18FC9489DEAAC3A33C6D8DBA7726DE016841BCDB38D15970DB1692995B6AC39E522113C1ACDD23F4657CFA950C1A9414754011F D
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#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWg w.....5.....!1..AQaq"..2.....B#.R..3$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\0MX4YUS9\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:	3:0SYWFFWlIYCzHRiRI5XwDKLRIHDfFRWdFTfqzrZqcdAqsKTCEIoENRgVoYARNin:0IFFli+56ZRWHTizlpdAxInVuNin
MD5:	C9B33444138B8312C889B87B157D7830
SHA1:	60CF82CB0DEF72CD46143D1BD562BE26BA874802
SHA-256:	8EB72810C473A7DBEAB9EA57FDBFAA004741DFFE2070CACCAC318052AF3B81A1
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\0MX4YUS9\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	451
Entropy (8bit):	5.15306034662849
Encrypted:	false
SSDEEP:	12:UJO6940FF5O6ZRoT6pWqoSEqFF5O6ZX6pWJ6Y:G9X3OYsRqPv3OYXR1
MD5:	DB91C45EEE6BD63149623993BC50F47C
SHA1:	D7AA4823DBAB16FDA2A88CD82F6259E6A265579F
SHA-256:	0DA50F78231A135A4BD11DBD7D4D6F24CDAA0EF1393447A38F5C79DA2867A34C
SHA-512:	C8D88C7313752BFD3AF9BCCDFE7D28F0E2A3B1583ED9C094901A801C8E59644827459DFBE4711F8507C6D3F8B4BD5DB3FECDE22A91FFADA056D6087F6C7745 ED
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Google%20Sans%3A400%2C500
Preview:	/*. * See: https://fonts.google.com/license/googlerestricted. */.@font-face {. font-family: 'Google Sans';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/googlesans/v27/4UaGrENHsxJlGDuGo1OIlL3Owpg.woff) format('woff');.}.@font-face {. font-family: 'Google Sans';. font-style: normal;. font-weight: 500;. src: url(https://fonts.gstatic.com/s/googlesans/v27/4UabrENHsxJlGDuGo1OIlLU94YtzCwA.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\down[1]	
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..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\0MX4YUS9\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
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.inner HTML='',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\0MX4YUS9\f27a2327937451811f326a3c5359709a[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8881
Entropy (8bit):	5.578033022059697
Encrypted:	false
SSDEEP:	96:44ZV9/jGja65BrzFVfdM2jzeX/gZa0unHrcx4kiZiTtd/tNOmXTZN2Kbhkccq2sR:L/jF65Brn2eubqnPjq75svT+yXRD
MD5:	F27A2327937451811F326A3C5359709A
SHA1:	52817A78E17B0A0BA57A9C2C9786A0C9CB92FEBD
SHA-256:	8EFA0B5F70F2F4DD60CBFF9F4D37628167042EEA2566DB828EDAF9AC558E95D6
SHA-512:	F958DFCCBB75CD96C2F7B3459206A0BF5D845322EDA8E15FA9E4517FAC2065BBEDC6E22175C6B84C728C271865351D91B5DCF7BDFAEA1BF148CA0E7DEFB5A 61E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/mysidia/f27a2327937451811f326a3c5359709a.js?tag=pingback
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';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 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 da=ca(this);function l(a,b){if(b)a:{var c=da;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&&ba(c,a,{configurable:!0,writable:!0,value:b})}}.function n(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:aa(a)}}var ea="function"==typeof Obje

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	253758
Entropy (8bit):	5.501823771178204
Encrypted:	false
SSDEEP:	3072:/lR1M7SRCcd4IvIRJJ8bVAwATA/E690cWD1JRkdBl651e3Z5fA:nZqIvIRJeV/ATA/E6ikdBl6re3Z54
MD5:	D0C00B8E9BC800A7464CA47E8F77B5A5
SHA1:	4DB4B9E775191D01EF30A40A0C43D7F3C618B1E0
SHA-256:	9B458D60B6E55B50F6AFE3912990E5577BD2C9B7065473EA05001359E5311D30
SHA-512:	252EDEE656A137917214C789328D3C86766A8F1AB515EBBFA00524B8B75E46C23C855E42AFB7A2B267B2A885DD4BD726F6A24BE3FCDA50A02E14CD0FCD5891 8
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\f[1].txt	
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/pagead/js/r20210429/r20190131/show_ads_impl_with_ama.js?client=ca-pub-4607443575710795&plah=localcoronavirus.com&amaexp=1
Preview:	(function(sttc){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .var r,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 da(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 ea=da(this),ha="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),v={},ia={};function w(a,b){var c=ia[b];if(null==c)return a[b];c=a[c];return void 0!==c?c:a[b]} .function x(a,b,c){if(b)a:{var d=a.split(".");a=1===d.length;var e=d[0],f;!a&&e in v?f=v:f=ea;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\0MX4YUS9\f[2].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	210
Entropy (8bit):	5.436915178303831
Encrypted:	false
SSDEEP:	6:tDpuPAtAGNNGjPLbIb7ALpV2jdcWaP0mjW:9pftAgTALpedTmq
MD5:	87CEE46DED232235CA4148FBEA3AC307
SHA1:	3619172E976D08E44CA0917BE259678D9771F609
SHA-256:	5A716656978AAEE538A9BB189C0D4B000D388AAEAA15427723B20710D8A98AC5
SHA-512:	CDF3148970E4E0F59D64C3AE3F04E09927FD376AB3DC6AB2FA04876E67664A73562AD8EF0B0BD45772AEF215DE8D43148698A4C956A58896A16BE7341D240AB
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
Preview:	_gfp_s_({"_cookies_":[{"_value_":"ID=e56d315663ea3c76-22b0e249c5c700e2:T=1620135589:RT=1620135589:S=ALNI_Mb3HA_1ETEXdPtDGNNg329xlt86Cw","_expires_":1653831589,"_path_":"/","_domain_":"localcoronavirus.com"}]});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\f[3].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	161534
Entropy (8bit):	5.464055852864097
Encrypted:	false
SSDEEP:	1536:FGWH+esk0tGzIff0neNonmbsafLNLIwtCJNnnY3vH8sogrDdyc6k2tEXb+fqmDO6:yQzIX0nXn5DnYR3dL6RFqmDOIEBxBVM
MD5:	9C6877C221C2B1FF9DC2CF1C6B22859A
SHA1:	D2186379C2DF201D480041B5FDEB5EA048D0EC60
SHA-256:	EA139025CE68B23127FA84E710D412E7851C3B62858DA72E53881793AAB56F9B
SHA-512:	9BF523A4CF60C632A1106291C3F42ABB333B518A3F0E1FB788F519E532223C9CEDCEF08D49E8CB77EB8A777FC12B3E15587C7C69829D8F94FF2C9817B077A51
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/pagead/js/r20210429/r20190131/reactive_library.js
Preview:	(function(sttc){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .var p;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 da(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 ea=da(this),fa="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),q={},ha={};function t(a,b){var c=ha[b];if(null==c)return a[b];c=a[c];return void 0!==c?c:a[b]} .function ia(a,b,c){if(b)a:{var d=a.split(".");a=1===d.length;var e=d[0],f;!a&&e in q?f=q:f=ea;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=fa&&"es6"===c?f[d]:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\feedback_grey600_24dp[1].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\0MX4YUS9\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
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\0MX4YUS9\fotonoticia_20210504113316_1024[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, 1024x670, frames 3
Category:	downloaded
Size (bytes):	62932
Entropy (8bit):	7.890400578548738
Encrypted:	false
SSDEEP:	1536:RvKrdsZl7xQzY5758CTsFxIgPBLiPmNBIK4dtKANqvb:1ezO24iYmNBOHqj
MD5:	EE3423047D3964A5A0F7458F91F045AC
SHA1:	79A414F0664475E3F66F29325FB223A48B29B89D
SHA-256:	B46444BEF2DF95B7F4B20A90C94E607F48DF9E849549BED7BF3950D4738F4485
SHA-512:	E1106F907AD6B336B9361B6BEE04EC1AF22F701B22AD8DBE22E9D747DE0F1FB8746AE9AD906242FD8B4CD2C1CD1F541AD5052CA77854986F60D371F98DFCE2D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img.europapress.es/fotoweb/fotonoticia_20210504113316_1024.jpg
Preview:	......JFIF.....``.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..b~.=(.....)(.s...A.~T.Z`;?O.?O.K@....?O..C.?O..?*J(.s.....?O.?O.(.....SH.....R.}?*u%....8...zc.1J.T..h.l.?*3...(.....?O....G.K._...\|...B..m.....Y.Z....U.X.....K.w..3 x.me =.y..7~..h7=..w=.{....$.O.|/s.X.~._.....?*3.....wV.).G.....4.....X....ip...9S.z.t....iv7Z...8#...z.....`c.nc..=...5.zM.....Z.7.S.f...B&WC.]...=s\.....l.3[.ly.d....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\fotonoticia_20210504113718_1024[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, 1024x560, frames 3
Category:	downloaded
Size (bytes):	73487
Entropy (8bit):	7.951173579378197
Encrypted:	false
SSDEEP:	1536:HZloZqCy5FGVu7qBbAx4Vl7Plw41emqjnchZEkWmueAFyooJLMc:4MCy50QqAx4oPlppNhZElbDFyRJLr
MD5:	DB0C3CF4823302D1DEF83D20B07B5F43
SHA1:	16D5C8E67550343DC2F5A94B85F537A6CC8DD757
SHA-256:	0B3B07A8BF3627B71D180B49307D09BC8BC512862709DB584BD5E20680ED33A9
SHA-512:	EE793A61B5F92C91AA845D306507E7AE30E81F2341B73572BB1351376B21566ADB4961C6C7557D3817D2C49B0F9CE302DC0D3A2BF9ECEA702EFA609F280D5FBF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img.europapress.es/fotoweb/fotonoticia_20210504113718_1024.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\fotonoticia_20210504113718_1024[1].jpg	
Preview:	......JFIF.....`.`.....C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222......0....".................... ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....?....{~T.>.9.4...d...I..E;.....~T.>.-.....~T.8..S.HzP../.I..".M"..I...2}.*v).P.I?.S.}.*..H..g>.F.p..G.*cL.0)Ih...a.dUi".>...E4....._.....U. .O...^.RK29...h.........U.<g.R)7...OU8?J<.. {..C...".&..u...V=..P`v84..G.(....G.N....P.P.)...kz...#{~U...>..0...K.o.......2C)...........G..#..r...).8a.)1.Q.g......>.!~z..Uq......q@.<..F...Ty........K....T].s.@./.?*ic.E74P!rq

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\fotonoticia_20210504121532_1024[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, 1024x1536, frames 3
Category:	downloaded
Size (bytes):	298411
Entropy (8bit):	7.979861151961286
Encrypted:	false
SSDEEP:	6144:DCJOCYzUVNkAXYb/II8ZyxlBaM/axdKZnROBY/sfc0Nj+BBjOZ:DMViMNkXjIlKWTcROG/McMj+TOZ
MD5:	E513A7641ED5A5658982F0EBA2804657
SHA1:	505ED048761136B0AAAE58DAE5B2461F7C77A22A
SHA-256:	2327EBA13E5540120D9C98F74581A8C3D5FA8CA282F1EA18D581FB99016CA07A
SHA-512:	3325C20E7AB03F74AC059CFFB7D41784438C7D6FBF168AA26BF031E615FE4B9E18C33DFE7D1022CB08B978454E4B751129330B43D1184131B60277AFD5E75BC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img.europapress.es/fotoweb/fotonoticia_20210504121532_1024.jpg
Preview:	......JFIF.....`.`......Photoshop 3.0.8BIM.......h..Z...%G...........@economia bolsa ibex 35 cotiza maximos anuales busca 9000 puntos .....5.....FIN..7..20200527..<..0000 00+0000..P..!Marta Fern.ndez Jara - Europa Pr..i.zEconom.a/Bolsa.- El Ibex 35 cotiza en m.ximos anuales y busca los 9.000 puntos, con un alza del 0,9% en la media sesi.n..n..Europa Press..s..Europa Press..x..27/05/2020 Puerta de entrada al edificio de la Bolsa de Madrid, el d.a en que el Ibex 35 ampliaba sus ganancias al 2,19% en la media sesi.n de este mi.rcoles, lo que le permit.a hacerse con la cota de los 7.100 puntos en una jornada marcada de nuevo por las tensiones entre Estados Unidos y China, los planes de reapertura econ.mica de distintos pa.ses, entre ellos Espa.a, y las noticias relacionadas con posibles vacunas para el Covid-19. En Madrid (Espa.a), a 27 de mayo de 2020...ECONOMIA ..Marta Fern.ndez Jara - Europa Press...!.........."$".$............

