ID: 409520
Cookbook: browseurl.jbs
Time: 10:10:15
Date: 10/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

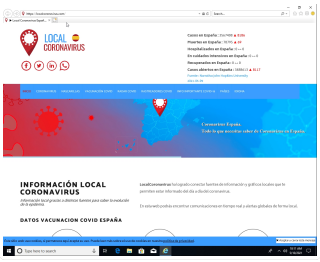
Analysis Report http://localcoronavirus.com

Overview

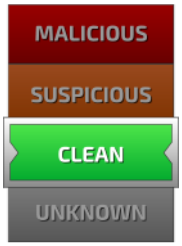
General Information

Sample URL:	http://localcoronavirus.com
Analysis ID:	409520
Infos:	

Most interesting Screenshot:



Detection

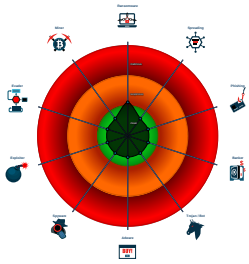


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5964 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5132 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5964 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- OpenWith.exe (PID: 5748 cmdline: C:\Windows\system32\OpenWith.exe -Embedding MD5: D179D03728E95E040A889F760C1FC402)
- **cleanup**

Malware Configuration

No configs have been found

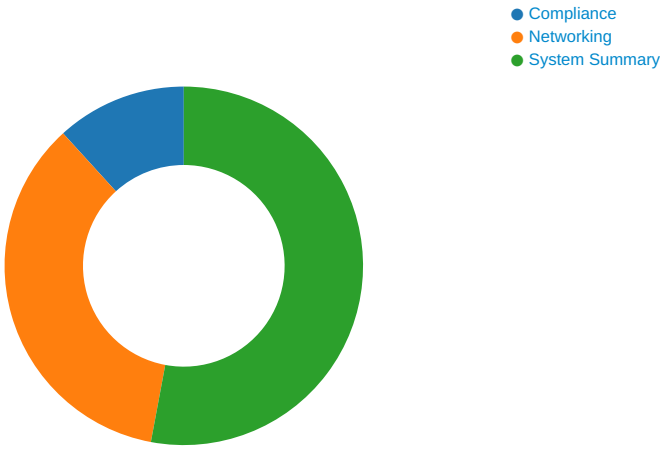
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



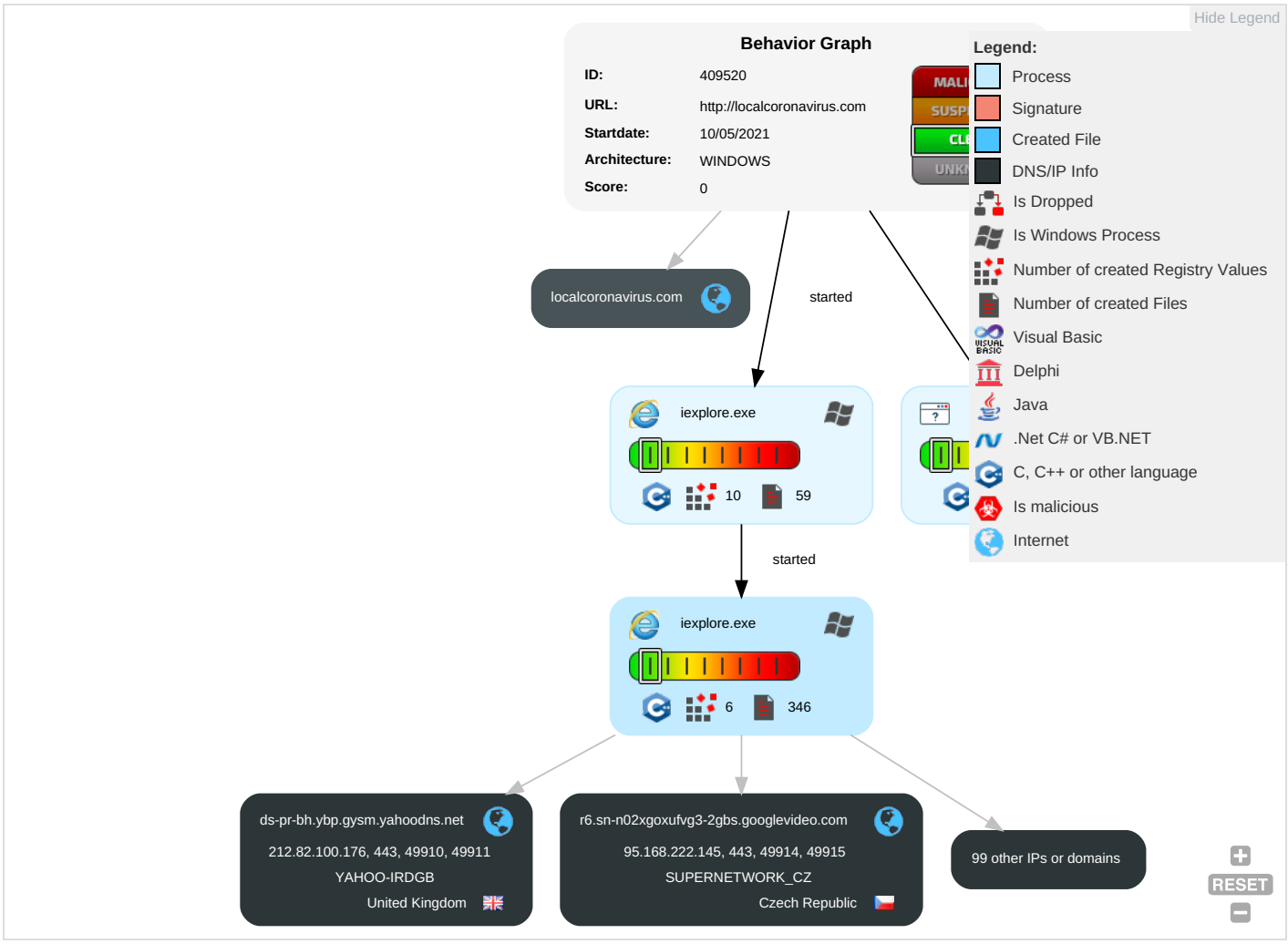
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billin Fraud

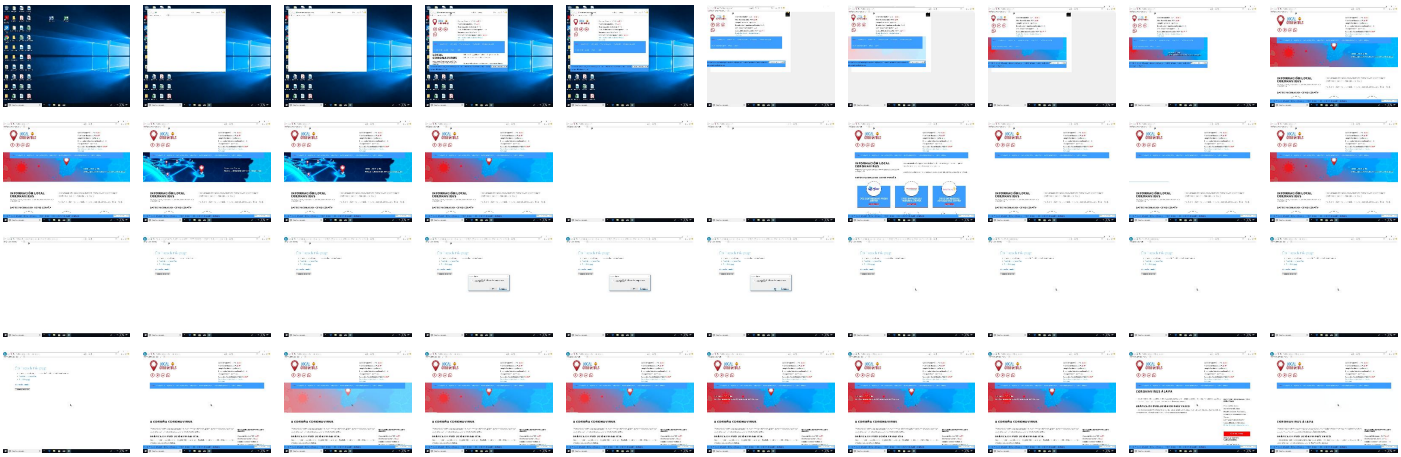
Behavior Graph

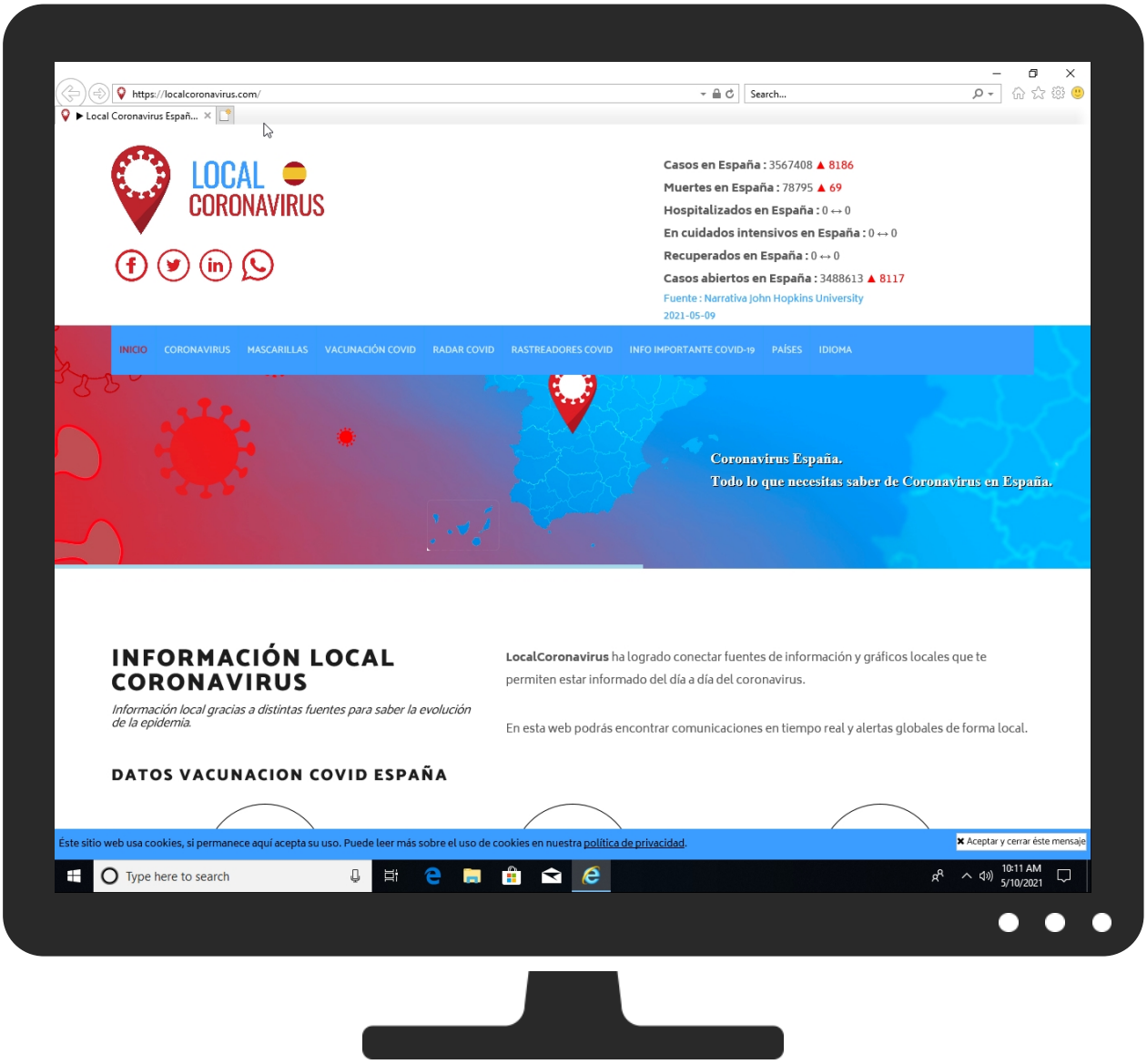


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://localcoronavirus.com	5%	Virustotal		Browse
http://localcoronavirus.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://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	