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\fotonoticia_20210504124210_1024[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, 1024x768, frames 3
Category:	downloaded
Size (bytes):	135924
Entropy (8bit):	7.978800297135593
Encrypted:	false
SSDEEP:	3072:M0vUDDz6pPQ7pfGaUyX5NzrMW3/VNKJ/JxoiozgRdahAt:M0vsQcGxyXbkeL8/JxoiomdeAt
MD5:	B11423B2E26746D93AD3039A238422E0
SHA1:	A0DE484AFA9FFD737FBF50FACED638E406B42F8A
SHA-256:	C823C6D030229127E5EB0992F09802C253297B3E497D255E8CC572780C476F3D
SHA-512:	24AD6068878B8C0D023FC34FAC5F20487EE5165A27C60EEB5D460443347457031F1D6A3D715F82AE1DB6615629EFC04C3753A5F0B5153FDB96AC15BE44143474
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img.europapress.es/fotoweb/fotonoticia_20210504124210_1024.jpg
Preview:	......JFIF.....`.`.....C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222...........".................... ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....?......C{....p.N>...o..I.3...>..8...<R*.0{..*]..h.?......J..QN4m...Fx...*.pJU.qPJ....co<s...o....}om0...u.YcW.. ..+PE..._......|.....DF....)..oc..>Y..n9.?*..5@.iljcPM...]......... R.s....x......"...\K.....XI.............%.B.......XqN..-.M.....k}...F+P....i2.@.L..Y.........[.+.6...8.....6W...Y.....J..[\.8....[..p...{....;....v..f...e6zz.(ib.....G....#..{m{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\httpErrorPagesScripts[1]	
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\0MX4YUS9\hv-TlzNxIFoO84YddZQ3KTdYVA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17504, version 1.1
Category:	downloaded
Size (bytes):	17504
Entropy (8bit):	7.963634538673749
Encrypted:	false
SSDEEP:	384:rVZ3Dxw0XUCyBFZOyfMrepchz6Yl6QOQGc:vO7CXjAYs5QZ
MD5:	96B6349F1F9D9C283DFA2BAB558107F0
SHA1:	302DD2CCCE155664207216B990DA9FBE6333AC11
SHA-256:	60F7288E67199372200CD3486AE493B921FC624C32233B2DA20FFB341ECF2768
SHA-512:	57B7E0A9A2AA9A998E591074883E45E3D41CF24D7A61C87BB6B84E18C32D03D790B3D5632D2BE39180A160B9B69C79867859E06FDB865ED2A62C87B289D6518
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/biryani/v6/hv-TlzNxIFoO84YddZQ3KTdYVA.woff
Preview:	wOFF.....D`.....yH.....GDEF..... ..."...xGPOS..... ... DvLuGSUB...../.....eOS/2.....L...`{..Icmap...<.....V.. .cvt .....I...d ...fpgm.....g...a.._.gasp..... ...glyf.....2W..[.1z.-head..<....6...6.?.$hhea..=.....$.0.mhmtx..=<.....g9$loca..?.....X.Atmaxp..@.... ... .D.yname..A.....H,.I.post..B.....}}d..prep..C....~.....la.x..... ....\}M.f.D0.e.%..\O>.....DFLT.....x..3Cpa.....k...F.m.....e755555...t.3w.{n<..N.a.b.....<...kiVm9.....0...../39.s._.....\|.....+.>.;.....X.Qdas..(...WP..y...c\...9.E. ...\..7.r.?..E.Y....R..\.kr]n...<&....!Miq..$...,...&'y...2o1<..vHA.n.z.....)..8.Ec..^k....g..b...5.....I'..7wF.<M.&.z.....:.2..N.R..".{.l.7.ru.x.c`f2g.``e``.....1...1.....D....4...^%!.....,L. ...&..l...)..V.....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.b..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\hv-TlzNxIFoO84Yddew1KTdYVA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17340, version 1.1
Category:	downloaded
Size (bytes):	17340
Entropy (8bit):	7.965169352792909
Encrypted:	false
SSDEEP:	384:jH5DimTKvxXtwwavipp/S6Zflar6nCiYA5IcPqTZt:1yvxXtwwaKpsO9iXScPqTZt
MD5:	D053AF7738508BE336B6EEF5F029F3DA
SHA1:	3B6005F31E20CEAA9FA2C76CB0F1C9484C3530F0
SHA-256:	372B9B889199C28126DD2426ACF59CFDADBE015FC18634689A6486ED1625ABC7
SHA-512:	1BAE74F5D2E7D0D25E885FB8E84C2A71E4242419A7EAAA0A19984CE69B03275B4CE1C786C826894FFF1DD3463E8176BD4796093C1A508002EDD121B1F357B54
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/biryani/v6/hv-TlzNxIFoO84Yddew1KTdYVA.woff
Preview:	wOFF.....C.....x.....GDEF..... ..."...xGPOS..... ... DvLuGSUB...../.....eOS/2.....M...`{..hcmap...@.....V.. .cvt .....I...d!..rfpgm... ...g...a.._.gasp..... ...glyf.....1...[$.B..head..<H...6...6.s..hhea..<.....$.b.Ehmtx..<.....k0.loca..>t.....MX6`maxp..@8... ... .A.wname..@X.....N..llpost..At.....}}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..$...,...&'y...2o1<..vHA.n.z.....)..8.Ec..^k....g..b...5.....I'..7wF.<M.&.z.....:.2..N.R..".{.l.7.ru.x.c`frcV``e``.b.```...q.F...@.....H.$?-....W I.%.o...K(..... 9&..o@.h...g.....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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\js[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	120080
Entropy (8bit):	5.543129599247584
Encrypted:	false
SSDEEP:	1536:BSJZ0eK9owZdVI0i+H7auo6Ni7QE12LsDjSdENQuSt81z9jKPfjGljAC2FSvOlH5:EJZ0eK9LZk0i4K9j8EZStlG58xFKx+
MD5:	E612BE6D7D1BE57E86A075326BD4263A
SHA1:	5D17A7B63B59195D582D006E12DDA8F8CC5B54C2
SHA-256:	10813E749A5F88A9D5B5597113AE336266C3B65238E71E3D5DFAC732C9D5C827
SHA-512:	9557FD9265BD3D39AE427854B80D105C28D939C97C795363F461F0EED72BE7A2EE4573891F4C5D4391F070BC60DB9E1905E86D3098C6CFFAB7A8D6279DA98A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagmanager.com/gtag/js?id=G-4HNKTZ3GH8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\js[1].js	
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"1",. . "macros":[{. "function":"__e". },{. "vtp_signal":1,. "function":"__c",. "vtp_value":1. },{. "function":"__c",. "vtp_value":"google.de". },{. "function":"__c",. "vtp_value":0. },{. "function":"__aev",. "vtp_varType":"URL",. "vtp_component":"IS_OUTBOUND",. "vtp_affiliatedDomains":["list"]. },{. "function":"__v",. "vtp_name":"gtm.triggers",. "vtp_dataLayerVersion":2,. "vtp_setDefaultValue":true,. "vtp_defaultValue":"". },{. "function":"__v",. "vtp_name":"gtm.elementId",. "vtp_dataLayerVersion":1. },{. "function":"__v",. "vtp_name":"gtm.elementClasses",. "vtp_dataLayerVersion":1. },{. "function":"__aev",. "vtp_varType":"URL",. "vtp_component":"URL_NO_FRAGMENT". },{. "function":"__aev",. "vtp_varType":"URL",.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\js[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	120103
Entropy (8bit):	5.543041004508416
Encrypted:	false
SSDEEP:	1536:BSJZ0eK9owZdVI0i+H74uo6Ni7QE12LsDjSdENQuSt81z9qKPfjGljAC2FSvOlHF:EJZ0eK9LZk0A4K9j8EZStuG58xFKz+
MD5:	76AD0A2A8E12EA04F493C2351D98ADC9
SHA1:	B8879140170AD074F12C9AB9709D7D187AA02BCC
SHA-256:	4AD3303B98D327E8C3955145FA6EEC22F488BB3867633C4B6ED594F15DA58057
SHA-512:	3343DC8A567A1BDC4D362183C54BB728B36CB44E9E1AEFCF1B361DFE737676253527D76C1E2FAC5DFADA5A7A34C5134A30C6293C27026B85FD9E8D331C2C72 5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagmanager.com/gtag/js?id=G-4HNKTZ3GH8&l=dataLayer&cx=c
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"1",. . "macros":[{. "function":"__e". },{. "vtp_signal":1,. "function":"__c",. "vtp_value":1. },{. "function":"__c",. "vtp_value":"google.de". },{. "function":"__c",. "vtp_value":0. },{. "function":"__aev",. "vtp_varType":"URL",. "vtp_component":"IS_OUTBOUND",. "vtp_affiliatedDomains":["list"]. },{. "function":"__v",. "vtp_name":"gtm.triggers",. "vtp_dataLayerVersion":2,. "vtp_setDefaultValue":true,. "vtp_defaultValue":"". },{. "function":"__v",. "vtp_name":"gtm.elementId",. "vtp_dataLayerVersion":1. },{. "function":"__v",. "vtp_name":"gtm.elementClasses",. "vtp_dataLayerVersion":1. },{. "function":"__aev",. "vtp_varType":"URL",. "vtp_component":"URL_NO_FRAGMENT". },{. "function":"__aev",. "vtp_varType":"URL",.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\layers[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):	66031
Entropy (8bit):	4.924868321474996
Encrypted:	false
SSDEEP:	384:ew45DokIn4Yb9k1pwjtoSRyrqqtXyezxfRNuqEYxVvUBAQhulzmkeHPRPF4ZD9wg:Oe8btR+jRe5b
MD5:	4A192124AB8A077D5AF731D63EF0BA88
SHA1:	11DA27D9A2FC225FC3FEF0B238F4A931451C5B9C
SHA-256:	90B749FE5655448C03FA19AEFA29DFAD2606C309DDAC206BFD9524711CAD94C2
SHA-512:	3965020D92EC43786AF5332375A6D1DBA7A6E7CB691BEC897C388147C08245193BABE4A930ABE5C97BE80CAC6504488642734D36B861D923F9796B09F14FADA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/css/layers.css
Preview:	.tp-caption.Twitter-Content a,.tp-caption.Twitter-Content a:visited{color:#0084b4!important}.tp-caption.Twitter-Content a:hover{color:#0084b4!important;text-decoration:underline!important}.tp-caption.medium_grey,.medium_grey{background-color:#888;border-style:none;border-width:0;color:#fff;font-family:Arial;font-size:20px;font-weight:700;line-height:20px;margin:0;padding:2px 4px;position:absolute;text-shadow:0 2px 5px rgba(0,0,0,.5);white-space:nowrap}.tp-caption.small_text,.small_text{border-style:none;border-width:0;color:#fff;font-family:Arial;font-size:14px;font-weight:700;line-height:20px;margin:0;position:absolute;text-shadow:0 2px 5px rgba(0,0,0,.5);white-space:nowrap}.tp-caption.medium_text,.medium_text{border-style:none;border-width:0;color:#fff;font-family:Arial;font-size:20px;font-weight:700;line-height:20px;margin:0;position:absolute;text-shadow:0 2px 5px rgba(0,0,0,.5);white-space:nowrap}.tp-caption.large_text,.large_text{border-style:none;border-width:0;color:#fff;font-fa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\mapa[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	21934
Entropy (8bit):	7.93330901879356
Encrypted:	false
SSDEEP:	384:GYNg7PUFdzUkAcKD0PVsltdILn1S5BWq6pKHDZ8yAoGfXV/o9Fs:GYybUFBUkAUqtdA1S/6pIDZ8yuf1ov
MD5:	4EFFF348E598BE63214650E32441B74B
SHA1:	7DA73A8AA4B2B2E69F6F6012822C451F9A139AFA
SHA-256:	989F66B9B767B198A838DAE7BA3BD449E9304B561141CB98302E0E9056AA301D
SHA-512:	C57B72A9E90038644E57400AAF147968B185A0CC7806A22D3C4BC0210C1F24116B0DE70F856BA93C7D7C6A155DC162A818F041591B74841F8F457041A4634A8C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/images/mapa.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\mapa[1].png	
Preview:	RIFF.U..WEBPVP8X....0.....ICCPH.....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.....,R eference Viewing Condition in IEC61966-2.1.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\modules.7225c79fe4e29708c611[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	224646
Entropy (8bit):	5.6624078063627366
Encrypted:	false
SSDEEP:	3072:AJEtPhhNHgwAU+DpElwHsHnMFNKbfli+/y6:EEtZhNHgwDSHHsHnMvKbAa6
MD5:	984CF1C2B2421205C097ACDAA5404F5F
SHA1:	25CE1EE04B378CF1F0797B50849402CBCFD368F2
SHA-256:	BB5824E55FB08D11D1BBCC144D776ACC19DDDF21298C684FF143C1B0CFD046AF
SHA-512:	DFB3D925C359058B5487ABAC98E66E66058230EB23F9FFD4B5BBEE3EC012BEC91ADFA13035769D8F866E7C6B104AB093F71C2650A328F4E3A908685E0C73FEF E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://script.hotjar.com/modules.7225c79fe4e29708c611.js
Preview:	!function(e){var t={};function n(i){if(t[i])return t[i].exports;var r=t[i]={i:i,l:!1,exports:{}};return e[i].call(r.exports,r,r.exports,n),r.l=!0,r.exports}n.m=e,n.c=t,n.d=function(e,t,i){n. o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:i})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag, {value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var i=Object.create(null);if(n.r(i),Object.defineProperty(i,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var r in e)n.d(i,r,function(t){return e[t]}.bind(null ,r));return i},n.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return n.d(t,"a",t),t},n.o=function(e,t){return Object.prototype.ha sOwnProperty.call(e,t)},n.p="",n(n.s=288)}({10:function(e,t,n){"use strict";n.d(t,"d",function(){return r}),n.d(t,"e",function(){r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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\0MX4YUS9\o-0bIpQoyXQa2RxT7-5B6Ryxs2E_6n1iPNHa5a7dvQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 10612, version 1.1
Category:	downloaded
Size (bytes):	10612
Entropy (8bit):	7.938455554680479
Encrypted:	false
SSDEEP:	192:0C4O2KXDBwUlVFdKZsFm6uxeOW5vfESQUOcJ+8OMfwyF98+Gpp1:UORBwSqCmzx/WpfEncA8h4gJi
MD5:	3C73EA4821E43477B4A2EC54D945B677
SHA1:	E854ADA0CDBC7A7E64D9F062A670EDA996CD89D2
SHA-256:	47B4AF9BD262AAD5CBD54D94E4FB36A3FA2CCF2B557762265BA0F671173B1039
SHA-512:	C6C9355597FF16D01DD22417A698B57C8708C263859A31B9FB7BC8DCD14C4D5B4D95B1AC5616E6F98E2362115E8CF0CA35797FE4D036AB9C194527BD307896A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/catamaran/v8/o-0bIpQoyXQa2RxT7-5B6Ryxs2E_6n1iPNHa5a7dvQ.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\o-0bIpQoyXQa2RxT7-5B6Ryxs2E_6n1iPNHa5a7dvQ[1].woff	
Preview:	wOFF.....)t.....E.....GDEF...l...4...F....GPOS..... ... DvLuGSUB..... ... .OS/2.....O...`g...STAT...0...&...*y.l.cmap...X...^.....+.Agasp.....glyf..... ...9. ....head..$D...6...6.#..hhea..$|.....$....hmtx..$.....#..loca..&l.....)../maxp..(..... ....name..(8.....p<.[~post..)X..... ...2prep..)l.....h...x.....@...y.....f]c..F..&.\c..Zc.q .8]....'~].!.....DFLT.....taml..tml2.....x.c`argna`e``.b.```...q.F...H...A.$...D..3.``P.e.....IF..a2H..).. .....@...x.c`.B. f`...2.L...% &....b.dna`..,.....x.....m. w.5f{...m.mM.m.C.\|;...;.@(.E.....5....*.....l....ObB.4.=..0.q.%....".."A..N00.\ 22Sd..$.@9...N.#.q.u.|.ch..9...l`...CH...$.41G!f.1..)A.....o~..\|.....<...z<..l..cO...U..].]_..kB.....t.F[l ..)..... w.Z.l..v..U..{..@.U.Zd.%.z..[...yn.....K...k.[...:...i..^z.~.h.....d.&Z.b.a..a.6Z.l....n...i.(....\.....x..{.`.G.....bYZ.k..$[f.c....,$...B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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):	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\0MX4YUS9\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\0MX4YUS9\pixel[3].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\0MX4YUS9\s[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	143
Entropy (8bit):	5.079318363208902
Encrypted:	false
SSDEEP:	3:PIy9JL/ZSGKHjJMzVJu+1vK3VYrSLIzECAXhxMAFjWAEtv0Gb:TJL/sGeMRJVSOGLIoDXhxVFjWAEd0Gb
MD5:	E4E31B474D3E0B577B3C8856E91F8659

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\s[1].htm	
SHA1:	A81311F7FCFA9B6B23A24D4E5C976D5F75B1B9B7
SHA-256:	18088C10E79C926292732AF98A0CE470E90F3FBCBA4BB4896AB3310C2D94E421
SHA-512:	A07961EB39C4CD4E39EE19E2C675E64E5BA5367DAA18E2F76A23772ABD62F46B002E6BE8FB0F35A70616941178FACC8DF579C4A68E5811B74313C12806AAFAE3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/drt/s?v=r20120211
Preview:	<!DOCTYPE HTML PUBLIC>.<html>. <head>. <meta http-equiv="refresh" content="0;url=https://www.google.com/pagead/drt/ui" />. </head>.</html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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\0MX4YUS9\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):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CUnl/7yltxlHh/:/+/
MD5:	07FFF40B5DD495ACA2AC4E1C3FBC60AA
SHA1:	E8AC224BA9EE97E87670ED6F3A2F0128B7AF9FE4
SHA-256:	A065920DF8CC4016D67C3A464BE90099C9D28FFE7C9E6EE3A18F257EFC58CBD7
SHA-512:	49B8DAF1F5BA868BC8C6B224C787A75025CA36513EF8633D1D8F34E48EE0B578F466FCC104A7BED553404DDC5F9FAFF3FEF5F894B31CD57F32245E550FAD65A
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\teruel_buj-k0zG--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 52x52, segment length 16, baseline, precision 8, 1024x512, frames 3
Category:	downloaded
Size (bytes):	104949
Entropy (8bit):	7.970860238294036
Encrypted:	false
SSDEEP:	3072:WBjjqs3z0e+hnqDyhyfsJalcstl5xR+KtvNxerl14w:Gjjqs3zIhGxskf5GKtHeP4w
MD5:	10E39D05DDFA0CA5DC9C3781D94A79D8
SHA1:	3FBA49949531FDAF2D3D4C1A831931426EB41D8B
SHA-256:	054A1E881423B858BF5FCAAA676FE6D2AB0BA38111B77EE6EB4163834C6FE31B
SHA-512:	7DCDF4C8028C8E2FADF6E8E171433BB435C519F06D186DBDE4E177D03AC4B43E21F605BC73E9DF221248F29A1E3DD65F9D5ABD70DDADCA200793D70C92D927D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static1.abc.es/media/espana/2021/05/04/teruel_buj-k0zG--1024x512@abc.JPG