Source	Detection	Scanner	Label	Link
http://https://www.hotjarconsent.com/sv.html	0%	URL Reputation	safe	
http://https://cdn.contentspread.net/oliro/oba/oba_icon.png	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://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://sonspring.com/journal/clearing-floats	0%	Avira URL Cloud	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://labs.skinkers.com/touchSwipe/	0%	URL Reputation	safe	
http://labs.skinkers.com/touchSwipe/	0%	URL Reputation	safe	
http://labs.skinkers.com/touchSwipe/	0%	URL Reputation	safe	
http://https://www.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://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://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://cdn.contentspread.net/oliro/tools/js/addDoubleBorder.js	0%	Avira URL Cloud	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	
http://https://www.excelsior.com.mx/adrenalina/la-actriz-ana-bertha-espin-es-la-fuerza-del-jimmy/1447936	0%	Avira URL Cloud	safe	
http://https://www.muchacomida.com/comida-a-domicilio/alava	0%	Avira URL Cloud	safe	
http://https://www.eluniversal.com.mx/mundo/gritos-musica-y-fiesta-en-espana-por-levantamiento-parcial-de-r	0%	Avira URL Cloud	safe	
http://https://www.linkedin.c	0%	URL Reputation	safe	
http://https://www.linkedin.c	0%	URL Reputation	safe	
http://https://www.linkedin.c	0%	URL Reputation	safe	
http://https://cdn2.excelsior.com.mx/media/styles/imagen_redes_sociales/public/pictures/2021/05/10/2575967.	0%	Avira URL Cloud	safe	
http://https://innovacion.nwc10.com/inicia-tu-idea/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
puntodebreak.com	185.125.78.79	true	false		high
px2.px.quantserve.com	91.228.74.133	true	false		high
di7juyclzlgyp.cloudfront.net	13.32.25.102	true	false		high
eu-u.openx.net	34.98.64.218	true	false		high
dbpabf0off7y1.cloudfront.net	65.9.66.100	true	false		high
cdn.contentspread.net	85.114.131.233	true	false		unknown
rtb.openx.net	35.186.253.211	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
platform.twitter.map.fastly.net	199.232.136.157	true	false		unknown
tagr-gcp-odr-euw4.mookie1.com	34.98.67.61	true	false		high
cm.g.doubleclick.net	216.58.214.226	true	false		high
facebook.com	31.13.92.36	true	false		high
ds-pr-bh.ybp.gysm.yahoodns.net	212.82.100.176	true	false		unknown
dsp.active-agent.com	85.114.159.66	true	false		high
match-1943069928.eu-west-1.elb.amazonaws.com	52.30.50.112	true	false		high
dspcluster.adfarm1.adition.com	85.114.159.67	true	false		high
id.rlcdn.com	35.244.174.68	true	false		high
static-cdn.hotjar.com	13.32.25.105	true	false		high
match.prod.bidr.io	52.209.246.140	true	false		unknown
pugm22000nf.pubmatic.com	185.64.189.115	true	false		high
cs491300.wpc.mucdn.net	192.229.220.196	true	false		unknown
us-u.openx.net	35.244.159.8	true	false		high
stats.l.doubleclick.net	74.125.140.155	true	false		high
akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com	52.211.67.210	true	false		high
dsp.adfarm1.adition.com	85.114.159.93	true	false		high
proteccion10.net	193.32.242.105	true	false		unknown
cec01.eug.edgetcdn.io	51.68.35.185	true	false		unknown
googleads.g.doubleclick.net	216.58.214.194	true	false		high
adizio.geo.iponweb.net	35.210.53.219	true	false		unknown
pixel-origin.mathtag.com	185.29.132.68	true	false		high
vc-live-cf.hotjar.io	65.9.66.63	true	false		unknown
www.googletagservices.com	172.217.19.98	true	false		high
r6.sn-n02xgoxufvg3-2gbs.googlevideo.com	95.168.222.145	true	false		high
cc.adingo.jp	54.178.254.210	true	false		unknown
republica.com.uy	108.170.35.187	true	false		unknown
scontent.xx.fbcdn.net	31.13.92.14	true	false		high
ad14.ad-srv.net	176.9.26.250	true	false		high
aec01.esg.rtve.edgetcdn.io	51.195.63.237	true	false		unknown
script.hotjar.com	13.32.25.86	true	false		high
d1j70itqjm2icu.cloudfront.net	13.32.25.9	true	false		high
localcoronavirus.com	172.67.183.244	true	false		unknown
d2dzdx91mh5kpx.cloudfront.net	65.9.66.66	true	false		high
d3cra5ec8gdi8w.cloudfront.net	13.35.253.104	true	false		high
www.google.de	172.217.16.99	true	false		high
pagead46.l.doubleclick.net	172.217.19.98	true	false		high
alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com	18.195.54.133	true	false		high
d37ub18b7ivraq.cloudfront.net	99.86.2.109	true	false		high
multisite-support.geo.kaspersky.com	185.85.15.23	true	false		high
www.elconfidencialdigital.com	172.67.82.88	true	false		high
dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com	3.125.99.7	true	false		high
vars.hotjar.com	99.86.2.91	true	false		high
partnerad.l.doubleclick.net	216.58.214.226	true	false		high
ad.ad-srv.net	46.4.10.47	true	false		high
prisa-us-eu.map.fastly.net	199.232.194.133	true	false		unknown
www.google.ch	172.217.19.99	true	false		high
pm.w55c.net	unknown	unknown	false		high
www.republica.com.uy	unknown	unknown	false		unknown
img.europapress.es	unknown	unknown	false		high
ficheracos.publico.es	unknown	unknown	false		high
as01.epimg.net	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
static2.abc.es	unknown	unknown	false		high
static4.abc.es	unknown	unknown	false		high
match.adsrvr.org	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
odr.mookie1.com	unknown	unknown	false		high
c1.adform.net	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
imagenes.20minutos.es	unknown	unknown	false		high
www.awin1.com	unknown	unknown	false		high
cronicaglobal.elespanol.com	unknown	unknown	false		high
phantom-elmundo.unidadeditorial.es	unknown	unknown	false		high
media.kaspersky.com	unknown	unknown	false		high
r6---sn-n02xgoxufvg3-2gbs.googlevideo.com	unknown	unknown	false		high
sync.mathtag.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high
www.puntodebreak.com	unknown	unknown	false		high
image6.pubmatic.com	unknown	unknown	false		high
s1.eestatic.com	unknown	unknown	false		high
cdn2.excelsior.com.mx	unknown	unknown	false		unknown
ep00.epimg.net	unknown	unknown	false		high
vc.hotjar.io	unknown	unknown	false		unknown
phantom-expansion.unidadeditorial.es	unknown	unknown	false		high
pr-bh.ybp.yahoo.com	unknown	unknown	false		high
x.bidswitch.net	unknown	unknown	false		unknown
adservice.google.ch	unknown	unknown	false		high
pixel.quantserve.com	unknown	unknown	false		high
img.huffingtonpost.com	unknown	unknown	false		high
img2.rtve.es	unknown	unknown	false		high
pool.admedo.com	unknown	unknown	false		high

Contacted URLs

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

URLs from Memory and Binaries

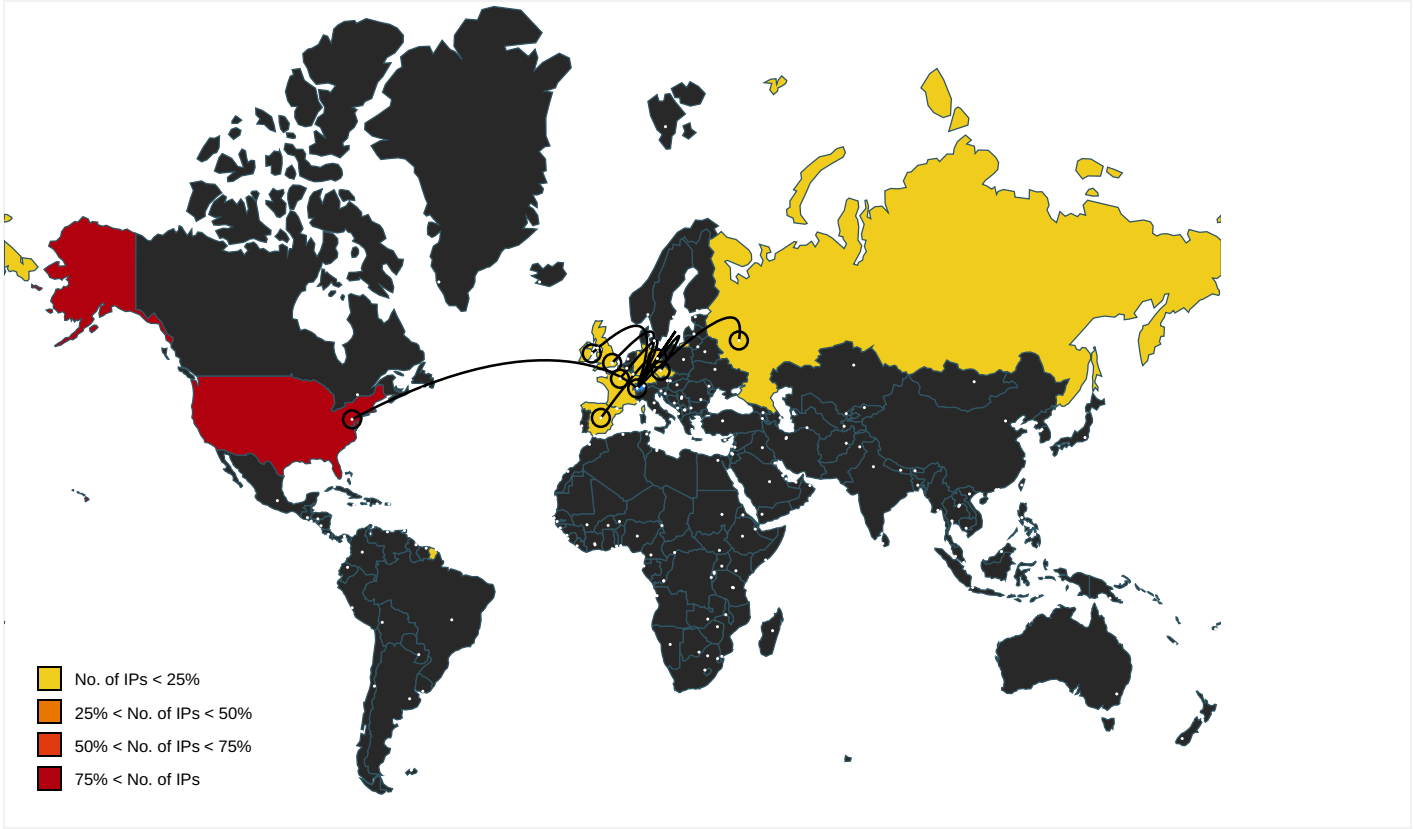
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.lavozdegalicia.es/default/2021/05/09/00121620573842504277471/Foto/O29Y8020.jpg	DWYDOY9Z.htm.3.dr	false		high
http://https://stats.g.doubleclick.net/g/collect	js[2].js.3.dr	false		high
http://https://www.hotjarconsent.com/sv.html	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.europapress.es/galicia/noticia-centros-dia-preparan-arrancar-desescalada-disminuir-25-oc	a-coruna-coronavirus[1].htm.3.dr	false		high
http://https://www.europapress.es/euskadi/noticia-delegado-gobierno-cree-no-momento-suavizar-medidas-euskad	alava-coronavirus[1].htm.3.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/interaction/%3Fai%3DCjIQS5eqYYMuqIcXt6gS0vYaIBpLuq6Vgg6Dv	ads[3].htm1.3.dr	false		high
http://https://www.elblogsalmon.com/mundo-laboral/todo-trabajo-que-se-ha-perdido-mundo-pandemia-puede-supon	DWYDOY9Z.htm.3.dr	false		high
http://https://imagenes.20minutos.es/files/og_thumbnail/uploads/imagenes/2021/05/04/coronavirus-madrid.jpeg	a-coruna-coronavirus[1].htm.3.dr	false		high
http://https://www.abc.es/espana/castilla-leon/abci-igea-si-tiene-volver-estado-alarma-gobierno-debe-dimiti	DWYDOY9Z.htm.3.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/html/r20210505/r20190131/zrt_lookup.html	{42ECE20D-B167-11EB-90EB-ECF4BBEA1588}.dat.2.dr	false		high
http://https://img.huffingtonpost.com/asset/6098cbc1260000e269b4296a.jpg?ops=1200_630	DWYDOY9Z.htm.3.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/interaction/%3Fai%3DCskMepuqYYK7nJszeywXs47C4ApKUvKtg86CT	ads[1].htm0.3.dr	false		high
http://https://phantom-elmundo.unidadeditorial.es/de450e428f4bd13b9bd4d4d7d5445edc/resize/1200/f/jpg/assets	DWYDOY9Z.htm.3.dr	false		high
http://getbootstrap.com/javascript/#tooltip	bootstrap[1].js.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ad14.ad-srv.net/viewability?s=6363240006114810090447901159001 4&a=92ba95ac&vb=v	request_content[1].htm.3.dr	false		high
http://https://cdn.contentspread.net/oliro/oba/oba_icon.png	request_content[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://getbootstrap.com)	bootstrap[1].css.3.dr	false	• Avira URL Cloud: safe	low
http://https://googleads.g.doubleclick.net/pagead/html/r20210505/r20190131/zrt_lookup.html#RS-0-&adk=181227	{42ECE20D-B167-11EB-90EB-ECF4BBEA1588}.dat.2.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.3.dr	false		high
http://https://cdn.ampproject.org/amp4ads-host-v0.js	f[1].txt0.3.dr	false		high
http://https://www.mscbs.gob.es/profesionales/saludPublica/ccayes/alertasActual/nCov/vacunaCovid19.htm	DWYDOY9Z.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.elmundo.es/ciencia-y-salud/salud/2021/05/10/6098bf1a21efa0e9398b45d6.html	DWYDOY9Z.htm.3.dr	false		high
http://https://www.lavozdegalicia.es/default/2021/05/09/00121620552901404464996/Foto/i09y1010.jpg	a-coruna-coronavirus[1].htm.3.dr	false		high
http://https://www.abc.es/gastronomia/abci-diez-restaurantes-donde-comer-buen-rabo-toro-madrid-202105100904	DWYDOY9Z.htm.3.dr	false		high
http://https://static.eldiario.es/clip/1068cc14-8437-42d1-baa8-9084e799bc4f_facebook-watermarked-aspect-rat	a-coruna-coronavirus[1].htm.3.dr	false		high
http://https://www.nwc10.com/politica-privacidad	alava-coronavirus[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.lavozdegalicia.es/default/2021/05/03/00121620068642701225646/Foto/L24A1025.jpg	alava-coronavirus[1].htm.3.dr	false		high
http://https://www.lavozdegalicia.es/noticia/sociedad/2021/05/09/mapa-festivo-gallego-ante-verano-pandemico	a-coruna-coronavirus[1].htm.3.dr	false		high
http://https://cdn.jsdelivr.net/npm/chart.js	alava-coronavirus[1].htm.3.dr, DWYDOY9Z.htm.3.dr	false		high
http://https://www.hotjarconsent.com/pl.html	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://sonspring.com/journal/clearing-floats	global[1].css.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/images/mtad/back_blue.png	ads[1].htm0.3.dr, ads[2].htm0.3.dr	false		high
http://https://www.hotjarconsent.com/fr.html	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/images/mtad/x_blue.png	{42ECE20D-B167-11EB-90EB-ECF4BBEA1588}.dat.2.dr, ads[3].htm1.3.dr, ads[4].htm.3.dr, ads[2].htm1.3.dr, ads[1].htm1.3.dr, ads[1].htm.3.dr, ads[4].htm0.3.dr	false		high
http://labs.skinkers.com/touchSwipe/	jquery.themepunch.tools.min[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://img.europapress.es/fotoweb/fotonoticia_20210509132417_1024.jpg	a-coruna-coronavirus[1].htm.3.dr	false		high
http://https://www.lavozdegalicia.es/noticia/sociedad/2021/05/03/xunta-decide-jueves-medidas-regiran-tras-e	alava-coronavirus[1].htm.3.dr	false		high
http://https://ep00.epimg.net/elcomidista/imagenes/2021/05/03/articulo/1620035561_444557_1620041680_rrss_no	DWYDOY9Z.htm.3.dr	false		high
http://www.modernizr.com/)	bootstrap[1].js.3.dr	false		high
http://https://www.20minutos.es/noticia/4690971/0/indicadores-epidemicos-siguen-descendiendo-primer-dia-sin	a-coruna-coronavirus[1].htm.3.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/interaction/%3Fai%3DChWlr5eqYYIKKFYmY7gT5hLuwDqTvv6Vi3vOi	ads[4].htm1.3.dr	false		high
http://https://ad14.ad-srv.net/viewability?s=6363240006114810090447901159001 4&a=92ba95ac&vb=m	request_content[1].htm.3.dr	false		high
http://https://imagenes.20minutos.es/files/og_thumbnail/uploads/imagenes/2021/05/10/primera-noche-en-barcel	DWYDOY9Z.htm.3.dr	false		high
http://https://ad14.ad-srv.net/viewability?s=6363240006114810090447901159001 4&a=92ba95ac&vb=e	request_content[1].htm.3.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&h=600&adk=	{42ECE20D-B167-11EB-90EB-ECF4BBEA1588}.dat.2.dr	false		high
http://https://ad.ad-srv.net/interaction.php?c=	request_content[1].htm.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.hotjarconsent.com/el.html	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.abc.es/espana/galicia/abci-feijoo-decaer-estado-alarma-jueces-no-merecen-estar-sometidos	a-coruna-coronavirus[1].htm.3.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/interaction/%3Fai%3DCZZfH4uqYYIDJLZPd6wS324bABZKE7-1hse-I	{42ECE20D-B167-11EB-90EB-ECF4BBEA1588}.dat.2.dr, ads[4].htm.3.dr	false		high
http://https://proteccion10.net/compras.html	alava-coronavirus[1].htm.3.dr, {42ECE20D-B167-11EB-90EB-ECF4BBEA1588}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap[1].css.3.dr	false		high
http://https://stats.g.doubleclick.net/g/collect?v=2&	js[2].js.3.dr	false		high
http://googleads.g.doubleclick.net	f[1].txt0.3.dr, f[2].txt0.3.dr	false		high
http://https://twitter.com/in	{42ECE20D-B167-11EB-90EB-ECF4BBEA1588}.dat.2.dr	false		high
http://https://www.hotjarconsent.com/zh.html	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/interaction/%3Fai%3DCWbcMwOqYYOSwCYi1ygWml7egDZKUvKtg86CT	ads[1].htm1.3.dr	false		high
http://https://www.hotjar.com	box-5e3cec51ed8e99df6977c199d27812d7[1].htm.3.dr	false		high
http://https://www.lavozdegalicia.es/default/2021/05/09/00121620586321924262441/Foto/GY10P34F5_205043.jpg	a-coruna-coronavirus[1].htm.3.dr	false		high
http://https://www.hotjarconsent.com/fi.html	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn.contentspread.net/oliro/tools/js/addDoubleBorder.js	request_content[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://platzi.com/r/nwc10/	alava-coronavirus[1].htm.3.dr, a-coruna-coronavirus[1].htm.3.dr	false		high
http://https://static4.abc.es/media/espana/2021/05/10/igea2-k0NH--1024x512	DWYDOY9Z.htm.3.dr	false		high
http://www.puntodebreak.com/2021/05/10/10-conclusiones-deja-mutua-madrid-open-2021	DWYDOY9Z.htm.3.dr	false		high
http://www.greensock.com/club/	jquery.themepunch.tools.min[1].js.3.dr	false		high
http://getbootstrap.com/javascript/#collapse	bootstrap[1].js.3.dr	false		high
http://getbootstrap.com/javascript/#modals	bootstrap[1].js.3.dr	false		high
http://https://www.infolibre.es/noticias/politica/2021/05/11/directo_infolibre_mayo_120312_1012.html	DWYDOY9Z.htm.3.dr	false		high
http://https://i.blogs.es/5837a8/todo-el-trabajo-que-22se-ha-perdido-22-en-el-mundo-por-la-pandemia---1/840	DWYDOY9Z.htm.3.dr	false		high
http://https://www.huffingtonpost.es/entry/gobierno-reforma-ley-estado-alarma_es_6098c329e4b0f73e530f3806	DWYDOY9Z.htm.3.dr	false		high
http://https://www.hotjarconsent.com/sq.html	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.hotjarconsent.com/it.html	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.elespanol.com/espana/politica/20210510/ultima-hora-covid-alarma-vacuna-directo-contagios	DWYDOY9Z.htm.3.dr	false		high
http://https://platform.twitter.com/widgets.js	alava-coronavirus[1].htm.3.dr	false		high
http://https://www.hotjarconsent.com	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://img.europapress.es/fotoweb/fotonoticia_20210506114015_1024.jpg	alava-coronavirus[1].htm.3.dr	false		high
http://https://img.europapress.es/fotoweb/fotonoticia_20210509113741_1024.jpg	a-coruna-coronavirus[1].htm.3.dr	false		high
http://https://www.20minutos.es/noticia/4689565/0/astrazeneca-y-el-dilema-de-que-hacer-con-las-segundas-dos	a-coruna-coronavirus[1].htm.3.dr	false		high
http://https://www.lavozdegalicia.es/default/2021/05/09/00121620560401825725153/Foto/GY9P5F1_133929.jpg	a-coruna-coronavirus[1].htm.3.dr	false		high
http://https://www.hotjarconsent.com/pt_br.html	modules.7225c79fe4e29708c611[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://getbootstrap.com/javascript/#affix	bootstrap[1].js.3.dr	false		high
http://https://amzn.to/31GOUWE	compras[1].htm.3.dr	false		high
http://getbootstrap.com/javascript/#popovers	bootstrap[1].js.3.dr	false		high
http://https://www.excelsior.com.mx/adrenalina/la-actriz-ana-bertha-espin-es-la-fuerza-del-jimmy/1447936	DWYDOY9Z.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ampproject.org/rtv/%	f[1].txt0.3.dr	false		high
http://https://googleads.g.doubleclick.net	f[1].txt0.3.dr, f[2].txt0.3.dr	false		high
http://https://static.hotjar.com/c/hotjar-	alava-coronavirus[1].htm.3.dr	false		high
http://https://www.elconfidencialdigital.com/articulo/ultima-hora/logista-gana-88-millones-euros-primer-sem	DWYDOY9Z.htm.3.dr	false		high
http://https://www.muchacomida.com/comida-a-domicilio/alava	alava-coronavirus[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.github.com/mattbryson	jquery.themepunch.tools.min[1].js.3.dr	false		high
http://https://amzn.to/2XQwbGR	compras[1].htm.3.dr	false		high
http://https://cronicaglobal.elespanol.com/uploads/s1/14/51/01/19/planas_12_658x347.jpeg	DWYDOY9Z.htm.3.dr	false		high
http://https://www.lavozdegalicia.es/noticia/amarina/2021/04/28/bodas-variopintas-medievales-indianas-pasan	a-coruna-coronavirus[1].htm.3.dr	false		high
http://https://www.eluniversal.com.mx/mundo/gritos-musica-y-fiesta-en-espana-por-levantamiento-parcial-de-r	a-coruna-coronavirus[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.linkedin.c	{42ECE20D-B167-11EB-90EB-ECF4BBEA1588}.dat.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn2.excelsior.com.mx/media/styles/imagen_redes_sociales/public/pictures/2021/05/10/2575967.	DWYDOY9Z.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/interaction/%3Fai%3DCPs70puqYYMrWL4zDywXwyo6IDOun0atewdq1	ads[3].htm.3.dr	false		high
http://https://innovacion.nwc10.com/inicia-tu-idea/	alava-coronavirus[1].htm.3.dr, a-coruna-coronavirus[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.europapress.es/castilla-lamancha/noticia-psoe-aboga-ejercer-libertad-responsabilidad-pid	a-coruna-coronavirus[1].htm.3.dr	false		high
http://https://www.elconfidencialdigital.com/media/elconfidencialdigital/sections/ecd-logo-mini-2.png	DWYDOY9Z.htm.3.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.82.88	www.elconfidencialdigital.com	United States		13335	CLOUDFLARENETUS	false
54.178.254.210	cc.adingo.jp	United States		16509	AMAZON-02US	false
35.210.53.219	adizio.geo.iponweb.net	United States		19527	GOOGLE-2US	false
31.13.92.36	facebook.com	Ireland		32934	FACEBOOKUS	false
13.35.253.104	d3cra5ec8gdi8w.cloudfront.net	United States		16509	AMAZON-02US	false
85.114.159.67	dspcluster.adfarm1.adition.com	Germany		24961	MYLOC-ASIPBackboneofmyLocmanagedITAGDE	false
85.114.131.233	cdn.contentspread.net	Germany		24961	MYLOC-ASIPBackboneofmyLocmanagedITAGDE	false
85.114.159.66	dsp.active-agent.com	Germany		24961	MYLOC-ASIPBackboneofmyLocmanagedITAGDE	false
185.125.78.79	puntodebreak.com	Spain		60458	ASN-XTUDIONETES	false
212.82.100.176	ds-pr-bh.ybp.gysm.yahoodns.net	United Kingdom		34010	YAHOO-IRDGB	false
65.9.66.100	dbpabf0off7y1.cloudfront.net	United States		16509	AMAZON-02US	false
176.9.26.250	ad14.ad-srv.net	Germany		24940	HETZNER-ASDE	false
18.195.54.133	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
185.85.15.23	multisite-support.geo.kaspersky.com	Russian Federation		200107	KL-EXTRU	false
52.211.67.210	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
216.58.214.226	cm.g.doubleclick.net	United States		15169	GOOGLEUS	false
95.168.222.145	r6.sn-n02xgoxufvg3-2gbs.googlevideo.com	Czech Republic		39392	SUPERNETWORK_CZ	false
192.229.220.196	cs491300.wpc.mucdn.net	United States		15133	EDGECASTUS	false
3.125.99.7	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
65.9.66.80	unknown	United States		16509	AMAZON-02US	false
74.125.140.155	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
172.217.19.99	www.google.ch	United States		15169	GOOGLEUS	false
35.244.174.68	id.rlcdn.com	United States		15169	GOOGLEUS	false
34.98.67.61	tagr-gcp-odr-euw4.mookie1.com	United States		15169	GOOGLEUS	false
216.58.214.194	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
31.13.92.14	scontent.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false
13.32.25.9	d1j70itqjm2icu.cloudfront.net	United States		7018	ATT-INTERNET4US	false
108.170.35.187	republica.com.uy	United States		20454	SSASN2US	false
35.244.159.8	us-u.openx.net	United States		15169	GOOGLEUS	false
46.4.10.47	ad.ad-srv.net	Germany		24940	HETZNER-ASDE	false
85.114.159.93	dsp.adfarm1.adition.com	Germany		24961	MYLOC-ASIPBackboneofmyLocmanagedITAGDE	false
199.232.194.133	prisa-us-eu.map.fastly.net	United States		54113	FASTLYUS	false
52.30.50.112	match-1943069928.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
13.32.25.86	script.hotjar.com	United States		7018	ATT-INTERNET4US	false
99.86.2.91	vars.hotjar.com	United States		16509	AMAZON-02US	false
185.64.189.115	pugm22000nf.pubmatic.com	United Kingdom		62713	AS-PUBMATICUS	false
91.228.74.133	px2.px.quantserve.com	United Kingdom		27281	QUANTCASTUS	false
99.86.2.109	d37ub18b7ivraq.cloudfront.net	United States		16509	AMAZON-02US	false
51.68.35.185	cec01.eug.edgetcdn.io	France		16276	OVHFR	false
35.186.253.211	rtb.openx.net	United States		15169	GOOGLEUS	false
51.195.63.237	aec01.esg.rtve.edgetcdn.io	France		16276	OVHFR	false
172.67.183.244	localcoronavirus.com	United States		13335	CLOUDFLARENETUS	false
65.9.66.63	vc-live-cf.hotjar.io	United States		16509	AMAZON-02US	false
34.98.64.218	eu-u.openx.net	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.32.242.105	proteccion10.net	Spain		41705	GRUPOBALADIGES	false
185.29.132.68	pixel-origin.mathtag.com	United Kingdom		30419	MEDIAMATH-INCUS	false
65.9.66.66	d2dzdx91mh5kpx.cloudfront.net	United States		16509	AMAZON-02US	false
13.32.25.102	di7juyclzlgyp.cloudfront.net	United States		7018	ATT-INTERNET4US	false
52.209.246.140	match.prod.bidr.io	United States		16509	AMAZON-02US	false
13.32.25.105	static-cdn.hotjar.com	United States		7018	ATT-INTERNET4US	false
199.232.136.157	platform.twitter.map.fastly.net	United States		54113	FASTLYUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	409520
Start date:	10.05.2021
Start time:	10:10:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 19s
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:	12
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@4/253@64/52
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/ • Browsing link: https://localcoronavirus.com/a-coruna-coronavirus • Browsing link: https://localcoronavirus.com/alava-coronavirus

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 52.113.196.254, 13.107.3.254, 104.43.193.48, 13.107.246.254, 92.122.145.220, 104.42.151.234, 88.221.62.148, 172.217.20.10, 172.217.16.104, 142.250.186.142, 172.217.18.66, 92.122.213.154, 92.122.213.162, 151.101.2.109, 151.101.66.109, 151.101.130.109, 151.101.194.109, 172.217.16.99, 52.255.188.83, 172.217.20.14, 172.217.19.98, 172.217.19.100, 172.217.19.97, 172.217.20.3, 69.173.144.139, 69.173.144.138, 69.173.144.165, 37.157.6.252, 37.157.4.28, 37.157.4.23, 37.157.4.41, 37.157.6.242, 37.157.6.246, 37.157.2.237, 37.157.2.236, 20.82.210.154, 152.199.19.161, 92.122.213.247, 92.122.213.194, 13.88.21.125, 74.125.198.94, 74.125.198.120, 95.101.22.163, 92.123.148.9 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, www.publico.es.edgekey.net, s-ring.msedge.net, partner.googleadservices.com, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, e11290.dspg.akamaiedge.net, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, www.google-analytics.com, fonts.googleapis.com, e12881.ksd.akamaiedge.net, pagead2.googlesyndication.com, s-ring.s-9999.s-msedge.net, skypedataprdcolcus15.cloudapp.net, t-9999.t-msedge.net, www3.l.google.com, s-9999.s-msedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, csi.gstatic.com, t-ring.t-9999.t-msedge.net, cs9.wpc.v0cdn.net, a1972.g2.akamai.net, pixel.rubiconproject.net.akadns.net, store-images.s-microsoft.com-c.edgekey.net, adservice.google.com, track.adformnet.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, iecvlist.microsoft.com, teams-9999.teams-msedge.net, e12564.dspb.akamaiedge.net, go.microsoft.com, www.googletagmanager.com, arc.trafficmanager.net, img-prod-cms-rt-microsoft-com.akamaized.net, dualstack.f3.shared.global.fastly.net, www.awin1.com.edgekey.net, static-abc.akamaized.net, e30101.b.akamaiedge.net, www-google-analytics.l.google.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, t-ring.msedge.net, skypedataprdcoleus17.cloudapp.net, tpc.googlesyndication.com, go.microsoft.com.edgekey.net, analytics.google.com, teams-ring.teams-9999.teams-msedge.net, teams-ring.msedge.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing network information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:12:07	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\E5F0NRSV\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):	1112262
Entropy (8bit):	5.20644013889706
Encrypted:	false
SSDEEP:	24576:cjxjxjWjKjKj8jsjsjKjsjsjsjZjnjnjnj3j4j3jTjej0jijjkj1jZjYjYjYjYv:cjxjxjWjKjKj8jsjsjKjsjsjsjZjnjnv
MD5:	A59C91103824E6389199363E411B68E9
SHA1:	42E33477E7E5CE4EA846F5BAEDFB501C29E1EFBF
SHA-256:	9243072742FA411D94E36386075F0D98BA1599EC2C11DFE77141ACD4CFD3B7DC
SHA-512:	2D15F55B5D5130820F77BB0C0225AA54105BBD8A3283E84EB575CB35C4A7721DBF698181F5B0AB22B82DF87182BDBFDA5EAA02A56BF946D170F28395B8ED064F
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="goog_pem_mod" value="269" ltime="142008144" htime="30885236" /><item name="google_experiment_mod34" value="198" ltime="142318144" htime="30885236" /><item name="google_experiment_mod53" value="176" ltime="142318144" htime="30885236" /><item name="google_experiment_mod36" value="58" ltime="142318144" htime="30885236" /><item name="google_experiment_mod37" value="494" ltime="142318144" htime="30885236" /><item name="google_experiment_mod44" value="745" ltime="142318144" htime="30885236" /></root><root><item name="goog_pem_mod" value="269" ltime="142008144" htime="30885236" /><item name="google_experiment_mod34" value="198" ltime="142318144" htime="30885236" /><item name="google_experiment_mod53" value="176" ltime="142318144" htime="30885236" /><item name="google_experiment_mod36" value="58" ltime="142318144" htime="30885236" /><item name="google_experiment_mod37" value="494" ltime="142318144" htime="30885236" /><item name="google_experiment_mod44" value="74