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\teruel_buj-k0zG--1024x512@abc[1].jpg	
Preview:	......JFIF.....4.4.....,Photoshop 3.0.8BIM.....4.....4.....C.....C....."..... .....Q.....!.1."AQ..aq2...#BR..3b..$CTr...4...%DSc..s..&'56Edt.....1.....!1.."A.2Q.#3aB.$q..C.....?.o]u4...H5..@*..B.. ..G;.C.....*.Q.3RDX.\m.5...HY.b..i.c.VN3RC....$...\85i .%....<.!*1e%i..{T.B...9g..*'..y3J8'.o..G..=y..*..!.}.4.J.#..=..).... ...hi4...P. ..M!..Q.\R`.h....n..9....;;sH@.IU....:.z U....`.1*.8..b...Fk.i.0*....]H. ..$../mt.R".....m.B...%I*.....1.....x....lw..?.K.U.....8Uh[.D..k.*...S.....N..|..7...L..qd.k...c.K..N)$...j....5HN3I..&?3K$/.b..J[Z...(p.7.Ez....F&..%Ra..${.*..t. (aB.C.....&..!.M`.....f..1.{..B.}(.....#....\O.....HR...aJ.":.....&..5G/.....=...)..b0h.A....0.x.IIzZP;...|..L:~.....4Q..}.#.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\vacuna[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	14850
Entropy (8bit):	7.858595309515447
Encrypted:	false
SSDEEP:	384:WYNg7Gs2r91S/AV3ilK+jXM6abHkCLzGOF2icmCAz:WYyv2rR3ilF0jkC/h9hL
MD5:	A5625AF26352BD61722B540E8E2CCEFF
SHA1:	A4FC573926444906FDF5D16204C750E546055D83
SHA-256:	B1A25B4978F30C3AD77685EED888B20268017851713F6D07EA1A441B3125FEDE
SHA-512:	237692AD7D378DD68075500F7D4F60E7A315713F1724135B63128ED415146AB2B3F2270D145D6A46ED76CFFB7DF2932E127864A5A507C5967FA1C1494AA53D6B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/images/vacuna.png
Preview:	RIFF.9..WEBPVP8X....0.....ICCPH.....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.....,R eference Viewing Condition in IEC61966-2.1.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\vacunas-completas[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	17934
Entropy (8bit):	7.907375826406186
Encrypted:	false
SSDEEP:	384:PYNg7sr9LBJ5DblzFTI1PAs3WDoTok7QxbWPccqRO0TrnzGAPzXMgBz:PYywrtBT557fDu78bChqRNvzxMgBz
MD5:	6C6F2A81E0380408078FD5BB9358DB06
SHA1:	50E4DC47334FD162320FEF6E2EABE8CF4B3B85C0
SHA-256:	50451B89AA22C5AB1092F5499DA22AAF57C1E2FC6C98086FA3D124750DE54067
SHA-512:	09E9EF496D5C2C70EAC8422C34E3D583CDC95865CCACB581807C2B0C1BD2CD0920993CCF9F8185C9D78058340D1DBDC94DED9DA5B7716533686D07B3F7398 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/images/vacunas-completas.png
Preview:	RIFF.F..WEBPVP8X....0.....ICCPH.....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.....,R eference Viewing Condition in IEC61966-2.1.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\zrt_lookup[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):	10289
Entropy (8bit):	5.476565958835486
Encrypted:	false
SSDEEP:	192:28d3tZlVcwxkGOxn/CP00/Y7CPcy4j18a2fDaIT7E:2ktpY6PT0CPcF132fDaITA
MD5:	063C53466924D2BD0F9A0D57F098A66B
SHA1:	0F3F95456E019D0F958C1103E61B71A1097D1F49
SHA-256:	A5CB642EF22434A24612329870579FBB272CB9FA7475360035596EA56FB0431A
SHA-512:	1B24A9AA3A7B1E08D45E2DA9E34059DBA2E2AEF3A59F14DC1214BFAF72E4C138EEC81ACD38FF6480EE944055629BBC194D1923C5E497AF4F183FBDBE52CA78 53
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/html/r20210429/r20190131/zrt_lookup.html

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\zrt_lookup[1].htm

Preview:	<!DOCTYPE html><html><head></head><body><script>.(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var aa="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 ba(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 ca=ba(this);.function da(a,b){if(b)a:{var c=ca;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&&aa(c,a,{configurable:!0,writable:!0,value:b})}}da("Array.prototype.find",function(a){return a?a:function(b,c){a:{var d=this;d instanceof String&&(d=String(d));for(var e=d.length,f=0;f<e;f++){var g=d[f];if(b.call(c,g,f,d)){b=g;break a}}b=void 0}return

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\3c073c1e-6442-44d7-9344-5d30b1589d28_facebook-watermarked-aspect-ratio_default_0[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=6, orientation=upper-left, xresolution=86, yresolution=94, resolutionunit=2], baseline, precision 8, 1200x628, frames 3
Category:	downloaded
Size (bytes):	170831
Entropy (8bit):	7.9764674767158805
Encrypted:	false
SSDEEP:	3072:JfEkQZTje/CxaiY4MbH5xCnrEnu4hLzGq+lt7ZzykDb9y0UjpW14lwCVat4:NCxSARYLbZxG4u45zGqELrVyGQw/t4
MD5:	5A247EE33E8306EB1BB00DFDBCCE9D5C
SHA1:	19BC96CE262E66F39AB89CBBCDD72FB3D462D2A4
SHA-256:	C31B65E6836488390FD88A740CDC0336C2C81B150C213B012C0B4CE944E85AF5
SHA-512:	66F8A6C15FCF1BE9D41CD393F856CF6C2B1963A022A03B3393CD6116D3C33FE0148453C0A9F96A706374024C55CE53C739A5868C46374A4A2904967A15C8CDA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.eldiario.es/clip/3c073c1e-6442-44d7-9344-5d30b1589d28_facebook-watermarked-aspect-ratio_default_0.jpg
Preview:	......JFIF.............Exif..II*..........................V..........^...(.......................i.......f......./......./................0210...................0100...............................t.........C.................................... .%...#... , #&')*)..-0-(0%()(...C..........(...((......t...."......................................^.........................!1.."AQa2q.......#B..3R....$br4C......%Ss... &57DTct...6Ud...8F..'Vu..............................4......................!.1A."Q.2aq..B....#R....$3.b...........?....R9O...d`Hv..8.*E.J...?.9...0....g..$.,.-.KY...F.....K9......c#.5...Z./k..^.n. ...0hkk.v.0..........g..@.x..x..W..6....9.....k.Z........z..e.28.5{oi>.w%......<...:..,.F.%.V..".B..du.....j...._...sF.....VX...4&....L....`.1.:...K$~.`....2....G.R..w.e{. =R`.~y....8.^..C) .>.M.G8.+..k?z:_.$...S..$C.o.......+..]..q.f...sRQY.$~"Yr.#.S.iv..?.......7.tA...(7....ns....-..i....t.\..r....t..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\466606[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):	42
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEy:1QEoy
MD5:	D89746888DA2D9510B64A9F031EAECD5
SHA1:	D5FCEB6532643D0D84FFE09C40C481ECDF59E15A
SHA-256:	EF1955AE757C8B966C83248350331BD3A30F658CED11F387F8EBF05AB3368629
SHA-512:	D5DA26B5D496EDB0221DF1A4057A8B0285D15592A8F8DC7016A294DF37ED335F3FDE6A2252962E0DF38B62847F8B771463A0124EF3F84299F262ED9D9D3CEE4
Malicious:	false
Reputation:	low
Preview:	GIF89a............!.......,..........D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\4UaGrENHsxJlGDuGo1OIlL3Owpg[1].woff

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26228, version 1.1
Category:	downloaded
Size (bytes):	26228
Entropy (8bit):	7.98323449413518
Encrypted:	false
SSDEEP:	768:DBOEuz6T0146JY/J6unqhOYK0GJenzOoyo6:DBHuea4j/vnqo304enzUo6
MD5:	6DD4AD69D53830BDF5232A13482BD50D
SHA1:	6FFF1079D7E5D02A2259CB5D7833E790239E01CF
SHA-256:	5CE48D9E9D748AD4686094D3CC33F5AE1E272A5B618F5C6D146C4D12EF02E4A6
SHA-512:	FC91E8C4EAE384D38667E330C5A5E4BF82EBAC9A23AB88439D7C22CCDD125DE7F1371DD953F18DEE60EF68B680DF49A32F684157D90F20E1DAC3BFFC9DF84 18
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/googlesans/v27/4UaGrENHsxJlGDuGo1OIlL3Owpg.woff
Preview:	wOFF......ft.......`........................GDEF.......\.......RGPOS.......#..+..P.LGSUB................OS/2.......U...`h...cmap...........~n..cvt ....y........fpgm...$.......uo..gasp................glyf.... ..=...m..N..head..Z....6...6..'.hhea..[.... ...$.0.6hmtx..[<........})9loca..]....z.....&..maxp..`p... ... .>..name..`........r.i6Ppost..a<........O...prep..e....p..... ..x.U....Q.F..=#.`ZD.@@<..... "...Zp....+.c.f...).>Z.bm.Om..?...\\.zi.f.^b...[y/.........x..Z.......%......033333333...e....r......U..u.r.....sV..Z..^..c..>v..p7.x...w.i...Y.....X...N<.k...0...kc];.u......4.j...@....y."......,....#.;...... ....9...1....q..b..c...{....i2.H..g..:.....du.FX.].w3...{y...G....E.....~..RdX.|.\..U.^.x!....e.|.:.RX.Wxg.*...&.5....2n.Q...5.{..2....Ia.Vb%....:.Yn..QI.Z...x..Z.6..?........G..W.*^#.e..#|l2p.S+.?'. <E..<....M.H..".>..d....>n%.(..."....<"........U/z.%..=...Le.cL3.4..4..znxgX!JD%.....s....&.a..z1._....O+..g.dm.?.9Vj.1...B...8..S........ ._.E..... .[#_..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\4UabrENHsxJlGDuGo1OIlLU94YtzCwA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26464, version 1.1
Category:	downloaded
Size (bytes):	26464
Entropy (8bit):	7.981932066790926
Encrypted:	false
SSDEEP:	768:OIYb4Auz6mM1gBEL1WuL1BU91c6HJ8Y4mAS:OI84AueNmwHpBU91qY4m7
MD5:	08F80DE0ACF68D82AABAB974A47D9E5F
SHA1:	E6F1C0F5395A9C297AA162468961C1FAF0EC1ED9
SHA-256:	4070911A1BB9CC52C4E4CD5E85CA186DCDE89308A0517A8FAA4715C2E0A9D45E
SHA-512:	720DE47FDDA648AF7CE5F3F574EFA3322191C4D0001E31181739D65FFE0CCECED56635AF58E5E828072A17EEE1ED1E318AF467B8ED7F4185EE0F5155501CD8D 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/googlesans/v27/4UabrENHsxJlGDuGo1OIlLU94YtzCwA.woff
Preview:	wOFF......g`.......d........................GDEF.......q........GPOS.......$..+..K.MGSUB................OS/2.......U...`i`..cmap...........~n..cvt ....fpgm...T.......uo..gasp................glyf...(..>W..mNU!.)head..[....6...6..'.hhea..[.... ...$...4hmtx..[..........1'jloca..^....~......t.maxp..a.... ... .name..a4.......V..4.post..a.........O...prep..e........^....x.D...Q...3..I.=D.@@....@... ..''...}......`.%.....x.........umW...g.WwO.....J..^?.Jci^N{.Nr..Jw@.n(.....t4....i...x..Z...6.=r..............q`.>....m.....fy.g..y4N...tAg..''KWWW.j.....8...n.3..:..1....9.+.}...b]....0..6V..).G.r... .....N...,R(.o.t.LU....;.{.l.y....i..w.{F..;p'.....,.........:3...|..,.`pGPAV.?....q!......=.(cn.'<......sK_...]..U.W.......b....E|.o..Jp.n.uX....*J.q'SFy...l..Cd..XZ..RP...#.w...C)..s../..D..1.G...Sx ...e.....x.o.mJ...~./L..r...Y..sD./.......>$R`..&.v......D..w.). .f.Y.''<..V/.zQ{.8./...X*................B..Jp#%.7.e>+L.Q.1..hd..k._...f..u....+....Q...N..\|....$Lv.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\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
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\2K7JPOQS\92e68fdb-8c43-4c6c-9f2a-e983059bdab4_16-9-aspect-ratio_default_0[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 880x495, frames 3
Category:	downloaded
Size (bytes):	54994
Entropy (8bit):	7.9799374883503615
Encrypted:	false
SSDEEP:	768:ZF9hZlAQRsO6qVTWlz4cOcXNVhZeatn2zpvbaxZ1a/WHRfCfaFBu8lZ7H:/DZae28cOKNVhU6ncpkDSWH5KL8lhH
MD5:	EBBA2F237E9B71F57FA8A386234C67A9
SHA1:	958C79874AA4182E33ADD1E65F58129168A0AFB2
SHA-256:	FFC03FBACA7E65C64B2891FCC5062EAC18610EC4C4AB7F99A1054EBE61349C16
SHA-512:	F4596391196C91A00EB10299B22BEFA51F0E4577DFB631B8C60B3DC3BF6E8905A8EE0D859232BC32B1B155FBC99DADD74DD393827E1387C56DFDFF8C264E44D D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://estaticos-cdn.elperiodico.com/clip/92e68fdb-8c43-4c6c-9f2a-e983059bdab4_16-9-aspect-ratio_default_0.jpg
Preview:	.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((........p..''...J.........................!1.AQa."q.2. ..#BR....3b..$CSr...4DT.%U....5cs.6...............................*......................!.1..AQ."a.2..$BR.............?...m.F.....@...P4........%..5Gd.6J.P5J.@.....PrP.j........A.....~.o...9Z.=...... .d.XWl=8..?.......5.....^..u.9......TVXtsB0.....TM....@..[...J..%j....4...SB..z&.P.J5K...]...L..Q_.x\..+G.W.D..Q......9...N..q..$o.k...M..b$....un..Q..uM?WV.;..h...O..7.^*..7.Tg.3. .!.^..P....=&..G..H}.w.[..)e..^.E..&F;B.P...../......JCR.`.......1..fL".Ag..o.)........../T..p.7.`.Qd.!.H..B..g.......n..-......r...'..5..=U.c-u.V...G...Ulw.L.pN,2x~...6'..].j..$....)......r.&..E.QH} ..Hyn.n.U!.....a.....Y...%..=.9 ...#.M..T!..W*..D0..L_.N.4...;{Dv?h$.q!....O....J...W4.............es..X...l.<..{..J&..scsr8.=.E...C........*)[US+.QQ.k@......

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\Linkedin_local_coronavirus[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 240 x 240, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	8490
Entropy (8bit):	7.8374960513554734
Encrypted:	false
SSDEEP:	192:4dgy7F8kn2UUU3XY9ItI5rhKcmhot/N2u6zd1IwFy20Yb9Xck6CAsPoOw2FEKIo+:uvNnf8D5scmQ/4ucWS06pck8sPUumz
MD5:	670E81FF5535F02CF68C7DBEAE9DB63A
SHA1:	3D64392FD3CC3AEE67D0ABFF1C408F8C6F175B63
SHA-256:	0690916EEBD0789A828A8119952B6AC354FE3C025EAF4141E1F991CEE2FAB2B6
SHA-512:	67D156F9E7C708BD27E96FA48492615CAE9B6ACE6C6E690DD62A72B9359A4FD0C88B39D718F7CD51BFD474F3D1464A563513C486C0CB079E24BC460307A73C C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/images/Linkedin_local_coronavirus.png
Preview:	.PNG.....IHDR.....>U....&iCCPAdobe RGB (1998)..(.c``2ptqre.``..+).rwR...R`?.....> v^~^*...v...D_....@..J.(*.....(%.8...../)..3...E..... vQH.3.}...K.....I..... ..H}: ....6....KR+@.28..T.e.g.(.ZZZ*8..'.*.W.....+x.%.....%.....B.....j..d.2.....9....bg.b..\ZT.e22...#.#.....B...a.....T...!...>..9...O..:6\....pHYs.....+.....iTXtXML:com.adobe.xmp..... <?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns: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:dc="http://p url.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xa p/1.0/sType/ResourceEvent#" xmp:CreatorTool="Adobe Photoshop CC 2018 (Windows)" xmp:CreateDate="2020-08-24T14:35:41+02:00" xmp:Modi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\a204a622610ec42c29322584ae03f5a9[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	10849
Entropy (8bit):	5.358225618041609
Encrypted:	false
SSDEEP:	192:5jR1UkBh0Cwk+hsPkj2JQfQ1k1yh2G1dfVDmhXrY:fbBh0CF+2sj2J251yh2G1dfKU
MD5:	A204A622610EC42C29322584AE03F5A9
SHA1:	AFFBEE57273CDE6123915D0453691A7FB44B565A
SHA-256:	234C9972689E21B21FCCC3822935C68AF190B86B75F565060D346169AD8E4A42
SHA-512:	0EDC8EB5BCF4253924056F326015E4FB6B1EF0E6BF707752A68348F4D103B0D3452D2F68A435382CE73F3AEE8164B570122EF3533EE7FC5D63D6EAB363382028
Malicious:	false
Reputation:	low
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';function aa(a){var b=0;return function(){return b<a.length?{d one:!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 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 l=ca(this);function da(a,b){if(b)a:{var c=l;a=a.split(".");for(var e=0;e<a.length-1;e++){var k=a[e];if(!(k in c))break a;c=c[k]}a=a[a.length-1];e=c[a];b=b(e);b!=e&&null!=b&&ba(c,a,{configurable:!0,writable:!0 ,value:b})}}.function n(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:aa(a)}}var ea="function"==typeof Objec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\a204a622610ec42c29322584ae03f5a9[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10849
Entropy (8bit):	5.358225618041609
Encrypted:	false
SSDEEP:	192:5jR1UkBh0Cwk+hsPkj2JQfQ1k1yh2G1dfVDmhXrY:fbBh0CF+2sj2J251yh2G1dfKU
MD5:	A204A622610EC42C29322584AE03F5A9
SHA1:	AFFBEE57273CDE6123915D0453691A7FB44B565A
SHA-256:	234C9972689E21B21FCCC3822935C68AF190B86B75F565060D346169AD8E4A42
SHA-512:	0EDC8EB5BCF4253924056F326015E4FB6B1EF0E6BF707752A68348F4D103B0D3452D2F68A435382CE73F3AEE8164B570122EF3533EE7FC5D63D6EAB363382028
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/mysidia/a204a622610ec42c29322584ae03f5a9.js?tag=client_fast_engine
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';function aa(a){var b=0;return function(){return b<a.length?{d one:!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 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 l=ca(this);function da(a,b){if(b)a:{var c=l;a=a.split(".");for(var e=0;e<a.length-1;e++){var k=a[e];if(!(k in c))break a;c=c[k]}a=a[a.length-1];e=c[a];b=b(e);b!=e&&null!=b&&ba(c,a,{configurable:!0,writable:!0 ,value:b})}}.function n(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:aa(a)}}var ea="function"==typeof Objec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\activeview[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\activeview[1].gif	
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	42
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEy:1QEoy
MD5:	D89746888DA2D9510B64A9F031EAECD5
SHA1:	D5FCEB6532643D0D84FFE09C40C481ECDF59E15A
SHA-256:	EF1955AE757C8B966C83248350331BD3A30F658CED11F387F8EBF05AB3368629
SHA-512:	D5DA26B5D496EDB0221DF1A4057A8B0285D15592A8F8DC7016A294DF37ED335F3FDE6A2252962E0DF38B62847F8B771463A0124EF3F84299F262ED9D9D3CEE4
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\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):	83686
Entropy (8bit):	6.065166095461158
Encrypted:	false
SSDEEP:	768:XVxGrhUZ1/MpxRoDGT+ahaN5XBnvuWGrcHBVgeGR1xhwmv9iCZA:WrhOuRoDGTHaN5XwWG0V4xhBY
MD5:	EF4E19537D78EB2BDB85A03758B4FBDF
SHA1:	00670F6FEEC959DDB4269E8C3E8DD7F1793380C5
SHA-256:	643D4D62CE802021A4438932633D83E755DD0397FA461BEC8BC81B3A7E6A49F0
SHA-512:	CC06EDC2152D868A0DDF32997DBD33CCD29FC62759221DD0F8206D24280F1D5F4AA88F2573B99948E5C2AF2D9DC2194304F703623C62626668336647B9CD195
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&h=280&adk=3209531498&adf=3684499108&pi=t.aa~a.810924589~rp.4&w=1140&fwrn=4&fwrnh=100&lmt=1620168014&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=1620168012311&bpp=40&bdt=1689&idt=1341&shv=r20210429&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3De56d315663ea3c76-22b0e249c5c700e2%3AT%3D1620135589%3ART%3D1620135589%3AS%3DALNI_Mb3HA_1ETEXdPtDGNNg329xlt86Cw&prev_fmts=0x0&nras=2&correlator=2836834130781&frm=20&pv=1&ga_vid=1292693962.1620167988&ga_sid=1620168014&ga_hid=1641196723&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=62&ady=297&biw=1280&bih=906&scr_x=0&scr_y=0&eid=31060932&oid=3&pvsid=96816254938719&pem=804&eae=0&fc=1920&docm=11&brdim=0%2C86%2C0%2C86%2C1280%2C%2C1280%2C906%2C1280%2C906&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=128&bc=1&ifi=2&uci=a!2&xpc=m3AOUMCnYB&p=https%3A//localcoronavirus.com&dtd=2329
Preview:	<!DOCTYPE html><html lang=fr><head><meta charset="UTF-8"><link rel="preload" href="https://www.gstatic.com/mysidia/a204a622610ec42c29322584ae03f5a9.js?tag=client_fast_engine" as="script"><script>var jscVersion = 'r20210429';</script><script>var google_casm=[];</script><script src="https://www.gstatic.com/mysidia/f27a2327937451811f326a3c5359709a.js?tag=pingback"></script><script>mys.pingback.init("CL6tyb6TsPACFcTK1QodnMMFmQ", [4,1],"text/vanilla_rda", {2:"server",1:"banner-large-eta-vanilla",4:"mysidia_upscale,mysidia_analytics"},3);</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{f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\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\2K7JPOQS\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:$scope.formData,gcapcha:document.getElementById("g-recaptcha-response").value,pageId:'contactUs'}),headers:{'Content-Type':'application/x-www-form-urlencoded'}}).success(function(data){$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\2K7JPOQS\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+KSIEhYAPl641: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\2K7JPOQS\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\box-5e3cec51ed8e99df6977c199d27812d7[1].htm	
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\2K7JPOQS\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:	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:	30BE2E73020EB97A67709E47DED40E999D352DA9B94EDD946D1315BDA65AD616AAA3CDFCFA675D061E4ED4AE1BAE3F0D245908D44411B2425C49B4345D2F6607
Malicious:	false
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\2K7JPOQS\coronavirus_mapa_localcoronavirus_slide_3[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 17:27:09], baseline, precision 8, 1920x300, frames 3
Category:	downloaded
Size (bytes):	84131
Entropy (8bit):	7.847414150702969
Encrypted:	false
SSDEEP:	1536:eD8k8OVfccqnoorJc1lqXC0vs6DA+xRKAxT9Pel8WrLxS6u:G8k8OV0Joot4lqvDA+XZHeJLxVu
MD5:	6B957D0A41483602A8F926562EB80B17
SHA1:	28ED326ADCBC3D7ABEDDE9EC00B84C1CFA46069B
SHA-256:	CABD93289026981BE19140A1038D341069B26872C4887E8A75461B8DA9BAC2FA
SHA-512:	64987322B87C0DE7264DC6695006C05B6C4104F4BAD0647B2081B386BC6B5A3FAB77D4641FE5960F5F1D307DBEA663930548E774573C91BC0DC4E962BF606EA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/images/coronavirus_mapa_localcoronavirus_slide_3.jpg
Preview:	.....Exif..MM.*.....b.....j.(.....1....."...r.2.....i.....-....'..-....'.Adobe Photoshop CC 2018 (Windows).2020:03:11 17:27:09.....,.....".....*.(.....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.....?.o...6..c..e.@...O.V?..g.N.....C.}..;{.[.dh.`...zv.".9-....V.qc.._..xl...g"}.~..1....f....k..k. ...i..\.....K.[.V>5..0.X.....}Zq...}...1uu.....?L.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	533
Entropy (8bit):	5.101982741986593
Encrypted:	false
SSDEEP:	12:jF/iO6ZN6pixsiJqF/iO6ZRoT6pixUEqF/iO6ZN76pixQvJY:5/iOYNNxsl/iOYsNxUv/iOYN7Nxn
MD5:	72DA71EACAE9E595F0429770C533F3E7
SHA1:	A4BB90C015F7C573F2B989490E1362412B9194AA
SHA-256:	00F13F954125777E8A26FD0E9F6BC730D763E9E59DCFB54D240602665B9B1B43
SHA-512:	EFD365A575C5DB8B1E225BB82B964DC3FC3D8FB1B8A4102160226662O1136305E06AFD8FC7FA95CCD4DE5EC3953A32677C7381323FA5C6E8E3BB74F974119E9
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\css[1].css	
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Roboto%3A300%2C400%2C700
Preview:	@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmSU5fBBc-.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\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.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\2K7JPOQS\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, 100x100, frames 3
Category:	downloaded
Size (bytes):	1911
Entropy (8bit):	7.621947858534851
Encrypted:	false
SSDEEP:	48:rwcwFCxCMVs7nz6uQEHt9AjuvedyeFb/SYHSfy/yfrCkq:joMu7nzVN9AKmdyqOYH7/Y+
MD5:	BA71F81377F6E06BD4864CAF64A16AD9
SHA1:	E7429A18496DABB8B73CA9AD30C4B7E49F787F59
SHA-256:	8BFF9EC3A2C218DB516F668F50F0B70958136D28892DC840BC0544A20EF7D61B
SHA-512:	7BEB75F7784ECC3625835B897D5B99B78EDFEB916094A0871A75EAB3BA5952325481E01DC5C9DF29014CDE3129397E0FAAF5F6285E0B3BC3ECAFE056807D844 5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/6525030626783894 69/downsize_200k_v1?w=100&h=100
Preview:	......JFIF..... ."" ...$(4,$&1'..-=-157:::#+?D?8C49:7.....7%.%7777777777777777777777777777777777777777777777777777.....d.d..... .....;.....!..1Aa..2."#7Qqst....Br.46bu.....?..h.....@.P(.....@.P(.....@.P(.....@.P(.....@.P(.....@.....f.J...I..(=.(...W.u.m.no..... .'..uZ.....R.....w.w..vr.....wH..(.c9Q....q<j.....;'.mR.oG.. ....,Rznr.79.,=.s.^t...yC(.).P.....pI....@.....+B.[JRH.#...2.....(q..~F...g.g..B.J\t..9.(.Nq..P^<..7.....J5.....G. 6N=W.....d....p...T.+@Q...@..>?.B...|.M.Z..F.?.*..xm...Z.v..e..O....Y.|.....*.x....mWVV.-{..q...QA.. x.A.....!.#...H.%).....I_.b...W9O.....Hl....e....dy..p....~..:....p.....@..... .'P.G...P.m..)..VR.{.A.|Q.B.~-_....;.v~.F..y2...N3Ek8R..:u$..g.z...[..x.....G.....!....4...=.V..$1.....].7.../.8y.[Dm..Dk.t....Zz./..'c.'c..o.^..%{=....8C..n.J...A..!.....}...QJ.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\ee0f5b345291fc213580710563fb55f7[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	4162
Entropy (8bit):	5.283638943120527
Encrypted:	false
SSDEEP:	48:CWHNhVzMvI0PaaNKPoTA4K0hi1t7RC7f4rL/SwjQ27cGVGbzoRGbzrc8Vj9uSdXd:PtT0I0SBPoE6+KQgGQFrc8VjdXd
MD5:	EE0F5B345291FC213580710563FB55F7
SHA1:	269368CF056671CADBE3535DC9107D5C8EE3A825
SHA-256:	3344DE4BD1802BC3AB6C1CC0CCA7B028FE0F501C03BD3620F813DFB6F80DBB40
SHA-512:	88770870B110717FA47287CFA781E9E0CF9C9211680E8FD4B9CD9E7B73D351FAE1B36949F5C92074FCB300FAA5F732F35301D8F943805029520EF325667B472A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/mysidia/ee0f5b345291fc213580710563fb55f7.js?tag=analytics_pingback

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\ee0f5b345291fc213580710563fb55f7[1].js	
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';var d="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},f;if("function"==typeof Object.setPrototypeOf)f=Object.setPrototypeOf;else{var g;a:{var k={a:!0},l={};try{l.__proto__=k;g=l.a;break a}catch(a){}g=!1}f=g?function(a,b){a.__proto__=b;if(a.__proto__!==b)throw new TypeError(a+" is not extensible");return a}:null}var m=f;function p(){}p.prototype.j=function(){};function q(a){var b;null===(b=window.AFMA_Communicator)||void 0===b?void 0:b.addEventListener("onshow",a)};function r(){this.g=!(!window.mys||!window.mys.pingback)}r.prototype.setAttribute=function(a,b){this.g&&window.mys.pingback.setAttribute(a,b)};r.prototype.setData=function(a,b){this.g&&window.mys.pingback.setData(a,b,4)};r.prototype.send=function(a){this.g&&window.mys.pingback.send(a)};var x=["googqscp","osdlfm"];.function y(){var a=this;this.g=new r;this.s=this.o.bi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	135276
Entropy (8bit):	5.559974423342489
Encrypted:	false
SSDEEP:	3072:H5kfO59PvOi0TNe8MEvirRPuQ7lDURW6a:dnshMEvANj7lIRW6a
MD5:	4D85A52F96B7F21C56292C2C9C9C6A23
SHA1:	37985D1865D0D638F047A7E3D3AA698F3A07751F
SHA-256:	BD02A9FE74094375001F382DE8066DD322A2E7C9A67821418104C9518BFE802B
SHA-512:	D009B2F666B8C9B3CCA614575CC6A176D038696C3EFFC84C29F84E5F11DF1123FBF5BB1E2F2F6BFF7838C8682973BF99D187B79B2FE59AC2245BD9FA8B16836
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 da(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 ea=da(this),fa="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),p={},ha={};function r(a,b){var c=ha[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=ea;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=fa&&"es6"===c?f[d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\f[2].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	21878
Entropy (8bit):	5.4097110490020635
Encrypted:	false
SSDEEP:	384:IXAmFuHJemiS2MwYArfa2iRop0PGHJxSyl0PLfQemrKvqY:sTxB2UrfeSSyl0Pz8eqY
MD5:	F720FA603B3E2514D36557034C3C6F0E
SHA1:	8F695234514B5F81167953C43C6E1006FF1865F1
SHA-256:	023AB520F198F85225F9E86CD2D4D7BC71EA1116D27F9A9B92E2A4F4993967F4
SHA-512:	F3D9B4D323C9F4372DE3AE62E7E695AD544E1E2E80F9B94752D47128B281D638974348C5D7A2E3DFAAC67C59A0C6E1EEC52AC10B2D75F82139878013E962128
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/pagead/js/r20210429/r20110914/elements/html/interstitial_ad_frame.js
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .var n;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 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 r=ca(this);function da(a,b){if(b)a:{var c=r;a=a.split(".");for(var e=0;e<a.length-1;e++){var f=a[e];if(!(f in c))break a;c=c[f]}a=a[a.length-1];e=c[a];b=b(e);b!=e&&null!=b&&ba(c,a,{configurable:!0,writable:!0,value:b})}} .function t(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:aa(a)}}var ea="function"==typeof Objec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\f[3].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1610
Entropy (8bit):	5.304847945185042
Encrypted:	false
SSDEEP:	48:axvWazPjHa5lM1JIO+22OqRFbB6u/t9cS:idzPjHB92OIFbB6ut
MD5:	D6B0A60B328FB34516306944169F75CC
SHA1:	0DCD12C584B2117829F4CC2B074F3B0F0A6B68E0
SHA-256:	8BC3D695C45FC0A4D3BFC67FE64F3BE04B08307D5F8EC6EBA1A9B54581BE178B
SHA-512:	E2FA46E1733A9226A5ACC16BC53383E70750A8743B6E49E10F7619DF994BEBAA6A5492A1DC4915A0241875B0D4D969B3BE3A3DDF2156A65A4193CCC1C8FC337 4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\f[3].txt	
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .function e(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}};var g=[];function h(){var a=g;g=[];var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];a=b?b.call(a):{next:e(a)};for(b=a.next();!b.done;b=a.next()){b=b.value;try{b()}catch(f){}}};var k=document;function m(){for(var a=k.head,b=a.querySelectorAll("link[data-reload-stylesheet][as=style][rel=preload]"),f=0;f<b.length;f++){var p=b[f],c="link",l=document;c=String(c);"application/xhtml+xml"===l.contentType&&(c=c.toLowerCase());c=l.createElement(c);c.setAttribute("rel","stylesheet");c.setAttribute("href",p.getAttribute("href"));a.appendChild(c)}if(0<b.length){var d=void 0===d?.01:d;if(!(Math.random()>d)){a=document.currentScript;a=(a=void 0===a?null:a)&&"26"===a.getAttribute("data-jc")?a:document.querySelector('[data-jc="26"]'); .d="https://pagead2.googlesyndication.com/pagead/gen_204?