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\URW0GA4Q\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:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FED
Malicious:	false
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{42ECE20B-B167-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{42ECE20B-B167-11EB-90EB-ECF4BBEA1588}.dat	
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.8696585485256638
Encrypted:	false
SSDEEP:	192:rtZeZk22WCtjif/tzzM+7BhhDcsfct6jrQil:rDKzt6ESyXLBf
MD5:	707ECC78A7CAC54E2E140D4EB70C76C5
SHA1:	F1CE13AEBC16DDDDA05DEAEA8943E87A7528CAF3
SHA-256:	2C0EC876E00DAE4AEC0418EAB6DE944C8CE828C6B6ED27E53655B7AC56AA4667
SHA-512:	082B789F787B4C6723177FDF283CF0599ECC6783072743D615B2F60F6766004EFD0A84513BB334DCF5CEB77E40028455B99D09DAD8562E268FE920137ED961C5
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\{42ECE20D-B167-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	1958614
Entropy (8bit):	4.092430799476353
Encrypted:	false
SSDEEP:	6144:fs3oNuTp4qEes3oNuTp4b5zuD6Nuv5zuD6NugP6amCjmNuAk6iCjmNuAfQ:fYywYyJEVEa6amEAk6iEA4
MD5:	3ECDEDAF34DB1304882114F853FF5885
SHA1:	809704652472F87BA2638AEFB282AE287E638006
SHA-256:	B0A3D229812AD7E99AC212F963D09E44EAC5FB32DD89D6E8FDD202856AFD1447
SHA-512:	E018967FDF07D1905BD94B09C0838E71351AE8A0B8BE18BDA69711F44DE4EE827E45D7EF022FFE86C5FA7A793E80E502CB0D6E93F6A5C3EC768F7EBEBE96C5A5
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\{4D45403E-B167-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5652101416160202
Encrypted:	false
SSDEEP:	48:Iwy0GcprEfGwpaUG4pQmGrapbScGQpK+G7HpRJTGIpG:ryoZEpQk6oBS0A5TvA
MD5:	08703B5E528B60962C4DF43B1550D9AA
SHA1:	60D481A97989A7AFEC151C4B83989D37F7E6A6D5
SHA-256:	13165E9A66782DD04366939E3786EE2EF7E2EED09E666D6564B718ECB3801E53
SHA-512:	2DCCB176D136F26378EA1E25C2BFC58C052CD4F54FCBAB9F39BFA84C8715316B020402594381A33D896AFE092AA36BC83D091C78328C8D3683A1DCB9F7DB3A2
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	5893
Entropy (8bit):	7.725263353847225
Encrypted:	false
SSDEEP:	96:ohuQ5Vo7FhknmWpYOxYbOLMHfmH0mgzdtsfNFeC933ktunIOys60yiiLEgY4yJVZ:oEQ07FhknOuM/muPs1Fqmd9nyiiZq7

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat</th></tr>
<tr><td>MD5:</td><td>2EAD016ECE3CE23FB53C3FC42B03C962</td></tr>
<tr><td>SHA1:</td><td>1C1FCB96823F8F7EF60D20D51BF768410256DA87</td></tr>
<tr><td>SHA-256:</td><td>D947BAF83AE6355160FDFA16DB5D7B68D20E003144A2F7B286E18248306E58F0</td></tr>
<tr><td>SHA-512:</td><td>681A82F9AA7E565BFCEC063757ECC4C14EC46A110AC8E7D240AC92E59D635866A280C87632DAC572C7EF2D35458A277700463A37EDEC8F08080E5F764092CC</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>Preview:</td><td>(.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.@,=.YA
x...U.;..b.p...azTd.7p....E.Z...<.....O..S?.....pHYs...#...#.x.?v....iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xm
lns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
<rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xap/1.0
/sType/ResourceEvent#" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/"</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\mms\I9NF2D02\videoplayback[1].dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ISO Media, MP4 v2 [ISO 14496-14]
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	7.4010577646464855
Encrypted:	false
SSDEEP:	24576:C1LYie57mOwo1RgQfXxvWS967d8l7L9i1p6k0w1haE/decBFXy:qhs7mhoYyv6ml7L9i6kL18E/deSFi
MD5:	BC20926BA80D72469451076CE182DAD2
SHA1:	728691C2CA4640CFF648648A1A3F7535A2E09F98
SHA-256:	86FE3354D7EE55A855329A480B4888D4AD3E4579AA9330A7AFE82C98437A45DA
SHA-512:	7647D8782212950D26E71FE67E0CB7C04560634CA312BAA1C5B064E28C0A6EF8E550168879AB49D0201C62B0B60AE25F003D1FDB0452B051130988236EF08CCF
Malicious:	false
Reputation:	low
Preview:	....ftypmp42....isommp42....moov...lmvhd...............7...@..................................trak...\tkhd...................7x...@..... ...h...../mdia... mdhd............2.....U......_hdlr........vide...........ISO Media file produced by Google Inc. Created on: 04/02/2019......minf...$dinf....dref............url ....hstb l....stsd............avc1..........................h.H...H..2avcC.B......gB........Z........ ...A......h.<.....stts...........c.......Xstsc.. ....stco..................b..%...}i......nw..................a.._8..1....X......{_...X...E..N......p...!..........V....Q...A..c{...L..9-....stsz...........c..#].......%.......>...A...I..............>... c..................2..............>...A............

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\15168161373849[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1200x1474, frames 3</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>533468</td></tr>
<tr><td>Entropy (8bit):</td><td>7.978764784772052</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>12288:fxY4adgrESOk6UFT62M+EQOR9MmsHm8UejRpL94ZuhV1UmTJU:ZdadgIS7VT6jaOR2mt8ZRXzhV1UmTJU</td></tr>
<tr><td>MD5:</td><td>BD25A1C1C570D514F7087FECBECD1247</td></tr>
<tr><td>SHA1:</td><td>50CF521D9BE29CDDEA7192F2EDBB6053A40F940C</td></tr>
<tr><td>SHA-256:</td><td>8E9C2DA04133E2E1D812C3A426C2728BD6D9D7C6F3F191A050C006282F98771A</td></tr>
<tr><td>SHA-512:</td><td>19B08DA48C2B5FEA59BEC4DFE04712772BAA25EFCFDC3D6249AC8BD0DC0725966A1180BC0BD5EF214EA479C67831D82F5890E5503A7478CD92F2EFBDE355A
E8</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://phantom-
expansion.unidadeditorial.es/45a148aa3fab38e202c7b4ba1e15612b/crop/0x0/2048x2515/resize/1200/f/jpg/assets/multimedia/imagenes/2018/01/24/15168161373849.jpg</td></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`.....C....................................%...#... , #&')*)..-0-(0%()(...C...........(...((...`.........................!1.A<br>Q."aq...2..#B....Rb..$3r..C.....4Sc...%Ds..&5Td.6Et....u..e...U.................................I......................!1..A."Qa.2q.........#BR...3.Sb....Cr.$.Tc..D..............?.. .0.`.MN..5g.O...
.D%_.E.&.'.B...#.j<.....m*C..V...<P.|.Y.'&=l.'..*....8.*.;+.-1V...XCO....1...+..'..\S......c..n...Q..rL.K..yD..j...W.f...H..ob.{.Xq9\L.u....#......6.5'.....T..#.x......#S...7Ez.p...Ix..3.Xq...'.......
w....7..V.'EjO.E.&X........J...u..3v.i.Z'u6.......{.N..[.3.p...X..c(.-H..Li*P...;....Mk.U....(.MZ...._..).....+.lB..D..7h..i..{7?.P...(.5..g......u.(n...;.Y.2..4S..[X..yx..f..:.PkVp.....wt....T;.N..?y
P*<..Q-.a)aK-...9.T...P....`5.9..\[*.T....;..7..?..,.2...=.....8}......Ik.L.-v.....S..~ufn...x.?.......D...%.^..M...t.v.</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\16183521443969[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, 1200x800, frames 3
Category:	downloaded
Size (bytes):	108838
Entropy (8bit):	7.9586818993717365
Encrypted:	false
SSDEEP:	3072:bC/ZOZI/z+U7X4T+dXFN7VQpvQLl+yifBG9oc:bC/ZfaU86dXFNhQKLlRi1c
MD5:	F5108D88A29018A9CB269E51EA281F4A
SHA1:	5FB15B1FF7A790231E572399605F49EF55D5E53D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\16183521443969[1].jpg

SHA-256:	867F63309DECC838A4D33157100C16EB9E0829C06C36061DE399424AD4BC105C
SHA-512:	8C75725D300F542990D79583D95A68D8307AD5CCEC3E18578F9DD5D477BD9E7E390C435B727F5F29352422A1C874CBB3B0AACD9E79784871BC34B49BECC98F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://phantom-expansion.unidadeditorial.es/04eaaedf7c88f097ad1fdefc32c89c6d/crop/0x0/2044x1363/resize/1200/f/jpg/assets/multimedia/imagenes/2021/04/14/16183521443969.jpg
Preview:	......JFIF.....`.`.....@ICC_PROFILE......0ADBE....mntrRGB XYZ ....3.;acspAPPL....none..........................-ADBE...cprt.......2desc...0...kwtpt.. ......bkpt........rTRC........gTRC........bTRC........rXYZ........gXYZ........bXYZ........text....Copyright 2000 Adobe Systems Incorporated...desc........Adobe RGB (1998).......... ....XYZ ....Q........XYZ ....curv.........3..curv.........3..curv.........3..XYZ ....O.....XYZ ......4....,....XYZ ......&1.../.......C........ ....%...#... , #&')*)..-0-(0%()(...C...........(...((...... ....L........................!1A..Qa"q...2B..#R..b.... $3Cr.....%4SDs.&..Tc..................................9........................!1A.Q."2a.q....BR...#3..Cb..$r.............?...kl.@Z.h..-.h.@Z.@A.5.Nb.....e..A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1620035561_444557_1620041680_rrss_normal[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v70), quality = 100", baseline, precision 8, 720x377, frames 3
Category:	downloaded
Size (bytes):	121080
Entropy (8bit):	7.686358632148006
Encrypted:	false
SSDEEP:	3072:oySkli2pc6UgabwYtXOb3n4jCVedDaOPcg:oySkB1Urtm34+VedaOPcg
MD5:	B61D36C0D8D8A642224EC7FBBD220543
SHA1:	87D4F8CC457AC931FAE2B20AEB3EB84F0E79C2FC
SHA-256:	6CB3222630AAE328EF18F27336C0C92F92A139BD375C6014C16EC132700BE0B5
SHA-512:	3B630CF520DEE95593FB5A02F0D5D4D55571A2863CC684FE272C3E36B7324AFE2A393210E35F03D0D71B19AB5E18EA2FD97787514A348076F31F14F211C2187B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ep00.epimg.net/elcomidista/imagenes/2021/05/03/articulo/1620035561_444557_1620041680_rrss_normal.jpg
Preview:	......JFIF.............<CREATOR: gd-jpeg v1.0 (using IJG JPEG v70), quality = 100....C..C.. ......y...."..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....?...........k..>...........;.{.....p.M..........W.~..........db.g.c..A............O....Z.t;x!..G...q.{......yko....?.?.../_....Y..WC...[.....Q..zW..^...?........V...+........_.. >...H<9............S.....}..ly|...............c.\A......=............?...<.-.=}...^....a0?...#.......T....^;v.n...WO.A.?.X....>?.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\20210413101942-diplomasin-texto[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 2019 (Macintosh), datetime=2019:12:11 02:13:51], baseline, precision 8, 6366x4562, frames 3
Category:	downloaded
Size (bytes):	3283726
Entropy (8bit):	6.676057012477454
Encrypted:	false
SSDEEP:	49152:Xp+yLWDnWefILlk0cEKaRrpWUCdvC3gjNUU6crWtc:Xp+P7WefImjEvWtC3EaMWe
MD5:	5B8E51745BD97FD4367755D7E25AAEBC
SHA1:	BB785D146B4EE6154C80879131A486F6F78DD3E6
SHA-256:	98610E80B8429F9CC9108100F066B2CD82C14E9ACE1539CB93FAA1B4C04D8A39
SHA-512:	F01493A16704461CAD078323786284EE81C18C496D22EF3F3013293FFDCB86152B6E114387A96344F396332F69F205339DB4766674213F1D38FBC5F3FAA9A0B5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ficheracos.publico.es/images/thumbnails/2021/20210413101942-diplomasin-texto.jpg
Preview:	......Exif..MM.*............................b...........j.(...........1.....$...r.2...........i...............-....'..-....'.Adobe Photoshop CC 2019 (Macintosh).2019:12:11 02:13:51...................................... ....&.............(.....................6..................H.......H..........Adobe_CM......Adobe.d.. ....s...."................?..3......!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'..............Vfv........7 GWgw........................5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%......&5..D.T..dEU6te....u..F...............Vfv........'7GWgw.................?...I%q.I$.JRI$...I$.$.I)I$.JRI$...I$.$. I)JU..9_....T.T..r....$....$I...w.*X..sj ....S.pn.].q.....G.j.Zd.I.)$.IJI$.x....0...J`..z...`k. ...;.5.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\2575967[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, progressive, precision 8, 664x498, frames 3
Category:	downloaded
Size (bytes):	127678
Entropy (8bit):	7.9885367426910845
Encrypted:	false
SSDEEP:	3072:cdFHa3UunsogFMhxaIuJXD1C/1+XOtStMOeVXSS:W+sNU/E8St9eVXZ
MD5:	DE432888AC3C58BC6D85F829ACEED73E
SHA1:	C47A1EB0649BCC86E4A623494DC54A9642886AA0
SHA-256:	8F7C265E9E59CEBEF6DE5D4040A00847BE8ABC730C89B9B29BE1EFBE783B36F6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\2575967[1].jpg	
SHA-512:	7D8C3D998F897D9481DB8A128C56E599D9D185FC57293B801D0DD369E799FBFDAD26D6EFE97E8C486EB3A37BECFF0D805EDBCBEC1032DA032F970CEA53FF5 44
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.excelsior.com.mx/media/styles/imagen_redes_sociales/public/pictures/2021/05/10/2575967.jpg

Preview:

......JFIF............C...C..."..J.o...!
.......fN...I.....#.n..V.g..{.=..J;....k......4}..".v.;_c.+..O.m..........Gn.7,.#.....n..a.x\......'.-.N..g.p..X....o.F.@....D.o.v....._9.MTS;.,..'..D..*./Z...-.5.l....`.'.!.I.d;..|...^..I_S..hJ...y=....FF.J~.;
X....!..8..=..U.&..Hb..].sZ..:.....lA..%HB.w...Qf.Mk...=.s.1.;..[V.h.....HL.b..yn.:.nZ.......6}u...E.].....<%.W....B6....U...#..%h*.r..c..M..K.OG7..e....F,....hD8`<.VJ.LI..G7.l...~.7.<....^k
.|..[...b..D]...3w:.3..|.r;D.k...]k.Y^.:.....U.Q..r.$.TvA+.cV....q.|\.!-$udF....../...,.#"56.Yf....8...e.B.0.f+s6W..Xe.}...Dd5.$..jB...mVIK...Xs ...%..L.2n........h....>.9.@.|.t..+..V.n1c...
A......S.r.N....o.o.a.....N5..}.....'.z...._t..y.....r.`s.w....v....F.Q.(.....v..........M.AV.B..M.U...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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):	84
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEqjdfXPQE/xlEy:1QEoqh3QEoy
MD5:	6A3F2D147842187CD48B1546EDDD5BA0
SHA1:	AB278C31189DF2939428CF81A3850A2C6DBF5E2E
SHA-256:	D4990F907BCA02F02B3D41216EEA5461609D4BCBA07A3CBEE0D7CF28A6D0D864
SHA-512:	998F55BF5C3D4A71CB3C23782B788F71E7625DF83A37FE8A18F915AAA3BDE5420183A3C709816664E262069EE2FE245CA44799E3476B6DE507B5D68FC86F8960
Malicious:	false
Reputation:	low