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\fbevents[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	93774
Entropy (8bit):	5.392602416896564
Encrypted:	false
SSDEEP:	1536:sM+OWt6w6aic9MeipKKqQqcThe7Kdv0a9sIOC1jaMu5Qm2B+QNSMngUSZYSlIUiX:sOQMj1SVBYDGKx
MD5:	077B8B6E85C9EDF74D372D155180E6D3
SHA1:	4A24BE343819AD355807ADB01579366A1E64B8B9
SHA-256:	A517525B8A7D39BCAF1CF5F9695C5BE8FCE7A6B920A3924C1A4F70E8EA748C05
SHA-512:	DB714A2EAF14E6727086795FE151F3729DA32BFA0B87AB74289B7DF9E0808E1FEBCA38D2622EF47B7AA263479BDB66857011E2302DD1AFC9E814EF6B74642DF9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/en_US/fbevents.js
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\global[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):	20958
Entropy (8bit):	4.978366287319688
Encrypted:	false
SSDEEP:	192:tYWabFARMfLjICF52FckilMPI4VTYXcdKDwvhq1RjyXX+bVo5o4wIq1R+ypi/VYs:qJbvqcki+PbVTYXcAG4zyHwBDuypi/Ws
MD5:	FEAB1DC4F0DBFD3E4A6FCA334FC9F02A
SHA1:	559422BBC737F9DE66723E125B8F276C9E5FBC60
SHA-256:	32EEA542AA56D0A6FEBCE533CB08222D95EF58E75CEB89483CD028D10F2F5DA8
SHA-512:	05A1780B87A5A0EEDFE898CAF351C64036C025E1C6A6563A67FD50ED68F9C81AC9A96E4899D56AB4595B9C6A557BFA8EEB9E44A67E51E319FCE81AE75D7E0D6B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/css/global.css
Preview:	html,body,div,span,applet,object,iframe,h1,h2,h3,h4,h5,h6,p,blockquote,pre,a,abbr,acronym,address,big,cite,code,del,dfn,em,img,ins,kbd,q,s,samp,small,strike,strong,sub,sup,tt,var,b,u,i,center,dl,dt,dd,ol,ul,li,fieldset,form,label,legend,table,caption,tbody,tfoot,thead,tr,th,td,article,aside,canvas,details,embed,figure,figcaption,footer,header,hgroup,menu,nav,output,ruby,section,summary,time,mark,audio,video{margin:0;padding:0;border:0;font-size:100%;font:inherit;vertical-align:baseline}article,aside,details,figcaption,figure,footer,header,hgroup,menu,nav,section{display:block}body{line-height:1}ol,ul{list-style:none}blockquote,q{quotes:none}blockquote:before,blockquote:after,q:before,q:after{content:"";content:none}table{border-collapse:collapse;border-spacing:0}*,:before,:after{box-sizing:border-box;-moz-box-sizing:border-box;-webkit-box-sizing:border-box}html{-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%;font-size:100%}body{font-size:62.5%;font-family:biryani,sans-serif}h1,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\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:	C40111C3CC0754E90CF71F72F7F16F43B835B7E808423DFD99F90DD5177538B702E64FF1D9EE8D3BC86AEAA11B6F7A0EF826184E354B162158839FFB75D174C0
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\jquery-1.11.3.min[1].js	
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\2K7JPOQS\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\2K7JPOQS\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
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\2K7JPOQS\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:	71C89629427869368096A28FB6917C01BB520F1E
SHA-256:	7C98661F1D1E8C9520747DC08681752E45CF4C5D3CEB1D28642CFDCAFC10E896
SHA-512:	B6A7E2A056B2A5E1300F0EF438D1839D25B1E502397BD7CF78F1B84DC65AC5792CB4DB8D329661EA03E1090EADD7024889A5B6CAA733609D9D9312069C0F773

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\jquery.themepunch.tools.min[1].js	
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\2K7JPOQS\js[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	120080
Entropy (8bit):	5.543311088077586
Encrypted:	false
SSDEEP:	1536:BSJZ0eK9owZdVI0i+H7muo6Ni7QE12LsDjSdENQuSt81z9jKPfjGljAC2FSvOlH5:EJZ0eK9LZk0e4K9j8EZStlG58xFKx+
MD5:	E969C77FA4E04BEEC38F0D365FCD23FC
SHA1:	0DCBB91C75482F8A49339E595878535FCE79AD71
SHA-256:	254AE6809FBE40B76C3198C941107AD8CE4141020F73A78152F8EA3C6F421C96
SHA-512:	2A45BCF6CB60F703A21F08A6697861ACA4A6BBE132217492DC1CF309E247DD9154D07B8859EFA27043B52908EB70862FC702C2F32AC4A2E9B715A3F2B339C4E
Malicious:	false
Reputation:	low
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"1",. . "macros":[{. "function":"__e". },{. "vtp_signal":1,. "function":"__c",. "vtp_value":1. },{. "function":"__c",. "vtp_value":"google.de". },{. "function":"__c",. "vtp_value":0. },{. "function":"__aev",. "vtp_varType":"URL",. "vtp_component":"IS_OUTBOUND",. "vtp_affiliatedDomains":["list"]. },{. "function":"__v",. "vtp_name":"gtm.triggers",. "vtp_dataLayerVersion":2,. "vtp_setDefaultValue":true,. "vtp_defaultValue":"". },{. "function":"__v",. "vtp_name":"gtm.elementId",. "vtp_dataLayerVersion":1. },{. "function":"__v",. "vtp_name":"gtm.elementClasses",. "vtp_dataLayerVersion":1. },{. "function":"__aev",. "vtp_varType":"URL",. "vtp_component":"URL_NO_FRAGMENT". },{. "function":"__aev",. "vtp_varType":"URL",.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\js[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	90459
Entropy (8bit):	5.506050341936455
Encrypted:	false
SSDEEP:	1536:Jb03wZdVQ0i+H7ouo6Ni7Q3iEN2LsD8vhtqddENQuSt81z9jKPfcRQWzcLF+:Jb0gZs0Q43lgqnEZSt/+
MD5:	B8036610EAE936BA530CBC926DAFCBDD
SHA1:	A86EE2495FCD15B96ACE0055E3456F92DE1EDAB7
SHA-256:	7A458C407BCA3114720AE7B97F8D1B9D37F162304A1A3A231FA2F9C9A0FCFDFF
SHA-512:	00E9A20F8381A55786F746EBB969AB702D7C700D40BB41680E3EAA44CBC687709F6C5833B44D604833E48C180D45796DC37FC26C0EC448F04ED742E5053320E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagmanager.com/gtag/js?id=UA-160283435-1
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"1",. . "macros":[{. "function":"__e". },{. "function":"__cid". }],. "tags":[{. "function":"__rep",. "once_per_event":true,. "vtp_containerId":["macro",1],. "tag_id":1. }],. "predicates":[{. "function":"_eq",. "arg0":["macro",0],. "arg1":"gtm.js". }],. "rules":[. [["if",0],["add",0]]].},."runtime":[].....};../*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var aa,ba=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},ca=function(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:ba(a)}},da="function"==typeof Object.create?Object.create:function(a){var b=function(){};b.prototype=a;return new b},ea;.if("function"==typeof Object.setPrototypeOf)ea=Object.setPrototypeOf;else{var ia;a:{var ja={a:!0},ma={};

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\la-consejeria-de-turismo-grupo-fuertes-y-hotel-puerto-juan-montiel-ganan-los-premios-hotels-tourism-de-caixabank[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):	99127
Entropy (8bit):	7.944372999974872
Encrypted:	false
SSDEEP:	3072:GEokoHB+o6A4fW30RRjqX1j0TUlYCXsfrpU:GcMGWQjqX1woKfrpU
MD5:	F08BC0D112E6403F8E74848022A85506
SHA1:	537B9A18DA50A083BA84F9DA08618BDC400466A0
SHA-256:	1BDC9FEE5F1F872EC31D7F284ADCE7667F5C643BE8C8F70E3BB0A4E3397BC4C3
SHA-512:	4D3645B63E771E5FC714D874F8F17F9362FFB50EB0F19CBA857506C36E41883AA4A53646E88A398EC5B1DEB00FFDC9F28FB698C513FBA7D9E3F58A012136B27
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\la-consejeria-de-turismo-grupo-fuertes-y-hotel-puerto-juan-montiel-ganan-los-premios-hotels-tourism-de-caixabank[1].jpg	
Reputation:	low
IE Cache URL:	http://https://imagenes.20minutos.es/files/og_thumbnail/uploads/imagenes/2021/05/04/la-consejeria-de-turismo-grupo-fuertes-y-hotel-puerto-juan-montiel-ganan-los-premios-hotels-tourism-de-caixabank.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...$4.%.....&'()*56789:CDEF GHIJSTUVWXYZcdefghijstuvwxyz.....?...RS...h.:.....Q@...;.....v)..4.i.1L"..F).4..)...M"...M"..4..L..zUi-co..j.E4.`flm*r...P. ..}.k .Q.H..Ph.?}....Tb=.Ux..).j..}.....s/C..Q.....H$'.4..Dpz.|.#.....J$5..'...4.R.].9....8..D..$5.....&.K.T@.^i.&....g=*<.9..}.0EC...W.9.Ji..9e..4...B.T.H....2.M4.39..4.~.J3.e.....Q...w|R.. jfh...i=.FA...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\las-farmacias-malaguenas-comenzaran-un-programa-de-seguimiento-y-atencion-a-pacientes-con-covid-persistente[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):	79980
Entropy (8bit):	7.959231468036861
Encrypted:	false
SSDEEP:	1536:i2VwJsOwZsOB598PV1VlQAL5EgZLAZSURnWBxcu//cNCTmnFnFNDUJ3:JyJsOwWFvVvL5EYLAZSURnWB6OmFFN+3
MD5:	1362FC99C88BF4BC8DDCEF389859C989
SHA1:	EEDD7D2A951C697B8551A494B245AE20D14108F0
SHA-256:	EA4AD81953EEC670738C47A11DEF0BBD8CCFAC9E4298906D1DC2C5AFFEB9641F
SHA-512:	D65D5C8578591453646945B70B1708281A3C4AF4D9BB3ED0B8816EFEE881073994C96A571444D9A4D676468E7A5F2EB38A4D29A7989A1C421D2C5B88408815A5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://imagenes.20minutos.es/files/og_thumbnail/uploads/imagenes/2021/05/04/las-farmacias-malaguenas-comenzaran-un-programa-de-seguimiento-y-atencion-a-pacientes-con-covid-persistente.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...$4.%.....&'()*56789:CDEF GHIJSTUVWXYZcdefghijstuvwxyz.....?...L.... ....RzTf...;..B.}..)}.k._Jp.})..".G7.m... _J`a....ys{..._Jx.=)...E .ot7.'i.D0..*)-.n..g( .y.."...I....O.D..EgK.D..(.1.G.I..?..f.....^].3."......i.`T.<..Ta.....k...P.m=4.N1Jr....7.I.CU$..q]zY).S}.1.,.d.d...,Ek..,...j{|..#...H!oC[....J.4...N.c..2..c.....\H.H..J.X.Jx.>....eZ.&QJ,O. <Y.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\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:	3016E2A24AC50CA85F99714CEF35C708303D35C161BDB0D35FD8F6E44E5C9CF55FBFB668F093B267E8C1D794E2FB28183498DCEC04A4DD852354AB7FA72AAD 1
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(funct ion(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].t ype.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.le ngth-(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.direct ories[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\2K7JPOQS\openx[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):	70
Entropy (8bit):	3.577769619550495
Encrypted:	false
SSDEEP:	3:CUul/Re/FemxhkYltxlzeze:E07ize
MD5:	58A7930CD4577FC33C35828C271EAB8F
SHA1:	406E57F86DC101E10F3A57BE1E2F7B93C4580474

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\openx[1].gif	
SHA-256:	8D70B3E6BADB6973663B398D297BB32EAEDD08826A1AF98D0A1CFCE5324FFCE0
SHA-512:	F7A5F748F4C0D3096A3CA972886FE9A9DFF5DCE7792779EC6FFC42FA880B3815E2E4C3BDEA452352F3844B81864C9BFB7861F66AC961CFA66CB9CB4FEBE568 8
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!..NETSCAPE2.0.....!.....,.....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\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\2K7JPOQS\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:	AFDBB72C9A58FD55912CD2A38AE7310397F40C129410F3A137384EE92CB4C3578A42A5E60184AA1E25526AD7044E1BCC5BA896970D7C27744BC1D860FD9A3FE 4
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\2K7JPOQS\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):	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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\pixel[1].png	
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\2K7JPOQS\revicons[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), revicons family
Category:	downloaded
Size (bytes):	12136
Entropy (8bit):	6.261379703810077
Encrypted:	false
SSDEEP:	192:xfDmzu+lqpPKvoZj2rpsD+lcsvDfM9A5sXa/MdMeHso478aumzNKzxgBm+G:xfDmFGyvoZSaDwvDfM9MYjMeHs5fg/
MD5:	2FEB69CCB596730C72920C6BA3E37EF8
SHA1:	F3A83BC4ABD0D4F968FC45EC14DA4636A8159B38
SHA-256:	9E4D4C6813568FDF70C61ECA9446D1BB80F84E79E8F2E5ED177365B6D5DE5FBF
SHA-512:	F88E5F714D87FC7C45FC4CC8DFA7C2B5452662ECF4FEA27C45DD5315D3D0F4850985C470486EC34FB97031411F76E80BF2A13791DEDD67DA9EBC053C1EFB3D3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/fonts/revicons/revicons.eot?5510888
Preview:	h/.....LP.....r.e.v.i.c.o.n.s.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .1...0.....r.e.v.i.c.o.n.s.....`OS/2>(H.....Vcmap...&...D....cvt .... ..$.....fpgm..x;..$.....gasp.....$.....glyf.!T.....jhead.j=....4...6hhea.....l...$hmtx|c.....loca.....@...Zmaxp.[.|..... name.+!.....post..O..."....!prep.....h...V.....z.....z.....1 .....PfEd.@...;.R.j.Z.R.....|.....`..... ./.4.6.;....."..1.6.:..... .....B.....&.B@?%$#! .....B...@.....j.....j..... .M.....T....H.....&.&....."...+.#'.#"....&7%6..2.....#!"&5.463.5'..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\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\2K7JPOQS\sodar2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	17641
Entropy (8bit):	5.328104698564835
Encrypted:	false
SSDEEP:	384:cb6evylwMi99H8ycdSy5W1TJf6twWmmwFLo6:U6lO99Hzcb5W3f66WmmwK6
MD5:	81ABECB080D4825BFE387366A2A214A5
SHA1:	F4A3CC0965EC913936A9DEA2FA598C542C58DE63
SHA-256:	C61A719B48533A1FA932729F4927BA1377A96C441B0D6A427096B867742B4645
SHA-512:	1F8DCB9762512CFB9770F412B5F09B50684C724701AA0610BFB49DF9EB06D4EB2974E807C175F3DECB82F0F26418E0573530D78310998E49205F3B34670AF92B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/sodar/sodar2.js

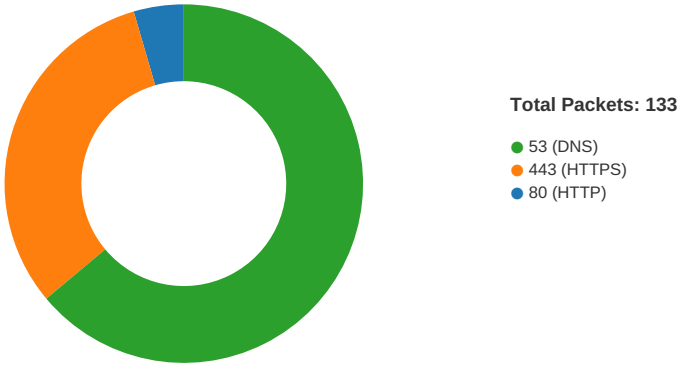
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\sodar2[1].js	
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}function ba(a){var b="undefined"!=typeof m.Symbol&&p(m.Symbol,"iterator")&&a[p(m.Symbol,"iterator")];return b?b.call(a):{next:aa(a)}}var ca="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},q="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,d){if(a==Array.prototype||a==Object.prototype)return a;a[b]=d.value;return a};.function da(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 d=a[b];if(d&&d.Math==Math)return d}throw Error("Cannot find global object");}var r=da(this),t="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),m={},v={};function p(a,b){var d=v[b];if(null==d)return a[b];d