Preview:

GIF89a.............!.......,...........D.;GIF89a.............!.......,...........D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\579456311_184747324_600x315[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 600x315, frames 3
Category:	downloaded
Size (bytes):	19265
Entropy (8bit):	7.957211166088654
Encrypted:	false
SSDEEP:	384:yqKEF4OAb1AlWOhAeBgkx/5WBFgjnrSG05mcF34Pg20pWHq90h8W1WcOI7on:tKwIkxUHiudF3U8WH+n
MD5:	C8277F7237B7E02EA89BC906B497E883
SHA1:	C5536CDF48197CA2F2AF6806E8836DBBF3DBDEBC
SHA-256:	99D6898B86B8F41B0C57368E4AEC1375210CEC6CC43461042FD586789E1072B9
SHA-512:	3384093821C0DB2E61E7086C83C1060A42A4038DD1A56FC5ADA41E37C95FD0CE57A54F45FBE8C611325C3251A9AFE67DD0A355A56A9A82DCE9DADEF8E5C4B 60
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s1.eestatic.com/2021/05/07/ciencia/salud/579456311_184747324_600x315.jpg

Preview:

......JFIF.....,.,.....C....................................%...#... , #&')*)..-0-(0%()(...C..........(...((......;.X..!..D..................
......!1.A.Qa.."2q.Bb..#R....3.%CDc...$...4STr...............................&.....................!1..A..Qa."#2qB............?.......r.....!.F..F.Gt.p.yK......Qx....7......~.b..@.Q5.t.......+.7..`.6R..;.....5
^A.Xu...?+PQ..by..;...;uu.G.?.B..y'.l..7..OX..t.I+.t.9%m2,...z.|..E.I..O.*Zph...M,U......\...7#-'b...]'.s}.......r.~\..u.t.5}9ud.1..v.^.d...[.5#....g..c.v!y._G..Ko.f..O...^...........S.=Vr.N
......J+-.`}%.dS9.....`.y...k..+.....I7.f............E.S&..-...6....5...*4.,.M....X.t.....J#%...6M!..B..<..I.j......Q....4m..rR.&|H..E.k.>...z...7.i".....p.g.........C...Y.....7.k..|y.<.!z\H.....b....
B0..#;e..Pp...B....(8B........`.D ..*7pPFxK.C....OI......I$...j.+;Dp.....^[P.c.JMK...xj.j..nq;...]..p{.;.F.\.TK!.;5.......2.d..N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\863871680303623[1].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.* 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\2WF3MMUU\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20396, version 1.1
Category:	downloaded
Size (bytes):	20396
Entropy (8bit):	7.974131663185347
Encrypted:	false
SSDEEP:	384:SfXdUIIA0zhyKR28ePpAwxZ5M3py8wtshtdf45DEVTGdYb7H2Q/VEgm:Svdj0zhbRmjIQ8wtsV4lEVGdY3/i/
MD5:	68D6DABFE54E245E7D5D5C16C3C4B1A9
SHA1:	7FDAB895EAEBECEDB3FB5473EAB94A1B292CEF19
SHA-256:	A01A632E56731A854F35701AA8C3A6A19A113290D9032FF9048F8064C45383BD
SHA-512:	44EB151F85178A2F9600E85AD43FAE470FABE0F247C9A03E67931B36028E600C7550D9DE2D69B3576A06577A5DEAF54822EE4BDC9DCBB47588D1972C8A959D4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...Q...`u...cmap.....#cvt .....H...H+~..fpgm...$...3...._...gasp...X..... ...glyf...d..< ..l..C^]hdmx..H....m....03#7head..H....6...6...\hhea..I,... ...$.&..hmtx..IL.....".J.loca..K.....maxp..M.... ... .4..name..M.....~..9.post..N..... .m.dprep..N.....)* v60x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m...../.&. /6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D._OK.$.Z.(..JR...\..\..\..\.\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....Hy.F.Jez....._? 7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\LOGO-WEB-MIN[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 2921 x 1224, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	101607
Entropy (8bit):	7.7502956138982535
Encrypted:	false
SSDEEP:	3072:ZabyiM/2HSLy456mkvB/dQL9ILqUDSGtk2iJf5:ZIyb/2yLye6mkZ/dQL9iDO2iJB
MD5:	AAD2A1DB4345246F997940CDF22A7E7D
SHA1:	1A42EE6332E3D000D74A9CD9FE0D6E51DAB57719
SHA-256:	0FE93D2ADCFF1A195547AF7D4A0BB6299105CD06759A668A04D4BD39FBCAA9B1
SHA-512:	A1C5814910F40E49F048B5AD9D642319FE98E112FAD665DD87BD2F7312756269A423558E30DF01F5B2628C377A125DDD5409BC2881A92FC219DC677DDE4C31F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/images/LOGO-WEB-MIN.png
Preview:	.PNG.....IHDR...i.....<.l&....pHYs...#...#.x.?v.. .IDATx...o.U.'..izS...kz..l....*g..3.h.U...i..2..K#..+#..W...8+#5.p.._YUiX...`.7... 3.....IW..%A...TQ.....z.O%e_..?..=...G*..9...s.. =..H....$.....r...8...!.5m....._.+!..y.....l.....^i.;.....T..1p]._...._..~.s.`v.;...a..3a.....m&..P@Y...g.....].....n.....LH.....e..{..{.q.....0'!m...%.L:...*..7+.M9....:+ .}.>>:e}.....KH.`..0.@....06.v!6n...i.{..... ...@Y.....Aal..B..Oy.....(.!m...J;._.....-q=.n..L..>>:e.....IH....!{`V.{..3.....6P9Y...A.o.....Wf....W.....@..i....d..d.XqJ d*.m.4.m_.....'....P._.}V.....SN.....P6<..6.....@..i.]E(..m&..a}\|.q.....6PxY.....b.R.g.l_1Z.....'o..f.B.6.gZ.....,..6P....c.U.B..l....^.$.....#..tD...<.. #.0.B.Y.(...>.C.....`nB.@.dI...`6..f..m.>>:e.....DH.XQY....WB.....4..>-..... ....<..J..g.P).....@..i.-.%i.c....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\X46327MF	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.5219280948873621
Encrypted:	false
SSDEEP:	3:hn:h
MD5:	FDA44910DEB1A460BE4AC5D56D61D837
SHA1:	F6D0C643351580307B2EAA6A7560E76965496BC7
SHA-256:	933B971C6388D594A23FA1559825DB5BEC8ADE2DB1240AA8FC9D0C684949E8C9
SHA-512:	57DDA9AA7C29F960CD7948A4E4567844D3289FA729E9E388E7F4EDCBDF16BF6A94536598B4F9FF8942849F1F96BD3C00BC24A75E748A36FBF2A145F63BF904C
Malicious:	false
Reputation:	low
Preview:	0....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU_europapress2721462cremafallamunicipalvalencia17marzocoronavirus_9cab9921[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 1200x675, frames 3
Category:	downloaded
Size (bytes):	106208
Entropy (8bit):	7.9716424141893745
Encrypted:	false
SSDEEP:	1536:xwkVd6fbB5Lzak/lBwsEPCVvPx6i8NkWr7qKBatxjNE2/VYp1Wl+OEkR682F3HJ5:xxVd6PksIXLruOaPpJfDC3HM/U
MD5:	C140AB4AAAA5227C699D38A54AD50868
SHA1:	26FCDB8765E947F67C1B67CE37DE71F48FF4E479
SHA-256:	6DDCD16A58F84C7A21E0A742A9B832D2A4262C099772987251C8B7B3B229EDE0
SHA-512:	A35D1799F58B5E914849D7EA8E4C887B1DAFFF6C81304786C6780F033D50A3DA537734F55E61DB0C35C0DEF4D0D16953B9BAAC65A6A234091B870F1A08BC13F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d3cra5ec8gdi8w.cloudfront.net/uploads/imagenes/social/2021/05/10/_europapress2721462cremafallamunicipalvalencia17marzocoronavirus_9cab9921.jpg?320f952da5bd9895b027428e2460627c
Preview:	......JFIF.....,.....XICC_PROFILE.....HLino....mntrRGB XYZ .....1..acspMSFT....IEC sRGB.....-HP .....cprt...P...3desc.....lwtpt.. .....bkpt.....rXYZ.....gXYZ...,....bXYZ...@....dmnd...T...pdmdd.....vued...L....view.....$lumi.....meas.....$tech...0....rTRC...<....gTRC...<....bTRC...<....text....Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1.....XYZ .....Q.....XYZ .....XYZ .. ....o...8.....XYZ .....b.....XYZ .....$.....desc.....IEC http://www.iec.ch.....IEC http://www.iec.ch.....desc.....IEC 61966-2.1 Default RGB colour space - sRGB.....IEC 61966-2.1 Default RGB colour space - sRGB.....desc.....,Reference Viewing Condition in IEC61966-2.1.....,Reference V iewing Condition in IEC61966-2.1.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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):	168786
Entropy (8bit):	5.74230018532362
Encrypted:	false
SSDEEP:	1536:11O7iT0OBHXs+c9Lyw2c/4MHlOTewhqAvVK6+SjH96iQ0+a28AOQjD+q8R0L+AMS:rYiTJ1s7h0fV4SjHUS6yWZIK
MD5:	6D10531EA5184027DB9BD4862337190B
SHA1:	A84DD8DCBCB632690AA2B419CEF83D9CA7E3E56A
SHA-256:	F875CB5610D4347CD4F9ED9A4BBFA7A07920C88A7EC7A6AF3D1527EF57AFFBB1
SHA-512:	63097463D3881C18C2AC9947D72B9244B10E2FC04052D9806D62F2518FA6D7E94F95A58A12D910559239DDEF11676BAB1E584E57357A111477A9C0BA62C7D8B2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&adk=1812271804&adf=3025194257&lmt=1620634269&plat=1%3A16777224%2C2%3A8%2C9%3A32776%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1048576%2C32%3A32&format=0x0&url=https%3A%2F%2Flocalcoronavirus.com%2F&ea=0&flash=29.0.0&pra=5&wgl=1&dt=1620634269185&bpp=75&bdt=3125&idt=274&shv=r20210505&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&nras=1&correlator=7099701174794&frm=20&pv=2&ga_vid=2036550515.1620634268&ga_sid=1620634270&ga_hid=54307727&ga_fc=0&u_tz=120&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=784&bih=554&scr_x=0&scr_y=0&eid=44739521&oid=3&pvsid=623394271874461&pem=269&eae=2&fc=1920&docm=11&brdim=44%2C114%2C36%2C36%2C1280%2C%2C800%2C640%2C784%2C554&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=0&bc=1&ifi=1&uci=a!1&dtd=771
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(5px); /*potential issue: minimal browser support*/-webkit-backdrop-filter: blur(5px); /*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: 30px;background-color: #fff;}.btn {display:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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):	147678
Entropy (8bit):	5.7115442446006295
Encrypted:	false
SSDEEP:	1536:5BHXs+cJLyw2c/4MHlOTewEpw3Q7uAa28AOQj1+c8R0L+AMmvFWaEIK:51svh0CU49WZIK
MD5:	5541D014F2451EB0E08F0349B3A297AD
SHA1:	5C87096ADDF207F47ACCCD0FCF5A570A787517BA
SHA-256:	DEFFD3B5FC8D368B8BC2AEE8F9725CEBD6DD8B5E0331EB239225E9E66FB83018
SHA-512:	2C3D4D30032098F60292B20B147BAC1136E7C8A671AA474F6088EEFC6C46222F90E8BD696666CDAF63223D3F7A44296EBC33DB001F2D087B1D3C2C8C27F5DA7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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=1620634299&plat=1%3A16809992%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=1620634298406&bpp=33&bdt=3351&idt=471&shv=r20210505&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3Dce7f47caa8065e01-22bebfc90bc800fd%3AT%3D1620634270%3ART%3D1620634270%3AS%3DALNI_MaPVA5E2E6UYS_tehOMD4IsHIcqpw&nras=1&correlator=4886060073280&frm=20&pv=2&ga_vid=2036550515.1620634268&ga_sid=1620634300&ga_hid=993524416&ga_fc=0&u_tz=120&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=44739524&oid=3&pvsid=3029286976782573&pem=269&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=1466
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\2WF3MMUU\ads[3].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):	77958
Entropy (8bit):	6.0987742894109065
Encrypted:	false
SSDEEP:	768:aguhUZAoMpWyoDGvXzApvvAQOX+r3HzUK85vRxo8BVgeKuZMR1xrnk4uzOZ+xIV8:vuhOTyoDGvcpXK+rX6tVZqxzTx4L2C
MD5:	CCC3B507F2F359508B072C30EA800444
SHA1:	FDFB02C4F01BD89FC4D13B7FC49FF3187107730A
SHA-256:	E644E565046A01BC32363A98F5ED5748D9E46187E2D00C003F2F2019523E24CA
SHA-512:	BE60CA4A3F39924C75EDAE46403E847DEB7D9478CC7BAD76ACAA79F515D7E9F50C1BFBFC81F197600E2A70A29F6D31CCBD2CA601609875A3993332659B6516F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&h=280&adk=167372081&adf=3365229702&pi=t.aa~a.140049771~rp.1&w=1140&fwrn=4&fwrnh=100&lmt=1620634300&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=1620634298441&bpp=10&bdt=3384&idt=1447&shv=r20210505&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3Dce7f47caa8065e01-22bebfc90bc800fd%3AT%3D1620634270%3ART%3D1620634270%3AS%3DALNI_MaPVA5E2E6UYS_tehOMD4IsHIcqpw&prev_fmts=0x0&nras=2&correlator=4886060073280&frm=20&pv=1&ga_vid=2036550515.1620634268&ga_sid=1620634300&ga_hid=993524416&ga_fc=0&u_tz=120&u_his=1&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=70&ady=1113&biw=1280&bih=906&scr_x=0&scr_y=0&eid=44739524&oid=3&pvsid=3029286976782573&pem=269&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&btvi=1&xpc=tXbrlWmtSR&p=https%3A//localcoronavirus.com&dtd=1950
Preview:	<!DOCTYPE html><html lang=es><head><meta charset="UTF-8"><script>var jscVersion = 'r20210505';</script><script>var google_casm=[];</script><style>HTML,BODY{height:100%;width:100%;margin:0;padding:0;overflow:hidden;}#mys-wrapper{height:100%;width:100%;overflow:hidden;position:absolute;top:0;left:0;align-items:center;display:flex;justify-content:center;line-height:normal;}.mys-wrapper A,.mys-wrapper A:visited,.mys-wrapper A:hover,.mys-wrapper A:active{color:inherit;cursor:pointer;text-decoration:inherit;}[dir=rtl] .flip-on-rtl{transform:scale(-1,1);transform-origin:center;}#mys-content{flex-shrink:0;position:relative;overflow:hidden;z-index:0;}</style><style x-ns-frdjm-l="banner-large-vanilla" x-phase="assemble">.ns-frdjm-l-banner-large-vanilla{opacity:.01;position:absolute;top:0;left:0;display:block;width:1140px;height:280px;}.ns-frdjm-e-0{line-height:1.3;border-color:#e6e7e8;border-style:solid;border-width:1px;box-sizing:border-box;display:-ms-flexbox;display:flex;-ms-flex-direction:co

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ads[4].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):	147734
Entropy (8bit):	5.713459877398905
Encrypted:	false
SSDEEP:	1536:lBHXs+cJLyw2c/4MHlOTew9nNqwa28AOQjP+d8R0L+AMmvpWaEIK:l1svh0PH21hWZIK
MD5:	80209599F657FABEDA715C384D9C1C86
SHA1:	58CB391D7A0D270634779317B1DA175506CB24BC
SHA-256:	E45BF08E294DCD6527691FE1D11221CEDFD9BD868ABFD9DF1E2C8F4D2B9FB478
SHA-512:	8F27CB6B75AFA8201019F2524A6FED5AB562D5B5C8513A3F89E6F9663DF58F665124FADDB1B6AD1CACBEF24EFABEDB69C1C8DF2ED36E4A1BE808EFF10A70DD7D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&adk=1812271804&adf=3025194257&lmt=1620634338&plat=1%3A16809992%2C2%3A32776%2C9%3A32776%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1081344%2C32%3A32&format=0x0&url=https%3A%2F%2Flocalcoronavirus.com%2Fa-coruna-coronavirus&ea=0&flash=29.0.0&pra=5&wgl=1&dt=1620634334302&bpp=864&bdt=3680&idt=866&shv=r20210505&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3Dce7f47caa8065e01-22bebfc90bc800fd%3AT%3D1620634270%3ART%3D1620634270%3AS%3DALNI_MaPVA5E2E6UYS_tehOMD4IsHIcqpw&nras=1&correlator=3073635131724&frm=20&pv=2&ga_vid=2036550515.1620634268&ga_sid=1620634338&ga_hid=862558432&ga_fc=0&u_tz=120&u_his=9&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=42530672%2C44739521&oid=3&pvsid=3872528305419811&pem=269&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=3951

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ads[4].htm	
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\2WF3MMUU\ads[5].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	405
Entropy (8bit):	5.44484548812152
Encrypted:	false
SSDEEP:	12:hax/XKB0OoLu4UlJ2fRelztFiYSB0Fgdu43o9fFUhbhtFiYG:haoDCfJ2f2BF5Kpp3iWfF5G
MD5:	3A3889C7447574C5ED3631903B141A67
SHA1:	9C6E1EBF43F62963B10E763A28B84F5E8203CA7C
SHA-256:	903018A9E877B1FEAF4ACA9D543E0AE633D8D8D55DC21A0C3B9FCC8B87A14065
SHA-512:	44AF6C1BC78ACB6724481DFCD2DB816B798CB2E5BB2C24C5FCFF4C7A76F62EA7D4D9D2C0E0000242E01717CCEAD14617C4E26F7C61FA0890AED98C351B64C40
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&h=280&adk=2758184060&adf=3318715310&pi=t.aa~a.123580784~i.8~rp.4&w=379&fwrn=4&fwrnh=100&lmt=1620634371&num_ads=1&rafmt=1&armr=3&sem=mc&pwprc=4903144676&psa=1&ad_type=text_image&format=379x280&url=https%3A%2F%2Flocalcoronavirus.com%2Falava-coronavirus&flash=29.0.0&fwr=0&pra=3&rh=315&rw=378&rpe=1&resp_fmts=3&wgl=1&fa=27&adsid=ChAI8LPjhAYQs5bl0v6R5aZiEi8ALyzY0fePj5iV5335666DEG7LluCXoPom13u3QUjmmg1-r5kMbrNW2mJBcTbZkw&dt=1620634371641&bpp=15&bdt=14142&idt=-M&shv=r20210505&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3Dce7f47caa8065e01-22bebfc90bc800fd%3AT%3D1620634270%3ART%3D1620634270%3AS%3DALNI_MaPVA5E2E6UYS_tehOMD4IsHIcqpw&prev_fmts=0x0&nras=2&correlator=2126365037244&frm=20&pv=1&ga_vid=2036550515.1620634268&ga_sid=1620634364&ga_hid=1692515415&ga_fc=0&u_tz=120&u_his=10&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=100&ady=2875&biw=1280&bih=906&scr_x=0&scr_y=0&eid=42530672%2C44739524%2C44739991&oid=3&pvsid=2412960947998 14&pem=269&eae=0&fc=1408&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=128&bc=1&ifi=2&uci=a!2&btvi=1&xpc=MajVT0gKLD&p=https%3A//localcoronavirus.com&dtd=228
Preview:	<!DOCTYPE html><html><head><script>window.top.postMessage('{"msg_type":"resize-me","key_value":[{"key":"r_nh","value":"0"},{"key":"qid","value":"CIePzcDVvvACFcxPGAodFlQOSw"}],"googMsgType":"sth"}', '*');</script><script>window.top.postMessage('{"msg_type":"adsense-labs","key_value":[{"key":"settings","value":"[\\\"ca-pub-4607443575710795\\\",[[1]]]"}],"googMsgType":"sth"}', '*');</script></head></html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\alava-coronavirus[1].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):	90321
Entropy (8bit):	5.169094320113122
Encrypted:	false
SSDEEP:	1536:1L83LI+7DCyiBRxYYepopglEBbbvXy3Qqa0MH1w0ep:1Y3lBiDxYYeWvXy3QqaJ6p
MD5:	A13CFEBBA7BCC425DB0E5F47EDE2F3E1
SHA1:	7B6B0A1D85A3A289D37E3266E7BA439A05888EB4
SHA-256:	ECC7483DD779F45FD0C50A15B3191D049FF0BB76D4EC2556D6955BD3A6207CAC
SHA-512:	05AD6801EEA8CA47714E257991D3247F095BD0E8615E3DA9F930EB3A41D1D9320EFDA2E960EC2A453CEC9C8D44E49B16FFEBD46E1D0C99818435088CADCEF3B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/alava-coronavirus
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>. .lava Coronavirus . .ltima hora .</title><meta name="description" content=". Datos de la evoluci.n del Coronavirus . .lava Casos de Coronavirus .lava . Muertes por Coronavirus .lava."><meta name="keywords" content=".lava Coronavirus, informaci.n .lava Coronavirus, alertas .lava Coronavirus, estad.sticas .lava Coronavirus, .ltima hora de las noticias en .lava 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="/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bootstrap[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	147430
Entropy (8bit):	5.021633004516903
Encrypted:	false
SSDEEP:	1536:08tv6SUZjywXjH53LBHaWj8g1UClzi6nOdG/JP9IZpPcJ23tsOCeY:0oUZO4x1HugCsVnOU/JP9IZpPcJ238

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bootstrap[1].css	
MD5:	957474C344C7131FB8E093449CC4893A
SHA1:	6987E3BDAD7A3A5D143DDF2453E29782DBD99C29
SHA-256:	EF9C554BCA3CE5B9F978B626FF8C3A441C0468AF2599BDB4E9B6B32F6743F058
SHA-512:	FBE6C72B450DACD1D6DCB54D2F38139B61BBB8E1FA29DF9579DD2CB2438BD3E4D8EE9AF901C590811D7D91D8C0872CA24110E31705EE6C31AA4EF8E74B4F434
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/css/bootstrap.css
Preview:	/*!. * Bootstrap v3.3.5 (http://getbootstrap.com). * Copyright 2011-2015 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */./*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */.html {. font-family: sans-serif;. -webkit-text-size-adjust: 100%;. -ms-text-size-adjust: 100%;.}. body {. margin: 0;.}.article,.aside,.details,.figcaption,.figure,.footer,.header,.hgroup,.main,.menu,.nav,.section,.summary {. display: block;.}.audio,.canvas,.progress,.video {. display: inline-block;. vertical-align: baseline;.}.audio:not([controls]) {. display: none;. height: 0;.}.[hidden],.template {. display: none;.}.a {. background-color: transparent;.}.a:active,.a:hover {. outline: 0;.}.abbr[title] {. border-bottom: 1px dotted;.}.b,.strong {. font-weight: bold;.}.dfn {. font-style: italic;.}.h1 {. margin: .67em 0;. font-size: 2em;.}.mark {. color: #000;. background: #ff0;.}.small {. font-size: 80%;.}.sub,.sup {. posit

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\box-5e3cec51ed8e99df6977c199d27812d7[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1514
Entropy (8bit):	5.492829226473901
Encrypted:	false
SSDEEP:	24:h+vFgj+AvQq9FkTqpNoVN96970UF2RS0GViso3RTsn4JRJ6MshCgrX4Nu:a1Ad8OpNgNAuUF2RtLR1Q4JRJChCgroU
MD5:	5E3CEC51ED8E99DF6977C199D27812D7
SHA1:	5547262C1169562043B7DC06A80FD832768726A1
SHA-256:	486762D56893F9B12FDFAD41C3A76F11FC745B5436E97E596A63C22EE13D2E33
SHA-512:	4ED903305DAA06CB822DC99636AF78E97A64A6339EE069C829F28DD1B77768FDA6783D3D46D91A97FDB30B4C3DFFB3C0704D17100ED38D28BF0F9255CDED56F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://vars.hotjar.com/box-5e3cec51ed8e99df6977c199d27812d7.html
Preview:	<!DOCTYPE html>..<html lang="en">.<head>.<meta charset="utf-8"/>.<script>(function(){function f(a){try{var b=JSON.parse(a.data);b.key&&g[b.key]&&g[b.key].parseCommand(b,a.origin)}catch(d){return null}}var p;try{p={cookie:{get:function(a){return(a=RegExp("(?:^|;)"+a+"=([^;]*)").exec(document.cookie))?a[1]:void 0},set:function(a,b,d,h){a=[a+"="+b,"path=/","expires="+d.toUTCString()].concat(h||[]).join("; ");document.cookie=a},remove:function(a){document.cookie=a+"=; expires=Tue, 13 Mar 1979 00:00:00 UTC; path=/;"}}}catch(u){return}var g={_hjOptOut:new function(a,b,d,h,.f){this.parseCommand=function(c,g){function q(){var a=JSON.stringify({messageId:r,value:k||1});window.parent.postMessage(a,"*")}var l=p[a],m=c.action,n=c.key,r=c.messageId,e=c.siteId,e=h?n:n+":"+e,k=c.value,s=c.expiresMinutes||1440*(c.expiresDays||365),t=function(){var a=new Date;a.setTime(a.getTime()+6E4*s);return a}();if(!function(){var a={_hjSet:d,_hjGet:b,_hjRemove:d}[m]||[];return 0<=a.indexOf("*")||0<=a.indexOf(g)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bullet[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):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\chart.js@2.8[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	156721
Entropy (8bit):	5.3437462807874025
Encrypted:	false
SSDEEP:	3072:9IqGk57miKaxSUE879VE7CjWX1gLQmZ23M:9IqG67miKaxSUE879VEXO3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\chart.js@2.8[1].js	
MD5:	B235B564DE9C2C1D61D7EF07FCF2B93B
SHA1:	2EBF900E0386749373E9887026590FE7DAFC30AE
SHA-256:	52FF41341B9CBC23E2A4A436352F706292668BC0D33847D303F9C7D9AA0900BC
SHA-512:	99FEFC2AE914FDAF2B8EBEDA051BC26B657083FAB4B548C984BB5C2B9DCF1C46C5C0212A43976EAE5CEF55381080AA6FF9FC8D313E99413D40ABAB6936A7F 9A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.jsdelivr.net/npm/chart.js@2.8.0
Preview:	/*!. * Chart.js v2.8.0. * https://www.chartjs.org. * (c) 2019 Chart.js Contributors. * Released under the MIT License. */.!function(t,e){"object"==typeof exports&&"undefi ned"!=typeof module?module.exports=e(function(){try{return require("moment")}catch(t){}}()):"function"==typeof define&&define.amd?define(["require"],function(t){return e(function(){try{return t("moment")}catch(t){}}())}):t.Chart=e(t.moment)}(this,function(t){"use strict";t=t&&t.hasOwnProperty("default")?t.default:t;var e={rgb2hsl:i,rgb2hs v:n,rgb2hwb:a,rgb2cmyk:o,rgb2keyword:s,rgb2xyz:l,rgb2lab:d,rgb2lch:function(t){return x(d(t))},hsl2rgb:u,hsl2hsv:function(t){var e=t[0],i=t[1]/100,n=t[2]/100;if(0===n)ret urn[0,0,0];return[e,100*(2*(i*=(n*=2)<=1?n:2-n)/(n+i)),100*((n+i)/2)]},hsl2hwb:function(t){return a(u(t))},hsl2cmyk:function(t){return o(u(t))},hsl2keyword:function(t){return s(u(t))},hsv2rgb:h,hsv2hsl:function(t){var e,i,n=t[0],a=t[1]/100,o=t[2]/100;return e=a*o,[n,100*(e=(e/=(i=(2-a)*o)<=1?i:2-i)||0),100*(i/=2)]},hsv

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\coronavirus-madrid[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 75", baseline, precision 8, 1200x675, frames 3
Category:	downloaded
Size (bytes):	81017
Entropy (8bit):	7.960347032711173
Encrypted:	false
SSDEEP:	1536:iLNf1O7/6PVCA55t753irf4pdeLViBoQit8btwr6W:YUjo5MrAps9awrR
MD5:	526DB7D37FA768D379AB31B482A50F1E
SHA1:	6A10953D09448C05634F9DB9028747F672A09E04
SHA-256:	B56531CB9471905FE8FF0F198939BD35061065E3D6279FCFEA98ECC6EC43D7B9
SHA-512:	7D1B42FAD2F2E29A64E6F1F39C02768CE250BEDC2DCE633E1E1C5B0A76C263931193B2C5D3F019E72F9BCD5BE471DDB468D99D03B66825EA2EC69250B5EF4A C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://imagenes.20minutos.es/files/og_thumbnail/uploads/imagenes/2021/05/04/coronavirus-madrid.jpeg
Preview:	......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 75....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!22222222222 2222222222222222222222222222222222222222.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTU VWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEF GHIJSTUVWXYZcdefghijstuvwxyz.....?...J....h..m.H..o.....G.H..(..P3..#...p.SO...k....r.r+..a..I..f.....NEv.2.#.....WA.\.....|.V. ..K.....5!.. ZE...@.8.p.....sR.H.R.@.....P).h.....m.nE.4.]....-;m=W...i..R.O.N..h..x.e.qAZ..-r."....@:.[.....x.B.....S.WOd<.Y.,...I..u...9%*.....B/\G....#.. ..K...8e.D+.I...Ct1.y.. .v.C.u....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\coronavirus_mapa_localcoronavirus_slide_3[1].jpg	
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#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWg w.....5.....!1..AQaq"..2.....B#.R..3$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\2WF3MMUU\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=1460
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMo reInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..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\2WF3MMUU\downsize_200k_v1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 399x209, frames 3
Category:	downloaded
Size (bytes):	12759
Entropy (8bit):	7.9692455649976575
Encrypted:	false
SSDEEP:	384:csrI7m3jOfHWGjlGO1pH0+FBHXghiVrgvvU+:cs0K3j6H9x316w30iVrovU+
MD5:	152464F6308B02708850B61D2E434D42