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:39:44.645512104 CEST	49699	80	192.168.2.7	104.21.18.245
May 4, 2021 15:39:44.645623922 CEST	49700	80	192.168.2.7	104.21.18.245
May 4, 2021 15:39:44.687597990 CEST	80	49699	104.21.18.245	192.168.2.7
May 4, 2021 15:39:44.687659025 CEST	80	49700	104.21.18.245	192.168.2.7
May 4, 2021 15:39:44.687803984 CEST	49699	80	192.168.2.7	104.21.18.245
May 4, 2021 15:39:44.687863111 CEST	49700	80	192.168.2.7	104.21.18.245
May 4, 2021 15:39:44.689212084 CEST	49700	80	192.168.2.7	104.21.18.245
May 4, 2021 15:39:44.731509924 CEST	80	49700	104.21.18.245	192.168.2.7
May 4, 2021 15:39:44.760124922 CEST	80	49700	104.21.18.245	192.168.2.7
May 4, 2021 15:39:44.760210991 CEST	49700	80	192.168.2.7	104.21.18.245
May 4, 2021 15:39:44.769124031 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:44.810107946 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:44.810283899 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:44.819904089 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:44.860721111 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:44.865667105 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:44.865731955 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:44.865819931 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:44.865880966 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:44.917979002 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:44.925179958 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:44.925501108 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:44.960661888 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:44.960694075 CEST	443	49701	104.21.18.245	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:39:44.960721016 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:44.960793018 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:44.961865902 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:44.967010021 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:44.967433929 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:44.969883919 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:44.969996929 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.047878981 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.304400921 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.304481983 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.305885077 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.305903912 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.305919886 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.305932999 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.305969954 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.306000948 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.306328058 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.306376934 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.307565928 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.307579041 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.307621956 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.307651043 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.307826042 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.307846069 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.307883024 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.307904959 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.341090918 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.341142893 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.341164112 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.341192961 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.341803074 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.341831923 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.341852903 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.341857910 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.341876030 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.341886997 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.341928005 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.341933012 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.342749119 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.342775106 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.342838049 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.344002008 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.344036102 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.344079018 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.344096899 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.344659090 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.344722033 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.431022882 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.431487083 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.431953907 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.432430029 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.432897091 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.433348894 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.433804989 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.434272051 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.434734106 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.438390017 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.471997023 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.472093105 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.472577095 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.473031998 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.473568916 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.474004030 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.474394083 CEST	443	49701	104.21.18.245	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:39:45.474867105 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.475405931 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.479130030 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.479366064 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.479430914 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.479458094 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.479506016 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.481235981 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.481260061 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.481317997 CEST	49701	443	192.168.2.7	104.21.18.245
May 4, 2021 15:39:45.481467009 CEST	443	49701	104.21.18.245	192.168.2.7
May 4, 2021 15:39:45.481487989 CEST	443	49701	104.21.18.245	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:39:35.625536919 CEST	57820	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:35.684514999 CEST	53	57820	8.8.8.8	192.168.2.7
May 4, 2021 15:39:35.777456999 CEST	50848	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:35.826289892 CEST	53	50848	8.8.8.8	192.168.2.7
May 4, 2021 15:39:36.670645952 CEST	61242	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:36.719398022 CEST	53	61242	8.8.8.8	192.168.2.7
May 4, 2021 15:39:37.619440079 CEST	58562	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:37.668364048 CEST	53	58562	8.8.8.8	192.168.2.7
May 4, 2021 15:39:38.418473005 CEST	56590	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:38.478571892 CEST	53	56590	8.8.8.8	192.168.2.7
May 4, 2021 15:39:38.987301111 CEST	60501	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:39.036088943 CEST	53	60501	8.8.8.8	192.168.2.7
May 4, 2021 15:39:39.849175930 CEST	53775	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:39.897814035 CEST	53	53775	8.8.8.8	192.168.2.7
May 4, 2021 15:39:40.902326107 CEST	51837	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:40.956463099 CEST	53	51837	8.8.8.8	192.168.2.7
May 4, 2021 15:39:41.884021997 CEST	55411	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:41.932735920 CEST	53	55411	8.8.8.8	192.168.2.7
May 4, 2021 15:39:43.230957985 CEST	63668	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:43.291587114 CEST	53	63668	8.8.8.8	192.168.2.7
May 4, 2021 15:39:43.559592962 CEST	54640	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:43.618928909 CEST	53	54640	8.8.8.8	192.168.2.7
May 4, 2021 15:39:44.564110041 CEST	58739	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:44.630589008 CEST	53	58739	8.8.8.8	192.168.2.7
May 4, 2021 15:39:45.438777924 CEST	60338	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:45.450920105 CEST	58717	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:45.484270096 CEST	59762	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:45.502707005 CEST	53	58717	8.8.8.8	192.168.2.7
May 4, 2021 15:39:45.506680012 CEST	53	60338	8.8.8.8	192.168.2.7
May 4, 2021 15:39:45.532593966 CEST	54329	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:45.532830954 CEST	53	59762	8.8.8.8	192.168.2.7
May 4, 2021 15:39:45.598272085 CEST	53	54329	8.8.8.8	192.168.2.7
May 4, 2021 15:39:45.612165928 CEST	58052	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:45.626430035 CEST	54008	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:45.643125057 CEST	59451	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:45.672298908 CEST	53	58052	8.8.8.8	192.168.2.7
May 4, 2021 15:39:45.683191061 CEST	53	54008	8.8.8.8	192.168.2.7
May 4, 2021 15:39:45.702503920 CEST	53	59451	8.8.8.8	192.168.2.7
May 4, 2021 15:39:45.888689995 CEST	52914	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:45.953743935 CEST	53	52914	8.8.8.8	192.168.2.7
May 4, 2021 15:39:46.628969908 CEST	64569	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:46.695158958 CEST	53	64569	8.8.8.8	192.168.2.7
May 4, 2021 15:39:46.747833967 CEST	52816	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:46.804392099 CEST	50781	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:46.807677984 CEST	53	52816	8.8.8.8	192.168.2.7
May 4, 2021 15:39:46.905610085 CEST	53	50781	8.8.8.8	192.168.2.7
May 4, 2021 15:39:47.066507101 CEST	54230	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:47.087203979 CEST	54911	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:39:47.093265057 CEST	49958	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:47.126611948 CEST	53	54230	8.8.8.8	192.168.2.7
May 4, 2021 15:39:47.146805048 CEST	53	54911	8.8.8.8	192.168.2.7
May 4, 2021 15:39:47.154268980 CEST	53	49958	8.8.8.8	192.168.2.7
May 4, 2021 15:39:47.156419992 CEST	50860	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:47.240957022 CEST	53	50860	8.8.8.8	192.168.2.7
May 4, 2021 15:39:47.288758039 CEST	50452	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:47.352834940 CEST	53	50452	8.8.8.8	192.168.2.7
May 4, 2021 15:39:47.577038050 CEST	59730	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:47.625554085 CEST	53	59730	8.8.8.8	192.168.2.7
May 4, 2021 15:39:47.853833914 CEST	59310	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:47.913525105 CEST	53	59310	8.8.8.8	192.168.2.7
May 4, 2021 15:39:48.026536942 CEST	51919	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:48.094099045 CEST	64296	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:48.097434998 CEST	53	51919	8.8.8.8	192.168.2.7
May 4, 2021 15:39:48.143748045 CEST	53	64296	8.8.8.8	192.168.2.7
May 4, 2021 15:39:48.173564911 CEST	56680	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:48.233587980 CEST	53	56680	8.8.8.8	192.168.2.7
May 4, 2021 15:39:48.364998102 CEST	58820	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:48.413005114 CEST	60983	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:48.432284117 CEST	53	58820	8.8.8.8	192.168.2.7
May 4, 2021 15:39:48.477870941 CEST	53	60983	8.8.8.8	192.168.2.7
May 4, 2021 15:39:48.667928934 CEST	49247	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:48.716645002 CEST	53	49247	8.8.8.8	192.168.2.7
May 4, 2021 15:39:49.054888010 CEST	52286	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:49.069432020 CEST	56064	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:49.071149111 CEST	63744	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:49.103770971 CEST	53	52286	8.8.8.8	192.168.2.7
May 4, 2021 15:39:49.115289927 CEST	61457	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:49.127942085 CEST	53	63744	8.8.8.8	192.168.2.7
May 4, 2021 15:39:49.137330055 CEST	53	56064	8.8.8.8	192.168.2.7
May 4, 2021 15:39:49.148324013 CEST	58367	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:49.155160904 CEST	60599	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:49.172260046 CEST	53	61457	8.8.8.8	192.168.2.7
May 4, 2021 15:39:49.213577986 CEST	53	58367	8.8.8.8	192.168.2.7
May 4, 2021 15:39:49.215703964 CEST	53	60599	8.8.8.8	192.168.2.7
May 4, 2021 15:39:49.278985977 CEST	59571	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:49.335864067 CEST	53	59571	8.8.8.8	192.168.2.7
May 4, 2021 15:39:49.751357079 CEST	52689	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:49.819180965 CEST	53	52689	8.8.8.8	192.168.2.7
May 4, 2021 15:39:50.885277987 CEST	50290	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:50.934498072 CEST	53	50290	8.8.8.8	192.168.2.7
May 4, 2021 15:39:50.938420057 CEST	60427	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:50.990410089 CEST	53	60427	8.8.8.8	192.168.2.7
May 4, 2021 15:39:51.924618006 CEST	56209	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:51.981616020 CEST	53	56209	8.8.8.8	192.168.2.7
May 4, 2021 15:39:53.665837049 CEST	59582	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:53.725661039 CEST	53	59582	8.8.8.8	192.168.2.7
May 4, 2021 15:39:55.549551010 CEST	60949	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:55.556458950 CEST	58542	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:55.572273970 CEST	59179	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:55.583679914 CEST	60927	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:55.603313923 CEST	57854	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:55.605262041 CEST	53	58542	8.8.8.8	192.168.2.7
May 4, 2021 15:39:55.611423969 CEST	53	60949	8.8.8.8	192.168.2.7
May 4, 2021 15:39:55.620960951 CEST	53	59179	8.8.8.8	192.168.2.7
May 4, 2021 15:39:55.632707119 CEST	53	60927	8.8.8.8	192.168.2.7
May 4, 2021 15:39:55.645494938 CEST	62026	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:55.676357031 CEST	53	57854	8.8.8.8	192.168.2.7
May 4, 2021 15:39:55.703552008 CEST	53	62026	8.8.8.8	192.168.2.7
May 4, 2021 15:39:56.162636042 CEST	59453	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:56.234570980 CEST	53	59453	8.8.8.8	192.168.2.7
May 4, 2021 15:39:56.620099068 CEST	62468	53	192.168.2.7	8.8.8.8
May 4, 2021 15:39:56.692456961 CEST	53	62468	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:40:01.467348099 CEST	52563	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:01.518996954 CEST	53	52563	8.8.8.8	192.168.2.7
May 4, 2021 15:40:03.456868887 CEST	54721	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:03.518199921 CEST	53	54721	8.8.8.8	192.168.2.7
May 4, 2021 15:40:09.143884897 CEST	62826	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:09.192761898 CEST	53	62826	8.8.8.8	192.168.2.7
May 4, 2021 15:40:10.781867981 CEST	62046	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:10.833328009 CEST	53	62046	8.8.8.8	192.168.2.7
May 4, 2021 15:40:11.823986053 CEST	51223	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:11.872908115 CEST	53	51223	8.8.8.8	192.168.2.7
May 4, 2021 15:40:13.589174986 CEST	63908	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:13.638474941 CEST	53	63908	8.8.8.8	192.168.2.7
May 4, 2021 15:40:14.294837952 CEST	49226	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:14.344454050 CEST	53	49226	8.8.8.8	192.168.2.7
May 4, 2021 15:40:14.591203928 CEST	63908	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:14.650482893 CEST	53	63908	8.8.8.8	192.168.2.7
May 4, 2021 15:40:15.369016886 CEST	49226	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:15.417836905 CEST	53	49226	8.8.8.8	192.168.2.7
May 4, 2021 15:40:16.953054905 CEST	49226	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:17.001820087 CEST	53	49226	8.8.8.8	192.168.2.7
May 4, 2021 15:40:18.151638985 CEST	63908	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:18.200269938 CEST	53	63908	8.8.8.8	192.168.2.7
May 4, 2021 15:40:18.440952063 CEST	60212	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:18.489721060 CEST	53	60212	8.8.8.8	192.168.2.7
May 4, 2021 15:40:18.967148066 CEST	49226	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:19.017131090 CEST	53	49226	8.8.8.8	192.168.2.7
May 4, 2021 15:40:19.810158014 CEST	58867	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:19.859133005 CEST	53	58867	8.8.8.8	192.168.2.7
May 4, 2021 15:40:19.967448950 CEST	50864	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:20.018222094 CEST	53	50864	8.8.8.8	192.168.2.7
May 4, 2021 15:40:20.164144039 CEST	63908	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:20.215264082 CEST	53	63908	8.8.8.8	192.168.2.7
May 4, 2021 15:40:23.184823990 CEST	49226	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:23.233541965 CEST	53	49226	8.8.8.8	192.168.2.7
May 4, 2021 15:40:24.391052961 CEST	63908	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:24.441531897 CEST	53	63908	8.8.8.8	192.168.2.7
May 4, 2021 15:40:26.251441956 CEST	61504	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:26.308677912 CEST	53	61504	8.8.8.8	192.168.2.7
May 4, 2021 15:40:26.689462900 CEST	60231	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:26.753448009 CEST	53	60231	8.8.8.8	192.168.2.7
May 4, 2021 15:40:27.207601070 CEST	50095	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:27.267213106 CEST	53	50095	8.8.8.8	192.168.2.7
May 4, 2021 15:40:28.500205040 CEST	59654	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:28.548939943 CEST	53	59654	8.8.8.8	192.168.2.7
May 4, 2021 15:40:29.673589945 CEST	58233	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:29.724342108 CEST	53	58233	8.8.8.8	192.168.2.7
May 4, 2021 15:40:30.600768089 CEST	56822	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:30.649302959 CEST	53	56822	8.8.8.8	192.168.2.7
May 4, 2021 15:40:31.210207939 CEST	62572	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:31.275563955 CEST	53	62572	8.8.8.8	192.168.2.7
May 4, 2021 15:40:33.209809065 CEST	57179	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:33.261506081 CEST	53	57179	8.8.8.8	192.168.2.7
May 4, 2021 15:40:35.175386906 CEST	56124	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:35.227240086 CEST	53	56124	8.8.8.8	192.168.2.7
May 4, 2021 15:40:48.107775927 CEST	62287	53	192.168.2.7	8.8.8.8
May 4, 2021 15:40:48.166623116 CEST	53	62287	8.8.8.8	192.168.2.7
May 4, 2021 15:41:19.534008026 CEST	54644	53	192.168.2.7	8.8.8.8
May 4, 2021 15:41:19.583895922 CEST	53	54644	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 15:39:44.564110041 CEST	192.168.2.7	8.8.8.8	0x5bf6	Standard query (0)	localcoron avirus.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 15:39:45.612165928 CEST	192.168.2.7	8.8.8.8	0x101e	Standard query (0)	www.republica.com	A (IP address)	IN (0x0001)
May 4, 2021 15:39:45.626430035 CEST	192.168.2.7	8.8.8.8	0xbde5	Standard query (0)	www.lavozdegalicia.es	A (IP address)	IN (0x0001)
May 4, 2021 15:39:45.643125057 CEST	192.168.2.7	8.8.8.8	0x6048	Standard query (0)	static.eldiario.es	A (IP address)	IN (0x0001)
May 4, 2021 15:39:45.888689995 CEST	192.168.2.7	8.8.8.8	0x359c	Standard query (0)	i.blogs.es	A (IP address)	IN (0x0001)
May 4, 2021 15:39:46.628969908 CEST	192.168.2.7	8.8.8.8	0xfd70	Standard query (0)	img.europapress.es	A (IP address)	IN (0x0001)
May 4, 2021 15:39:46.747833967 CEST	192.168.2.7	8.8.8.8	0xd370	Standard query (0)	static1.abc.es	A (IP address)	IN (0x0001)
May 4, 2021 15:39:46.804392099 CEST	192.168.2.7	8.8.8.8	0x8e06	Standard query (0)	estaticos-cdn.elperiodico.com	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.066507101 CEST	192.168.2.7	8.8.8.8	0x4edb	Standard query (0)	www.meneame.net	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.087203979 CEST	192.168.2.7	8.8.8.8	0xf4b9	Standard query (0)	media.revistagq.com	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.093265057 CEST	192.168.2.7	8.8.8.8	0xc57f	Standard query (0)	imagenes.20minutos.es	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.156419992 CEST	192.168.2.7	8.8.8.8	0x1419	Standard query (0)	s.libertaddigital.com	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.288758039 CEST	192.168.2.7	8.8.8.8	0x51ac	Standard query (0)	platform.twitter.com	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.577038050 CEST	192.168.2.7	8.8.8.8	0x7bb1	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.853833914 CEST	192.168.2.7	8.8.8.8	0x9c21	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
May 4, 2021 15:39:48.026536942 CEST	192.168.2.7	8.8.8.8	0x10b9	Standard query (0)	static.hotjar.com	A (IP address)	IN (0x0001)
May 4, 2021 15:39:48.173564911 CEST	192.168.2.7	8.8.8.8	0xa8b6	Standard query (0)	proteccion10.net	A (IP address)	IN (0x0001)
May 4, 2021 15:39:48.364998102 CEST	192.168.2.7	8.8.8.8	0xb85a	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
May 4, 2021 15:39:48.413005114 CEST	192.168.2.7	8.8.8.8	0xfca	Standard query (0)	script.hotjar.com	A (IP address)	IN (0x0001)
May 4, 2021 15:39:49.069432020 CEST	192.168.2.7	8.8.8.8	0x4463	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
May 4, 2021 15:39:49.071149111 CEST	192.168.2.7	8.8.8.8	0x2dba	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
May 4, 2021 15:39:49.148324013 CEST	192.168.2.7	8.8.8.8	0xde18	Standard query (0)	adservice.google.de	A (IP address)	IN (0x0001)
May 4, 2021 15:39:49.278985977 CEST	192.168.2.7	8.8.8.8	0x63e3	Standard query (0)	www.googletagservices.com	A (IP address)	IN (0x0001)
May 4, 2021 15:39:49.751357079 CEST	192.168.2.7	8.8.8.8	0x85dc	Standard query (0)	vars.hotjar.com	A (IP address)	IN (0x0001)
May 4, 2021 15:39:55.549551010 CEST	192.168.2.7	8.8.8.8	0x2cb1	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
May 4, 2021 15:39:55.556458950 CEST	192.168.2.7	8.8.8.8	0xb70e	Standard query (0)	odr.mookie1.com	A (IP address)	IN (0x0001)
May 4, 2021 15:39:55.572273970 CEST	192.168.2.7	8.8.8.8	0xea54	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
May 4, 2021 15:39:55.583679914 CEST	192.168.2.7	8.8.8.8	0x7ec3	Standard query (0)	image6.pubmatic.com	A (IP address)	IN (0x0001)
May 4, 2021 15:39:55.603313923 CEST	192.168.2.7	8.8.8.8	0xcd8b	Standard query (0)	token.rubiconproject.com	A (IP address)	IN (0x0001)
May 4, 2021 15:39:55.645494938 CEST	192.168.2.7	8.8.8.8	0xcbf3	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
May 4, 2021 15:39:56.162636042 CEST	192.168.2.7	8.8.8.8	0xe591	Standard query (0)	cc.adingo.jp	A (IP address)	IN (0x0001)
May 4, 2021 15:40:03.456868887 CEST	192.168.2.7	8.8.8.8	0xb71	Standard query (0)	localcoronavirus.com	A (IP address)	IN (0x0001)
May 4, 2021 15:40:19.967448950 CEST	192.168.2.7	8.8.8.8	0xde82	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
May 4, 2021 15:40:26.251441956 CEST	192.168.2.7	8.8.8.8	0xdc61	Standard query (0)	facebook.com	A (IP address)	IN (0x0001)
May 4, 2021 15:40:26.689462900 CEST	192.168.2.7	8.8.8.8	0x19f7	Standard query (0)	m.facebook.com	A (IP address)	IN (0x0001)
May 4, 2021 15:40:27.207601070 CEST	192.168.2.7	8.8.8.8	0xf324	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 15:39:44.630589008 CEST	8.8.8.8	192.168.2.7	0x5bf6	No error (0)	localcoronavirus.com		104.21.18.245	A (IP address)	IN (0x0001)
May 4, 2021 15:39:44.630589008 CEST	8.8.8.8	192.168.2.7	0x5bf6	No error (0)	localcoronavirus.com		172.67.183.244	A (IP address)	IN (0x0001)
May 4, 2021 15:39:45.672298908 CEST	8.8.8.8	192.168.2.7	0x101e	No error (0)	www.republica.com	republica.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:45.672298908 CEST	8.8.8.8	192.168.2.7	0x101e	No error (0)	republica.com		146.255.19.152	A (IP address)	IN (0x0001)
May 4, 2021 15:39:45.683191061 CEST	8.8.8.8	192.168.2.7	0xbde5	No error (0)	www.lavozdegalicia.es	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:45.683191061 CEST	8.8.8.8	192.168.2.7	0xbde5	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		52.211.67.210	A (IP address)	IN (0x0001)
May 4, 2021 15:39:45.683191061 CEST	8.8.8.8	192.168.2.7	0xbde5	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		54.194.190.147	A (IP address)	IN (0x0001)
May 4, 2021 15:39:45.683191061 CEST	8.8.8.8	192.168.2.7	0xbde5	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		34.249.141.22	A (IP address)	IN (0x0001)
May 4, 2021 15:39:45.683191061 CEST	8.8.8.8	192.168.2.7	0xbde5	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		52.211.217.51	A (IP address)	IN (0x0001)
May 4, 2021 15:39:45.683191061 CEST	8.8.8.8	192.168.2.7	0xbde5	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		52.210.129.255	A (IP address)	IN (0x0001)
May 4, 2021 15:39:45.683191061 CEST	8.8.8.8	192.168.2.7	0xbde5	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		54.194.71.119	A (IP address)	IN (0x0001)
May 4, 2021 15:39:45.702503920 CEST	8.8.8.8	192.168.2.7	0x6048	No error (0)	static.eldiario.es	static.eldiario.es.cdn.bitban.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:45.702503920 CEST	8.8.8.8	192.168.2.7	0x6048	No error (0)	static.eldiario.es.cdn.bitban.net	caching.c19.edge2befaster.io		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:45.702503920 CEST	8.8.8.8	192.168.2.7	0x6048	No error (0)	caching.c19.edge2befaster.io	aec01.esg.eldiario.edgetcdn.io		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:45.702503920 CEST	8.8.8.8	192.168.2.7	0x6048	No error (0)	aec01.esg.eldiario.edgetcdn.io		84.17.62.22	A (IP address)	IN (0x0001)
May 4, 2021 15:39:45.702503920 CEST	8.8.8.8	192.168.2.7	0x6048	No error (0)	aec01.esg.eldiario.edgetcdn.io		84.17.62.23	A (IP address)	IN (0x0001)
May 4, 2021 15:39:45.953743935 CEST	8.8.8.8	192.168.2.7	0x359c	No error (0)	i.blogs.es	d1j70itqjm2icu.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:45.953743935 CEST	8.8.8.8	192.168.2.7	0x359c	No error (0)	d1j70itqjm2icu.cloudfront.net		13.225.74.97	A (IP address)	IN (0x0001)
May 4, 2021 15:39:45.953743935 CEST	8.8.8.8	192.168.2.7	0x359c	No error (0)	d1j70itqjm2icu.cloudfront.net		13.225.74.64	A (IP address)	IN (0x0001)
May 4, 2021 15:39:45.953743935 CEST	8.8.8.8	192.168.2.7	0x359c	No error (0)	d1j70itqjm2icu.cloudfront.net		13.225.74.128	A (IP address)	IN (0x0001)
May 4, 2021 15:39:45.953743935 CEST	8.8.8.8	192.168.2.7	0x359c	No error (0)	d1j70itqjm2icu.cloudfront.net		13.225.74.3	A (IP address)	IN (0x0001)
May 4, 2021 15:39:46.695158958 CEST	8.8.8.8	192.168.2.7	0xfd70	No error (0)	img.europapress.es	d2dzdx91mh5kpx.cloudfront.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 15:39:46.695158958 CEST	8.8.8.8	192.168.2.7	0xfd70	No error (0)	d2dzdx91mh5kpx.cloudfront.net		13.224.193.60	A (IP address)	IN (0x0001)
May 4, 2021 15:39:46.695158958 CEST	8.8.8.8	192.168.2.7	0xfd70	No error (0)	d2dzdx91mh5kpx.cloudfront.net		13.224.193.96	A (IP address)	IN (0x0001)
May 4, 2021 15:39:46.695158958 CEST	8.8.8.8	192.168.2.7	0xfd70	No error (0)	d2dzdx91mh5kpx.cloudfront.net		13.224.193.101	A (IP address)	IN (0x0001)
May 4, 2021 15:39:46.695158958 CEST	8.8.8.8	192.168.2.7	0xfd70	No error (0)	d2dzdx91mh5kpx.cloudfront.net		13.224.193.112	A (IP address)	IN (0x0001)
May 4, 2021 15:39:46.807677984 CEST	8.8.8.8	192.168.2.7	0xd370	No error (0)	static1.abc.es	static.abc.es		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:46.807677984 CEST	8.8.8.8	192.168.2.7	0xd370	No error (0)	static.abc.es	static-abc.akamaized.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:46.905610085 CEST	8.8.8.8	192.168.2.7	0x8e06	No error (0)	estaticos-cdn.elperiodico.com	prensaiberica.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:46.905610085 CEST	8.8.8.8	192.168.2.7	0x8e06	No error (0)	prensaiberica.map.fastly.net		199.232.194.133	A (IP address)	IN (0x0001)
May 4, 2021 15:39:46.905610085 CEST	8.8.8.8	192.168.2.7	0x8e06	No error (0)	prensaiberica.map.fastly.net		199.232.198.133	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.126611948 CEST	8.8.8.8	192.168.2.7	0x4edb	No error (0)	www.meneame.net		52.212.89.238	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.126611948 CEST	8.8.8.8	192.168.2.7	0x4edb	No error (0)	www.meneame.net		108.128.145.3	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.146805048 CEST	8.8.8.8	192.168.2.7	0xf4b9	No error (0)	media.revistagq.com	cni-digital.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:47.146805048 CEST	8.8.8.8	192.168.2.7	0xf4b9	No error (0)	cni-digital.map.fastly.net		151.101.2.133	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.146805048 CEST	8.8.8.8	192.168.2.7	0xf4b9	No error (0)	cni-digital.map.fastly.net		151.101.66.133	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.146805048 CEST	8.8.8.8	192.168.2.7	0xf4b9	No error (0)	cni-digital.map.fastly.net		151.101.130.133	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.146805048 CEST	8.8.8.8	192.168.2.7	0xf4b9	No error (0)	cni-digital.map.fastly.net		151.101.194.133	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.154268980 CEST	8.8.8.8	192.168.2.7	0xc57f	No error (0)	imagenes.20minutos.es	di7juyclzlgyp.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:47.154268980 CEST	8.8.8.8	192.168.2.7	0xc57f	No error (0)	di7juyclzlgyp.cloudfront.net		13.225.74.99	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.154268980 CEST	8.8.8.8	192.168.2.7	0xc57f	No error (0)	di7juyclzlgyp.cloudfront.net		13.225.74.23	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.154268980 CEST	8.8.8.8	192.168.2.7	0xc57f	No error (0)	di7juyclzlgyp.cloudfront.net		13.225.74.87	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.154268980 CEST	8.8.8.8	192.168.2.7	0xc57f	No error (0)	di7juyclzlgyp.cloudfront.net		13.225.74.48	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.240957022 CEST	8.8.8.8	192.168.2.7	0x1419	No error (0)	s.libertaddigital.com		213.149.255.231	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.352834940 CEST	8.8.8.8	192.168.2.7	0x51ac	No error (0)	platform.twitter.com	cs472.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:47.352834940 CEST	8.8.8.8	192.168.2.7	0x51ac	No error (0)	cs472.wac.edgecastcdn.net	cs1-apr-8315.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:47.352834940 CEST	8.8.8.8	192.168.2.7	0x51ac	No error (0)	cs1-apr-8315.wac.edgecastcdn.net	wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:47.352834940 CEST	8.8.8.8	192.168.2.7	0x51ac	No error (0)	cs1-lb-eu.8315.ecdns.net	cs491.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 15:39:47.352834940 CEST	8.8.8.8	192.168.2.7	0x51ac	No error (0)	cs491.wac.edgecastcdn.net		192.229.233.25	A (IP address)	IN (0x0001)
May 4, 2021 15:39:47.625554085 CEST	8.8.8.8	192.168.2.7	0x7bb1	No error (0)	cdn.jsdelivr.net	dualstack.f3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:47.913525105 CEST	8.8.8.8	192.168.2.7	0x9c21	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:47.913525105 CEST	8.8.8.8	192.168.2.7	0x9c21	No error (0)	scontent.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
May 4, 2021 15:39:48.097434998 CEST	8.8.8.8	192.168.2.7	0x10b9	No error (0)	static.hotjar.com	static-cdn.hotjar.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:48.097434998 CEST	8.8.8.8	192.168.2.7	0x10b9	No error (0)	static-cdn.hotjar.com		13.225.74.20	A (IP address)	IN (0x0001)
May 4, 2021 15:39:48.097434998 CEST	8.8.8.8	192.168.2.7	0x10b9	No error (0)	static-cdn.hotjar.com		13.225.74.66	A (IP address)	IN (0x0001)
May 4, 2021 15:39:48.097434998 CEST	8.8.8.8	192.168.2.7	0x10b9	No error (0)	static-cdn.hotjar.com		13.225.74.74	A (IP address)	IN (0x0001)
May 4, 2021 15:39:48.097434998 CEST	8.8.8.8	192.168.2.7	0x10b9	No error (0)	static-cdn.hotjar.com		13.225.74.30	A (IP address)	IN (0x0001)
May 4, 2021 15:39:48.233587980 CEST	8.8.8.8	192.168.2.7	0xa8b6	No error (0)	proteccion10.net		193.32.242.105	A (IP address)	IN (0x0001)
May 4, 2021 15:39:48.432284117 CEST	8.8.8.8	192.168.2.7	0xb85a	No error (0)	googleads.g.doubleclick.net		172.217.16.130	A (IP address)	IN (0x0001)
May 4, 2021 15:39:48.477870941 CEST	8.8.8.8	192.168.2.7	0xfca	No error (0)	script.hotjar.com		13.224.193.31	A (IP address)	IN (0x0001)
May 4, 2021 15:39:48.477870941 CEST	8.8.8.8	192.168.2.7	0xfca	No error (0)	script.hotjar.com		13.224.193.122	A (IP address)	IN (0x0001)
May 4, 2021 15:39:48.477870941 CEST	8.8.8.8	192.168.2.7	0xfca	No error (0)	script.hotjar.com		13.224.193.38	A (IP address)	IN (0x0001)
May 4, 2021 15:39:48.477870941 CEST	8.8.8.8	192.168.2.7	0xfca	No error (0)	script.hotjar.com		13.224.193.121	A (IP address)	IN (0x0001)
May 4, 2021 15:39:49.127942085 CEST	8.8.8.8	192.168.2.7	0x2dba	No error (0)	www.google.de		142.250.185.227	A (IP address)	IN (0x0001)
May 4, 2021 15:39:49.137330055 CEST	8.8.8.8	192.168.2.7	0x4463	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:49.137330055 CEST	8.8.8.8	192.168.2.7	0x4463	No error (0)	stats.l.doubleclick.net		74.125.140.155	A (IP address)	IN (0x0001)
May 4, 2021 15:39:49.137330055 CEST	8.8.8.8	192.168.2.7	0x4463	No error (0)	stats.l.doubleclick.net		74.125.140.157	A (IP address)	IN (0x0001)
May 4, 2021 15:39:49.137330055 CEST	8.8.8.8	192.168.2.7	0x4463	No error (0)	stats.l.doubleclick.net		74.125.140.156	A (IP address)	IN (0x0001)
May 4, 2021 15:39:49.137330055 CEST	8.8.8.8	192.168.2.7	0x4463	No error (0)	stats.l.doubleclick.net		74.125.140.154	A (IP address)	IN (0x0001)
May 4, 2021 15:39:49.172260046 CEST	8.8.8.8	192.168.2.7	0x8587	No error (0)	partnerad.l.doubleclick.net		142.250.185.194	A (IP address)	IN (0x0001)
May 4, 2021 15:39:49.213577986 CEST	8.8.8.8	192.168.2.7	0xde18	No error (0)	adservice.google.de	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:49.213577986 CEST	8.8.8.8	192.168.2.7	0xde18	No error (0)	pagead46.l.doubleclick.net		142.250.186.98	A (IP address)	IN (0x0001)
May 4, 2021 15:39:49.335864067 CEST	8.8.8.8	192.168.2.7	0x63e3	No error (0)	www.googletagservices.com		142.250.186.34	A (IP address)	IN (0x0001)
May 4, 2021 15:39:49.819180965 CEST	8.8.8.8	192.168.2.7	0x85dc	No error (0)	vars.hotjar.com		13.224.193.91	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 15:39:49.819180965 CEST	8.8.8.8	192.168.2.7	0x85dc	No error (0)	vars.hotjar.com		13.224.193.12	A (IP address)	IN (0x0001)
May 4, 2021 15:39:49.819180965 CEST	8.8.8.8	192.168.2.7	0x85dc	No error (0)	vars.hotjar.com		13.224.193.73	A (IP address)	IN (0x0001)
May 4, 2021 15:39:49.819180965 CEST	8.8.8.8	192.168.2.7	0x85dc	No error (0)	vars.hotjar.com		13.224.193.116	A (IP address)	IN (0x0001)
May 4, 2021 15:39:55.605262041 CEST	8.8.8.8	192.168.2.7	0xb70e	No error (0)	odr.mookie1.com	tagr-gcp-odr-euw4.mookie1.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:55.605262041 CEST	8.8.8.8	192.168.2.7	0xb70e	No error (0)	tagr-gcp-odr-euw4.mookie1.com		34.98.67.61	A (IP address)	IN (0x0001)
May 4, 2021 15:39:55.611423969 CEST	8.8.8.8	192.168.2.7	0x2cb1	No error (0)	id.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
May 4, 2021 15:39:55.620960951 CEST	8.8.8.8	192.168.2.7	0xea54	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
May 4, 2021 15:39:55.620960951 CEST	8.8.8.8	192.168.2.7	0xea54	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
May 4, 2021 15:39:55.632707119 CEST	8.8.8.8	192.168.2.7	0x7ec3	No error (0)	image6.pubmatic.com	pugm22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:55.632707119 CEST	8.8.8.8	192.168.2.7	0x7ec3	No error (0)	pugm22000nfc.pubmatic.com	pugm22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:55.632707119 CEST	8.8.8.8	192.168.2.7	0x7ec3	No error (0)	pugm22000nf.pubmatic.com		185.64.189.115	A (IP address)	IN (0x0001)
May 4, 2021 15:39:55.676357031 CEST	8.8.8.8	192.168.2.7	0xcd8b	No error (0)	token.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:39:55.703552008 CEST	8.8.8.8	192.168.2.7	0xcbf3	No error (0)	cm.g.doubleclick.net		172.217.16.130	A (IP address)	IN (0x0001)
May 4, 2021 15:39:56.234570980 CEST	8.8.8.8	192.168.2.7	0xe591	No error (0)	cc.adingo.jp		18.179.240.58	A (IP address)	IN (0x0001)
May 4, 2021 15:39:56.234570980 CEST	8.8.8.8	192.168.2.7	0xe591	No error (0)	cc.adingo.jp		54.178.184.38	A (IP address)	IN (0x0001)
May 4, 2021 15:39:56.234570980 CEST	8.8.8.8	192.168.2.7	0xe591	No error (0)	cc.adingo.jp		52.68.53.67	A (IP address)	IN (0x0001)
May 4, 2021 15:39:56.234570980 CEST	8.8.8.8	192.168.2.7	0xe591	No error (0)	cc.adingo.jp		54.250.196.226	A (IP address)	IN (0x0001)
May 4, 2021 15:39:56.234570980 CEST	8.8.8.8	192.168.2.7	0xe591	No error (0)	cc.adingo.jp		35.72.120.200	A (IP address)	IN (0x0001)
May 4, 2021 15:39:56.234570980 CEST	8.8.8.8	192.168.2.7	0xe591	No error (0)	cc.adingo.jp		54.64.53.220	A (IP address)	IN (0x0001)
May 4, 2021 15:39:56.234570980 CEST	8.8.8.8	192.168.2.7	0xe591	No error (0)	cc.adingo.jp		18.180.1.224	A (IP address)	IN (0x0001)
May 4, 2021 15:39:56.234570980 CEST	8.8.8.8	192.168.2.7	0xe591	No error (0)	cc.adingo.jp		54.178.254.210	A (IP address)	IN (0x0001)
May 4, 2021 15:40:03.518199921 CEST	8.8.8.8	192.168.2.7	0xb71	No error (0)	localcoronavirus.com		172.67.183.244	A (IP address)	IN (0x0001)
May 4, 2021 15:40:03.518199921 CEST	8.8.8.8	192.168.2.7	0xb71	No error (0)	localcoronavirus.com		104.21.18.245	A (IP address)	IN (0x0001)
May 4, 2021 15:40:20.018222094 CEST	8.8.8.8	192.168.2.7	0xde82	No error (0)	match.adsrvr.org	match-1943069928.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:40:20.018222094 CEST	8.8.8.8	192.168.2.7	0xde82	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		54.76.6.247	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 15:40:20.018222094 CEST	8.8.8.8	192.168.2.7	0xde82	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.30.73.5	A (IP address)	IN (0x0001)
May 4, 2021 15:40:20.018222094 CEST	8.8.8.8	192.168.2.7	0xde82	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		34.240.192.98	A (IP address)	IN (0x0001)
May 4, 2021 15:40:20.018222094 CEST	8.8.8.8	192.168.2.7	0xde82	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.208.69.189	A (IP address)	IN (0x0001)
May 4, 2021 15:40:20.018222094 CEST	8.8.8.8	192.168.2.7	0xde82	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.210.202.173	A (IP address)	IN (0x0001)
May 4, 2021 15:40:20.018222094 CEST	8.8.8.8	192.168.2.7	0xde82	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		34.252.153.38	A (IP address)	IN (0x0001)
May 4, 2021 15:40:20.018222094 CEST	8.8.8.8	192.168.2.7	0xde82	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.210.189.83	A (IP address)	IN (0x0001)
May 4, 2021 15:40:20.018222094 CEST	8.8.8.8	192.168.2.7	0xde82	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		34.250.165.246	A (IP address)	IN (0x0001)
May 4, 2021 15:40:26.308677912 CEST	8.8.8.8	192.168.2.7	0xdc61	No error (0)	facebook.com		31.13.92.36	A (IP address)	IN (0x0001)
May 4, 2021 15:40:26.753448009 CEST	8.8.8.8	192.168.2.7	0x19f7	No error (0)	m.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:40:26.753448009 CEST	8.8.8.8	192.168.2.7	0x19f7	No error (0)	star-mini.c10r.facebook.com		31.13.92.36	A (IP address)	IN (0x0001)
May 4, 2021 15:40:27.267213106 CEST	8.8.8.8	192.168.2.7	0xf324	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:40:27.267213106 CEST	8.8.8.8	192.168.2.7	0xf324	No error (0)	star-mini.c10r.facebook.com		31.13.92.36	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- localcoronavirus.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49700	104.21.18.245	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 15:39:44.689212084 CEST	349	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