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\downsize_200k_v1[1].jpg	
SHA1:	0EDA4A93064626A371A8DF6F621E1CD3EDFDB55A
SHA-256:	25C8F93A969257DB740A000ADE8D6C044A54E8415828B32EF7389545920F4365
SHA-512:	1F1F13EFDB56F9DB935CBD8B56C4DEFD02DA72B7A60A2E46A91423E7AB50934BB5E1C4D2418F9D48171F2F002F5AD0049677630CB6F2D252852CB9148A120E3C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/9089639398148746623/downsize_200k_v1?w=400&h=209
Preview:	......JFIF..... ."" ...$(4,$&1'..-=-157:::#+?D?8C49:7.....7%.%77777777777777777777777777777777777777777777777777777777777."..... .....O.....!1..AQ."aq.#2r.....3BR$4bc.....s.....5C.6DSt...%TU.....;.....!1.2A..Q.."3Baq...R.....#..4CSc.....?.....\|VV.K6 ..g..IT.(..0..7....-;.J.:,Ty6...%.Dwj!....qAzv.mY.>.c.=...5.D.1..4B...1h;...#.o..."xcwCr^.....f x.eX.....^9g..r1)....2R...6YQ.r0.....d.\|d....d.k.S\|p.....N.e.....u...X<_.R..doY.<so....f-.2...z...jav.u[...9...P=..or..t....m.en..+`.\|....7..r.d.g.!..\...x.U.F.u%.:x...`...M.....GA...<.e..h...mo.cOvJ.UD..}....i1...'.M\|....>..O.sO."..U.w..]..$.)\K&..+Ob..x.fe..b.S<.?...5.;F} H.. .....+?.....K.....c.>.N.*.6....8..}_.v.....u...._.Y.KF..NC.T].s.'.}.j..'.....U.Ey.....o.l@..*J...>.....95.?.L~.+...z o.....]..yrS.T{.lxF.;R_sVm.....#+nNMkY.....LB.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\downsize_200k_v1[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 399x209, frames 3
Category:	downloaded
Size (bytes):	9691
Entropy (8bit):	7.944111549470995
Encrypted:	false
SSDEEP:	192:1slMjH7xRNOfEOZlFfQk9wWl5iFL8xy6RLM+Xl9wB9ggrVTl:GlM5DAHZl2k9PiFLh6RLXjm/z
MD5:	47B6DBBE249C2D16B6602446807F0D6C
SHA1:	DE8234232EEF5FE001D47C7BBDC61206B2949A58
SHA-256:	62EBBBC949F64ADF3D9DC4961A05D30AE4AE7886C3A07D18C8417C6623A0C6B7
SHA-512:	21533E7AA5CD17C5DC4B1DBD0E38F6E5176A56AEB03D00C43D2D39E9A895ED136E9D826452D92658E4C37CE08BF54894D0FBC5EA5963BB84049435D1B5BC064
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/5618836558336947399/downsize_200k_v1?w=400&h=209
Preview:	......JFIF..... ."" ...$(4,$&1'..-=-157:::#+?D?8C49:7.....7%.%77777777777777777777777777777777777777777777777777777777777."..... .....C.....!1.AQ."2aq.B...#3R...4br...$CDS.....5Tcs....."..... .....!.1.A"2Q.....?..f.....W..C*.....(.V.&....f`d.....\..}8lcNK.0..CZ. ....:la...;.|.c.T"oD.....H....-M.H...i..lv]..F.[.,...[5.....)....-...._.Z....d...[...q.. .....2...w.>N..N...15XA..;0{I.. ...q.3=....e;NP..\..@.N..e..X.4.+n..*6....=.....*9\.v.)....M.s...Z.gJ.....".....Un.(ng.F9.e....Shl.66.z..pN.....X..nj....x~J..-...nZe....F...%.<.o...v..c+.o.~....J.Xbk...`.....J...#Uj..P2.}..K.i..ST.2.c.n.6h[ .!.D.GnC...."........8.*.....;z..:.-.H..l....X.:.:...QX.3.Uj) r.dO0..<e)..2.\.)..y.92G....SH..*.4Vu$.yB.9..E...&.....:...]....`...DZ.N...P}.h.~.F.l.|q..."....#i*>.Z.F.p..s..6.Y..)..J;5....0.p.....B.I.#V...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\downsize_200k_v1[3].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):	1872
Entropy (8bit):	7.617957613830919
Encrypted:	false
SSDEEP:	48:r3bm7nA2eS/72emLUrD2QZsssBH4Pmvtv7rsY3x:TqDA2eQx4QCsA0mZYY3x
MD5:	85ECCD08913DFE23A056BF69A7452F79
SHA1:	CDF2C5C6EF969D5E80BC61A4D153379B2B751851
SHA-256:	89B5E052F9813D9A2C8AF873672D730F2471AC92CFC71A70ACF42D20357CF4C7
SHA-512:	D075369CECB463852FEF421770746B42099D54DADF46DCE759BC49A398B1C5165C7F9D39FC4835C1979F9C126A16CEBA4E0E506FB3BAF2EBE5DD8B0545D8C39
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/14757595309220132507/downsize_200k_v1?w=100&h=100
Preview:	......JFIF..... ."" ...$(4,$&1'..-=-157:::#+?D?8C49:7.....7%.%77777777777777777777777777777777777777777777777777777777777.....d.d..... .....5.....!1A."2Qa..q..BRbc.....(.....1A.!Qa3"Bq...#.....?../.|.....cNXN..m.=}4.o'..`...'. 4.Y..E.'...{&.."}..M.5.....M%F{!#...3....sQ.f/.5.....b-h.q.].y....E-)!.jw.5...@#...[..<Gw.urb.g.;OY..... ....B`.HpI.h8.:.w.'.^.....[..%3..-V...W+..C.llgh.H.g...<.X.c$.XM.RqW.L*. .d.1....OzW...R.....X.x.N.M)&..?.\.e.V.GO.y{.z.p..8(qf.;Bl...y.R..5...r.W*{D...$a.BO!.:.....16.r.5&...<>.l.....-.t;.p^.G..0....KmE=.Y.{]9..m..h...!.....{w./.w.....?..T.m."..-..sy...^ A[.5....(.k)..#..8..q...y.,=V.lE.g..i..v....2Z.....rZ.A.w.....;['W.....9..f.8n.....8.1.^..R.....+3.rG..m...-.....d.....{..ym%).W(....c.d..z+...*._.....vu^...^..7.#.g.....<.^.b....2uf

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\downsize_200k_v1[4].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 399x209, frames 3
Category:	downloaded
Size (bytes):	12005
Entropy (8bit):	7.961418664008049
Encrypted:	false
SSDEEP:	192:Z5AgQs4hCLIijwx/YwnaDLI3+fe4K83CLhrqmmZ50L2Z7tcuoGE9O5HGqilU:vAnDCLIEiwwSL7fuqML2Z7eJ5c5+W
MD5:	DA27E583D25F82EA4313FE1E53563295

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\downsize_200k_v1[4].jpg	
SHA1:	958D50BE5B8508BDB29D31EC1DC57574D4F72700
SHA-256:	6D0E5B5EF2271F46330EF33ED94370A2BFA3FEC5692000A7119145A7750E52D0
SHA-512:	AD4F5A0CDD92B3795A06CCF7F6D491561CE3E3C212728FB1C43465E4CCC6126FB64F7B4BE574ABC9BE149CCB6412CDDF22EB24FCF329A2BE8C4B6C76377CE 0FE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/3871948583101367734/downsize_200k_v1?w=400&h=209
Preview:	......JFIF..... ."" ...$(4,$&1'..-=-157:::#+?D?8C49:7.....7%.%7777777777777777777777777777777777777777777777777777."..... .....H.....!.1."2AQaq.#3..R.....$4Br.5..Cbst...%cd...ES.....+.....1.!."2AQ.q..B.#3a.....?..327.).....7.1'...1...!6w$...w"(.[w.r ...2....~.}.k~5n.\.c.Q.."..S../.k..N3.Z.F.r.#.r...$v.!7.....t...a8c../?.;..R....;.iX4..f5+...ff.[[jX.....e.*`-.q*..+.5.A..{.&.K.5..m.....hQ. .cF.[..T.x.....0....e.&.)...*a$.aJTQ...B..ST..D..P6...x...-~...UI%..8h#.O..n...p...e....6..3.ug.MOe.m.uUt.,O....#Zq.G..0....2.OS..7>..aR+.3Q...oQx....T.c..,M .....A.T..a.H.e. .#o.R.+.0yu[.....?fJ.W.}..[.$.f.>IC.2.....??...v.;U..(..c..3. 5....V.WJ..-sA=.....\bJ..if.v...r....i.c8#..l....*.GQ..<...7.>).....m.7W..{.\H.ai.|...%%t5z.z..v.x....."....(wWMJ.i.....M.N.....`...E..Qi%F..{C.....6.2.+@.....B.^..B..Y.i%A_.%.l....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\downsize_200k_v1[5].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 399x209, frames 3
Category:	downloaded
Size (bytes):	12094
Entropy (8bit):	7.96155426688887
Encrypted:	false
SSDEEP:	192:HRafUCkS3AakSkBMsBj2yli81bmSOLZFQ+QXE9nt818XyXb1cl+P9hQ5ZvYqY9hv:xqU3mZkLBkrLZFQ+QX2tQGl4rQ5vohNp
MD5:	96253A9A86EC5EE6CA670B66485FEE0D
SHA1:	9929ABDD2BCA4C6644C9BA587F14D9C4C861967E
SHA-256:	F932623FB46BB6C3EAC0AD8BFB1B5285F4236BC433F665659C56667E2925F9C8
SHA-512:	9E04DF90542445F4F00A6FC2C089EEB6D6D0BC99A30BAF4B7FFEF34DA56425819139B952D94AF1B5137D928CF81ED4FD366A3DF336DF18884E40C2B7B9D202E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/1777629087445599O126/downsize_200k_v1?w=400&h=209
Preview:	......JFIF..... ."" ...$(4,$&1'..-=-157:::#+?D?8C49:7.....7%.%7777777777777777777777777777777777777777777777777777."..... .....[.....!1AQ.."aq.2.....#BRUbrt....36Cs....$457ES...DFcd....T%&'.....$.....1.!.A2Qa".B3.....?...!...B.B.... .!...B.B.... .!...B.B.... .$j*a.m.0u.L%. o..<.M.N.KR.....QD.u.i\...z..D.....b.....u....'...f..n?*....S.zO$.....H...Wb.N.K.....fq...T^i....<.R....cJ^.:...$..k.U..EK.ut.Q..Ig.I.<T..nZ.,d...M.})..V..R ....V.S..S.&N..G.q.R.D.r6.....v.e/B....L.....!.!..@.B.....&8.'O.aU8.Y.4.....z..K.....}5c...[WYP'M....mV.qK.....n.G.....nzD.....v.....!q..!...=....U.\Q....q...W.{p...k....p...k~.....8.\q\x t.H~:...n.C..w..{.v.....4...(....W}yF....p...~.|q}.....r[...w.Qq.q...~1].....+.....8.\q\{.....x....^..G.....=..|m].....N5.w.....+.(.8.>...k]...{f.~4...P.Z6<]]..'.26..t.f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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.querySelec torAll("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\2WF3MMUU\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\errorPageStrings[1]	
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	254886
Entropy (8bit):	5.4992095591998575
Encrypted:	false
SSDEEP:	3072:HzGZ61d4IFLOZmXsYh7JHBdvYPc9PhH0OriJ8GdJSEYJW3wcxl:yWqIFLOZmX37tBdAPc9PHGdJSEyW3wcf
MD5:	DDB45A4A9B53C16169892A27FFD29FA5
SHA1:	2B3BA49478BE4A19BC446A6008E3D835D1244490
SHA-256:	411609939445F7701625CFD1FA6397C3BD53B2A837C5231CEA15F63B13F1CD8A
SHA-512:	56A19A4D53207EF5AE8880A5243F980A2BF87DF56430E1799F4640A691939645BEF39CEB1A4EFB92E256E8784BD1E956B3CFC3C50F16614D2E73528479B35126
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/pagead/js/r20210505/r20190131/show_ads_impl.js
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\2WF3MMUU\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):	5.470946662451581
Encrypted:	false
SSDEEP:	3:tDptoBWs56TESPshLj+IXXD3F3LTXGYubLzkwJT5204V269W77r6PXIZEGDLwTjW:tDpuPP3n53nXGbEwa04V2X7uP0mjW
MD5:	193911A150B3F069EB753FF6C2DD1F52
SHA1:	041936CD455738C3073A5F7247514EAFE997CF8F
SHA-256:	DC08ACD6BCE477CB7D44A4778B46EB139F67C87616D6B6D4E3F7821B267263DC
SHA-512:	59EBB0C846254BFA6D8EB960FD74E1D99CB1028FAECE759B2D5724B73FF4D075985BC0BE2347DCB02700D48FB8260D958B508F24E76FF8526F12152282DEC38
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=ce7f47caa8065e01-22bebfc90bc800fd:T=1620634270:RT=1620634270:S=ALNI_MaPVA5E2E6UYS_tehOMD4IsHIcqpw","_expires_":1654330270,"_path_":"/","_domain_":"localcoronavirus.com"}]});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\f[3].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1610
Entropy (8bit):	5.304847945185042
Encrypted:	false
SSDEEP:	48:axvWazPjHa5lM1JIO+22OqRFbB6u/t9cS:idzPjHB92OIFbB6ut
MD5:	D6B0A60B328FB34516306944169F75CC
SHA1:	0DCD12C584B2117829F4CC2B074F3B0F0A6B68E0
SHA-256:	8BC3D695C45FC0A4D3BFC67FE64F3BE04B08307D5F8EC6EBA1A9B54581BE178B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\f[3].txt	
SHA-512:	E2FA46E1733A9226A5ACC16BC53383E70750A8743B6E49E10F7619DF994BEBAA6A5492A1DC4915A0241875B0D4D969B3BE3A3DDF2156A65A4193CCC1C8FC337 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/pagead/js/r20210505/r20110914/client/load_preloaded_resource.js
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,va lue: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","s tylesheet");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\2WF3MMUU\f[4].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	22386
Entropy (8bit):	5.409422639498625
Encrypted:	false
SSDEEP:	384:fVvNB4ViWplMmaSKBzUdqgJRqMviQY0OkfrlCXr+iRcPldQUMy4UWyW6h6:NMV6pzBzUdqgJUMviECXr4RRlh6
MD5:	38EA71B92AAFE4EA2D63FB55E0E916E4
SHA1:	F97705C3190A3E802BF658B9381002F5F14EAA36
SHA-256:	8F6579B2C579AA6A2E089F3D0F7BEDA646657CCBC948B87D1C3FF972BD05FA4E
SHA-512:	B87CE9F2955FC3619EB9949D5133063F2E42E65850FE437DBAFA5969C50736C16D24A1B217BE30FDDB290B911B1D9DCDB665BE136446B370A823FD30BFC1D1D 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/pagead/js/r20210505/r20110914/abg_lite.js
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .function aa(a){var b=0;return function(){return b<a.length?{done:!1,v alue: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 n=ca(this);function da(a,b){if(b)a:{var c=n;a =a.split(".");for(var e=0;e<a.length-1;e++){var g=a[e];if(!(g in c))break a;c=c[g]}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 ea(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:aa(a)}}var fa="function"==typeof Object.cre