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 15:39:44.760124922 CEST	349	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 04 May 2021 13:39:44 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Tue, 04 May 2021 14:39:44 GMT Location: https://localcoronavirus.com/ cf-request-id: 09d9343bda000096e61d384000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=mR9PLL8WMMOgIxGkgdzWBbVhDrbeKxsePcE0Zw3qdumGJMJuOuL2VVhuOCWCD1BYWiokuR7duy623X6Po02wr7OwpyDN7fWl4UC42PUXzbGFirdKcQ%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Vary: Accept-Encoding Server: cloudflare CF-RAY: 64a2230c8f3796e6-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

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 4, 2021 15:39:44.865731955 CEST	104.21.18.245	443	192.168.2.7	49701	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 4, 2021 15:39:46.275760889 CEST	84.17.62.22	443	192.168.2.7	49712	CN=15m2016.eldiario.es CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 25 23:25:48 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Thu Jun 24 00:25:48 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 4, 2021 15:39:46.338226080 CEST	84.17.62.22	443	192.168.2.7	49713	CN=15m2016.eldiario.es CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 25 23:25:48 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Thu Jun 24 00:25:48 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 4, 2021 15:39:46.441715956 CEST	52.211.67.210	443	192.168.2.7	49715	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

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 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 4, 2021 15:39:46.632251978 CEST	146.255.19.152	443	192.168.2.7	49711	CN=republica.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.	Thu Feb 04 11:00:51 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed May 05 12:00:51 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 4, 2021 15:39:46.654767036 CEST	52.211.67.210	443	192.168.2.7	49714	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 4, 2021 15:39:46.663449049 CEST	146.255.19.152	443	192.168.2.7	49710	CN=republica.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.	Thu Feb 04 11:00:51 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed May 05 12:00:51 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 4, 2021 15:39:46.676975965 CEST	13.225.74.97	443	192.168.2.7	49717	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		

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 4, 2021 15:39:46.723145962 CEST	13.225.74.97	443	192.168.2.7	49716	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 4, 2021 15:39:46.788299084 CEST	13.224.193.60	443	192.168.2.7	49718	CN=img.europapress.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	Tue Jun 16 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	Fri Jul 16 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		

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 4, 2021 15:39:46.788968086 CEST	13.224.193.60	443	192.168.2.7	49719	CN=img.europapress.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	Tue Jun 16 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	Fri Jul 16 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 4, 2021 15:39:46.934322119 CEST	13.224.193.60	443	192.168.2.7	49720	CN=img.europapress.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	Tue Jun 16 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	Fri Jul 16 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 4, 2021 15:39:47.101131916 CEST	199.232.194.133	443	192.168.2.7	49723	CN=*.albaeditorial.es CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Apr 26 22:21:49 CEST 2021	Sat May 28 22:21:48 CEST 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
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
May 4, 2021 15:39:47.101300955 CEST	199.232.194.133	443	192.168.2.7	49724	CN=*.albaeditorial.es CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Apr 26 22:21:49 CEST 2021	Sat May 28 22:21:48 CEST 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
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
May 4, 2021 15:39:47.272176981 CEST	151.101.2.133	443	192.168.2.7	49725	CN=cni-digital1.map.fastly.net, O="Fastly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Mar 29 18:12:10 CEST 2021	Sat Mar 26 14:09:35 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
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
May 4, 2021 15:39:47.273112059 CEST	13.225.74.99	443	192.168.2.7	49729	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 Apr 25 01:59:59 CEST 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
					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 4, 2021 15:39:47.286612034 CEST	151.101.2.133	443	192.168.2.7	49726	CN=cni-digital1.map.fastly.net, O="Fastly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Mar 29 18:12:10 CEST 2021	Sat Mar 26 14:09:35 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
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 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
May 4, 2021 15:39:47.287478924 CEST	13.225.74.99	443	192.168.2.7	49730	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 4, 2021 15:39:47.310153008 CEST	52.212.89.238	443	192.168.2.7	49728	CN=meneame.net 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	Sat Jan 02 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	Tue Feb 01 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 4, 2021 15:39:47.319683075 CEST	52.212.89.238	443	192.168.2.7	49727	CN=meneame.net 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	Sat Jan 02 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	Tue Feb 01 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 4, 2021 15:39:47.466960907 CEST	192.229.233.25	443	192.168.2.7	49734	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	Wed Nov 10 00:59:59 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
							Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					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 4, 2021 15:39:47.484309912 CEST	192.229.233.25	443	192.168.2.7	49733	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	Wed Nov 10 00:59:59 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
							Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					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 4, 2021 15:39:48.003976107 CEST	31.13.92.14	443	192.168.2.7	49737	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 4, 2021 15:39:48.016166925 CEST	31.13.92.14	443	192.168.2.7	49738	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:39:48.190032005 CEST	13.225.74.20	443	192.168.2.7	49739	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 4, 2021 15:39:48.210690022 CEST	13.225.74.20	443	192.168.2.7	49740	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 4, 2021 15:39:48.424429893 CEST	193.32.242.105	443	192.168.2.7	49748	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	Tue Jun 22 03:05:17 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 4, 2021 15:39:48.432892084 CEST	193.32.242.105	443	192.168.2.7	49747	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	Tue Jun 22 03:05:17 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 4, 2021 15:39:48.618469000 CEST	172.217.16.130	443	192.168.2.7	49749	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:36:35 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:36:34 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 4, 2021 15:39:48.620079994 CEST	13.224.193.31	443	192.168.2.7	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		

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 4, 2021 15:39:48.633018970 CEST	172.217.16.130	443	192.168.2.7	49750	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:36:35 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:36:34 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 4, 2021 15:39:48.742821932 CEST	13.224.193.31	443	192.168.2.7	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 4, 2021 15:39:49.240765095 CEST	142.250.185.227	443	192.168.2.7	49756	CN=www.google.de CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:41:49 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:41:48 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 4, 2021 15:39:49.240824938 CEST	142.250.185.227	443	192.168.2.7	49757	CN=www.google.de CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:41:49 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:41:48 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 4, 2021 15:39:49.247693062 CEST	74.125.140.155	443	192.168.2.7	49758	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 4, 2021 15:39:49.252089024 CEST	74.125.140.155	443	192.168.2.7	49759	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 4, 2021 15:39:49.292249918 CEST	142.250.185.194	443	192.168.2.7	49760	CN=*.googleadservices.com CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:40:58 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:40:57 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 4, 2021 15:39:49.292557955 CEST	142.250.185.194	443	192.168.2.7	49761	CN=*.googleadservices.com CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:40:58 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:40:57 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 4, 2021 15:39:49.347215891 CEST	142.250.186.98	443	192.168.2.7	49763	CN=*.google.de CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:46:01 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:46:00 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 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 4, 2021 15:39:49.349062920 CEST	142.250.186.98	443	192.168.2.7	49762	CN=*.google.de CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:46:01 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:46:00 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 4, 2021 15:39:49.450577021 CEST	142.250.186.34	443	192.168.2.7	49766	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:36:35 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:36:34 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 4, 2021 15:39:49.451131105 CEST	142.250.186.34	443	192.168.2.7	49767	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:36:35 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:36:34 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 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 4, 2021 15:39:49.909080029 CEST	13.224.193.91	443	192.168.2.7	49768	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 4, 2021 15:39:49.909220934 CEST	13.224.193.91	443	192.168.2.7	49769	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 4, 2021 15:39:55.712995052 CEST	34.98.67.61	443	192.168.2.7	49781	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 4, 2021 15:39:55.714593887 CEST	34.98.67.61	443	192.168.2.7	49783	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 4, 2021 15:39:55.722531080 CEST	35.244.174.68	443	192.168.2.7	49784	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 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 4, 2021 15:39:55.723762035 CEST	35.244.159.8	443	192.168.2.7	49785	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 4, 2021 15:39:55.723990917 CEST	35.244.159.8	443	192.168.2.7	49786	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 4, 2021 15:39:55.732021093 CEST	35.244.174.68	443	192.168.2.7	49782	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 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:39:55.745229959 CEST	185.64.189.115	443	192.168.2.7	49788	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 4, 2021 15:39:56.058798075 CEST	34.98.67.61	443	192.168.2.7	49791	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 4, 2021 15:39:56.191210032 CEST	185.64.189.115	443	192.168.2.7	49787	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 4, 2021 15:39:56.252998114 CEST	172.217.16.130	443	192.168.2.7	49792	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:36:35 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:36:34 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 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=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 4, 2021 15:39:56.263909101 CEST	172.217.16.130	443	192.168.2.7	49793	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:36:35 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:36:34 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 4, 2021 15:39:56.759427071 CEST	18.179.240.58	443	192.168.2.7	49794	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 4, 2021 15:39:56.761528969 CEST	18.179.240.58	443	192.168.2.7	49795	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 4, 2021 15:40:20.149255991 CEST	54.76.6.247	443	192.168.2.7	49804	CN=*.adsrvr.org CN=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	CN=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3 CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Thu Mar 18 23:45:32 CET 2021 Tue Jul 28 02:00:00 CEST 2020 Wed Mar 18 11:00:00 CET 2009	Wed Apr 20 00:45:32 CEST 2022 Sun Mar 18 01:00:00 CET 2029 Sun Mar 18 11:00:00 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=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
					CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Mar 18 11:00:00 CET 2009	Sun Mar 18 11:00:00 CET 2029		

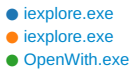
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:40:20.151808977 CEST	54.76.6.247	443	192.168.2.7	49805	CN=*.adsrvr.org CN=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	CN=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3 CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Thu Mar 18 23:45:32 CET 2021 Tue Jul 28 02:00:00 CEST 2020 Wed Mar 18 11:00:00 CET 2009	Wed Apr 20 00:45:32 CEST 2022 Sun Mar 18 01:00:00 CET 2029 Sun Mar 18 11:00:00 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=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
					CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Mar 18 11:00:00 CET 2009	Sun Mar 18 11:00:00 CET 2029		
May 4, 2021 15:40:26.400860071 CEST	31.13.92.36	443	192.168.2.7	49806	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 Tue Oct 22 14:00:00 CEST 2013	Sun Jul 04 01:59:59 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 4, 2021 15:40:26.442815065 CEST	31.13.92.36	443	192.168.2.7	49807	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 Tue Oct 22 14:00:00 CEST 2013	Sun Jul 04 01:59:59 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 4, 2021 15:40:26.886846066 CEST	31.13.92.36	443	192.168.2.7	49808	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 Tue Oct 22 14:00:00 CEST 2013	Sun Jul 04 01:59:59 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 4, 2021 15:40:26.887716055 CEST	31.13.92.36	443	192.168.2.7	49809	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 Tue Oct 22 14:00:00 CEST 2013	Sun Jul 04 01:59:59 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

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 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 4, 2021 15:40:27.489130974 CEST	31.13.92.36	443	192.168.2.7	49810	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 Tue Oct 22 14:00:00 CEST 2013	Sun Jul 04 01:59:59 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 4, 2021 15:40:27.532010078 CEST	31.13.92.36	443	192.168.2.7	49811	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 Tue Oct 22 14:00:00 CEST 2013	Sun Jul 04 01:59:59 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		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 4872 Parent PID: 792

General

Start time:	15:39:42
Start date:	04/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff62f920000
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: 5680 Parent PID: 4872

General

Start time:	15:39:43
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4872 CREDAT:17410 /prefetch:2
Imagebase:	0x1e0000
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: 7128 Parent PID: 792

General

Start time:	15:41:10
Start date:	04/05/2021
Path:	C:\Windows\System32\OpenWith.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\OpenWith.exe -Embedding
Imagebase:	0x7ff602ab0000
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