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\f[5].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:tDKn:tDK
MD5:	124D3918819AB4C349A7F9FA979BEF07
SHA1:	6AD167D76A8768130783CD19AA6D8143C0B1BF37
SHA-256:	DAA795332E5DBCF893ADF2D5F3349F02B8C1CB957FF3B5F4C11B742E33C3376F
SHA-512:	4F7F15B28C6B38FC66002DBEE29688B801A689B716093BA63ADBE23FFFE144621198973A8AC4981FF2D20881BD4C84E45130A631E5B9A5EAE3A5FE26C106F7D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://partner.googleadservices.com/gampad/cookie.js?domain=localcoronavirus.com&callback=_gfp_s_&client=ca-pub- 4607443575710795&cookie=ID%3Dce7f47caa8065e01- 22bebfc90bc800fd%3AT%3D1620634270%3ART%3D1620634270%3AS%3DALNI_MaPVA5E2E6UYS_tehOMD4IsHIcqpw
Preview:	_gfp_s_({});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\f[6].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	15836
Entropy (8bit):	5.443481957824485
Encrypted:	false
SSDEEP:	384:KAkj7TW2wTyHtx41laMkYtviAFM+T3K24/amuaH:27TjwTT1lRXbT3K2oamus
MD5:	8BDC71E7FFC44A603ED7A63D908029AD
SHA1:	AC8860FC17606B38EC162787F2C93484684B33F6
SHA-256:	4D8470086B6A72C24D72AEBD855F89DA6D6A2E407164EC46014BE7E1465FAAF1
SHA-512:	A8945F406162C068E79777985AB08D6C1349FD368321DEF63D10DC4080D3FCCB8B3FD5A2DE8FEFA665C09F9F937A4238397C10E456DCBB8EE955D1C3CD0335

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\f[6].txt	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/pagead/js/r20210506/r20110914/client/qs_click_protection.js
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .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 ea(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 k(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:aa(a)}}function fa(a){if(!(a instanceof Ar

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\feedback_grey600_24dp[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 48 x 48, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	205
Entropy (8bit):	6.471232950817362
Encrypted:	false
SSDEEP:	6:6v/lhPmvbPM6ArwrgPowQka3cQhWb8i4NI1Q/2up:6v/7OvzZ6IRwIcQEb7461Q2c
MD5:	4087858E2C9DB9AA8F6A840AEDCFB533
SHA1:	D1FFE861DA6BD0E95FD1A365B0C3D3CEB6CD58A3
SHA-256:	4D45982F2DC34F36C9045EE46A75A1943666BB7FD64E103CAC8C7429E7012840
SHA-512:	541228667C513266FFAC017AA43CCACEA410E20BF27D30599276E9984FAC2C433AC58288C19F7A5BFEB1C9B4074B8C9C472080BF1C706303F97B2CE73DBD634
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/images/icons/material/system/2x/feedback_grey600_24dp.png
Preview:	.PNG.....IHDR...0...0.....1.....IDATx...1..1.DQ.f....@H.....%`..j.M&"....5....;...;.....\.....\..U.4..pe.<.P.....%... ...@....p.....@...X...5..{.$.x^....y=..z.....|.....+.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	low
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\hv-TlzNxIFoO84YddYQyKTdYVA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17436, version 1.1
Category:	downloaded
Size (bytes):	17436
Entropy (8bit):	7.965352471070945
Encrypted:	false
SSDEEP:	384:ChlDcp5BWeKjusp5cqGp6sbnmBrzqlUToVYH1/jY:wAxWeeuHqGpjbmB3qmoGY
MD5:	FAE921830A5CD9C547291C01A4CC69FC
SHA1:	67A6D64EC90969D7F2B5ED5EAF00B75DB66BC2F2
SHA-256:	5DD422BF3BA941E0CD33C3F16ACDB0442727B3419668930F9C97B814CD2E051E
SHA-512:	B647D1456FC3A8CD48D19CB80F302EF17D52E0156D6EC7A307ABBA313F918128E249F99398C2B932F393056815014A9B7DC9B955B377AB9C37BEAF911AEAABF9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/biryani/v6/hv-TlzNxIFoO84YddYQyKTdYVA.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\hv-TlzNxIFoO84YddYQyKTdYVA[1].woff	
Preview:	wOFF.....D.....z.....GDEF..... ..."...xGPOS..... ... DvLuGSUB...../.....eOS/2.....N...`y...cmap...@.....V.. .cvt .....F...d....fpgm.....g...a.._.gasp..... ...glyf.....2(..\.d..head..<....6...6...Thhea..<.....$....hmtx..=.....;Fnloca..>.....i/maxp..@.... ... .K.wname..@.....T.RKKpost..A.....}}d..prep..C....~.....la.x.....\}M.f.D0 .e.%..\O>.....DFLT.....x..3Cpa.....k...F.m.....e755555...t.3w.{n<..N.a.b.....<...kiVm9.....0...../39.s._.....\|.....+.>.;.....X.Qdas..(...WP..y...c\...9.E....\..7.r.?. .E.Y....R..\.kr]n...<&....!Miq..$...,...&'y...2o1<..vHA.n.z.....)..8.Ec..^k....g..b...5.....I'..7wF.<M.&.z.....:.2..N.R..".{.l.7.ru.x.c`fRd.f`e``.b.```...q.F...@.....H.$?-....WI.%.o...K(..... 9&%.o@J.....&....x.].3.\....Y.c;?{.m.m.nc.m...i.*6..A.....B..py...J".<..m..n{...j.>...~.....X._P<..l...%{.....*n..v..^...,.i...E.o..s...m.7.^.}.....lz.M..Q.uO...&4.....6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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
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\2WF3MMUU\kl_kts_160x600px[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 160x600, frames 3
Category:	dropped
Size (bytes):	32759
Entropy (8bit):	7.970930453569607
Encrypted:	false
SSDEEP:	768:ZKg5a9ag410H3N8ESOGU5ELcXQCOP1BVDI8wZiwpuKuLRYEPhJ:dTH10H3N8ESlU52e+13DI8twpjuOEPhJ
MD5:	5C0B13E6B12F8E367BFFC5D96DC29E50
SHA1:	3AB82B9C4B11E6C69A300DB0CA76842A94FECC64
SHA-256:	8C21D42EF538CBD6C6B87D2EC51DFDDBE50CECE4F78E12595AC5AB86749C76A2
SHA-512:	DB0F94B165FA8096F2AED4D6AB1A3438F8DF00B5452BA8B913AB888A2D310EA2DBEC8F24F24D12DE3AB403CD258FC8878F4FFBD46378A351E82E634F25A2EAF3
Malicious:	false
Reputation:	low
Preview:	......Exif..II*.....Ducky.....V.....Adobe.d.....X..... .....!...1A.Qa".q...2B#....W.....Rbg.r.3%...w9..S$d.G....CsT5e..&F.c...4Dtu78x.....!1A..Qaq....."....2BRbr.....#....e6...3.Ss4ECc$D.&. .%.....?.....C?/..JL..TH.0.l.lF..l.n6.8.c..p..vH. .5..bl.../.b...2.X.ehR.Z..i.!BiiX..u#iR..8V<....D~.X... C_ .=a< -..*..02...\WHq5..=>.]W.hiU....."U..5.n.i..8.].g..dO..D...P.fe.B.H.q ....e.oL>..u."...xV4..)L5.K...(...".B...XW&^..&..Ea.e..#...Y.D.TxV4...L...U.p...6.*.[.U.`f..\W..03Z.....i.{..r.\....+..%....V4a@dO..I.j.C2%[.B...$.....X.*.. ....Y.....u.b,D.~...".P."yV.. .....}..."........6.n.%x..l+M<..V.l+_w...(.....3.eV.:..5(..W..P.'U...dC .....\(....O*.I.<*...".[.B...,....>..Tv.P.k.l..cr.....{rp..]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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):	340
Entropy (8bit):	5.335916817166796
Encrypted:	false
SSDEEP:	6:6v/lhPfZMQC19s/6TdKXTECL6yR/iVQv/lhPfZMQC19s/6TdKXTECL6yR/iVB:6v/7CQ2s/6TdKXIMKev/7CQ2s/6TdKXS
MD5:	F4CD90073BD7951FDA6290556A302D50
SHA1:	3921ABDAD56DFE9859E3A96694F9D55FBF87B489
SHA-256:	2584CB7CBFC2A125E8690B0442153E184AA75F21536FA403D3E0E31935025F57
SHA-512:	27088B48CFD27BBD7501C451EDB8D60921A9FF9161244A412317CE9303DA8BFC1D0DB1C89BFE59894015899B7AC57DB2803F40081DBBA4025E52D7DCC350F02
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....bKGD.....pHYs.....tIME.....-Q.7n....tEXtComment.Created with The GIMP.d%n....IDAT..c.iy.....+.....IEND.B`...PNG.....IHDR..... .....bKGD.....pHYs.....tIME.....-Q.7n....tEXtComment.Created with The GIMP.d%n....IDAT..c.iy.....+.....IEND.B`..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\primera-noche-en-barcelona-sin-estado-de-alarma[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):	111212
Entropy (8bit):	7.963536403171785
Encrypted:	false
SSDEEP:	3072:mEa5EXyQ4Jmhg4hp/a7QblHlrxwZOwBh0e:7CQCm7J1lrWZ7b
MD5:	A887526359CE27627EEBBBCB1C9F57F2
SHA1:	5D479D92AE355E97E7F65E7B4525C3EE4BEB98B2
SHA-256:	9DF656A16FA1EACD9779DEAAAA09739A1B2145A4FD46BBF51666E6FE19BC722F
SHA-512:	4E77E78849F298662C8F275ED9411215A643F74A5F25D4B5B65006B49C73A60F87699BAAEF40FE190EDC61BA7EACDD9F4F005B30B9C3656E4FB4F735DC84699
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://imagenes.20minutos.es/files/og_thumbnail/uploads/imagenes/2021/05/10/primera-noche-en-barcelona-sin-estado-de-alarma.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...?...A4r2h#.fP...8SA>.S.....>.._. ..=..i..N.....0.y.S...0.....=cf|g.Ii.8.(.TT...........5 mX..z.S..Qq..c...8g.N!....B...j+..if.....j...R..C.......46.l.6.,J;...NE&........,S......:q.B...b..q.....`.......`.h......{@...Ym.....#..b.i..........{.....>j...d.\B............9.7.3...].1.Rr.c..2..d.u..[.![.... .l.G.Q.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\reporting[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.0314906788435274
Encrypted:	false
SSDEEP:	3:CUnaaatwltxlHh/:f/
MD5:	FB02F374B8F73825415DB1BCCD4BD76D
SHA1:	B103AA629CACDD90B39538A7561DA7F8E49AD73F
SHA-256:	CAA849B179BEFA2645A8E2C474D2E82A76777A3305315ECE911013E8EE9A916C
SHA-512:	3BE8176915593E79BC280D08984A16C29C495BC53BE9B439276094B8DCD3764A3C72A046106A06B958E08E67451FE02743175C621A1FAA261FE7A9691CC77141
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dsp.active-agent.com/reporting/?winningPrice=YJjrBAAG5PkDogfQAAeyOIeR9jrZqbURCXfFoA&bannerId=9461112&campaignId=3023964&auctionId=96/-104/-21/4/0/7/116/72/3/-94/7/57/-44/12/-69/-37&impressionId=1&ssp=2&xr=0.99&xc=978cff8f7561120dd300593612811b3045368aa8&contentUnitId=3849937&bid=6960571626517735820
Preview:	GIF89a.............!.......,...........D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\revolution.extension.layeranimation.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	50765
Entropy (8bit):	5.406783791470186
Encrypted:	false
SSDEEP:	768:TMWnklSBI13hxS4rU3i08gqM+hvAfN64hT5jLqROq:TMy6HlGxhsN
MD5:	7FE78C8164CA4153681F7B00D4D4D89C
SHA1:	0675260BF9246E32D45739C30597B63F2B21611E
SHA-256:	F76B9458B63B2DFF156DBC21C539453EDE466C39A642D4987C4D2B485535F506
SHA-512:	9F9C7282C309E54085EC4A6F91B9A9DBCC752ED9A1924EECFB180C292A2F4CBCA67B01BB4F91F36885C2D1002A6DE48E97AD5646B76AF89CD4A95EACF5502 4F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/extensions/revolution.extension.layeranimation.min.js
Preview:	/***. * REVOLUTION 5.0 EXTENSION - LAYER ANIMATION. * @version: 1.1.5 (23.10.2015). * @requires jquery.themepunch.revol ution.js. * @author ThemePunch.***/..(function($) {..var _R = jQuery.fn.revolution,.._ISM = _R.is_mobile();..// /////.// .EXTENDED FUNCTIONS AVAILABLE GLOBAL //.//.jQuery.extend(true,_R, {...// MAKE SURE THE ANIMATION ENDS WITH A C LEANING ON MOZ TRANSFORMS. .animcompleted : function(_nc,opt) {......var t = _nc.data('videotype'),....ap = _nc.data('autoplay'),....an = _nc.data('autoplayonly firsttime');.......if (t!=undefined && t!="none")... if (ap==true || ap=="true" || ap=="on" || ap=="1sttime" || an) {........_R.playVideo(_nc,opt);.......if (an || ap=="1sttime") {....._nc .data('autoplayonlyfirsttime',false);....._nc.data('autoplay',"off");....}... }.else ... if (ap=="no1sttime") ...._nc.data('autoplay','on'

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sd[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sd[1].gif	
Category:	dropped
Size (bytes):	43
Entropy (8bit):	2.9889835948335506
Encrypted:	false
SSDEEP:	3:CUkxl7/lHh/:slf/
MD5:	B4491705564909DA7F9EAF749DBBFBB1
SHA1:	279315D507855C6A4351E1E2C2F39DD9CD2FCCD8
SHA-256:	4E0705327480AD2323CB03D9C450FFCAE4A98BF3A5382FA0C7882145ED620E49
SHA-512:	B8D82D64EC656C63570B82215564929ADAD167E61643FD72283B94F3E448EF8AB0AD42202F3537A0DA89960BBDC69498608FC6EC89502C6C338B6226C8BF5E1
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\settings[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	34024
Entropy (8bit):	5.287067971028489
Encrypted:	false
SSDEEP:	384:ZCKDskPW3m1sQ1V/r1z16d1IkUqWfLpw1O1j1TYf1r3V96stY0LAnwrth9hiyG1N:+e/xkUqWfLpudrF95HLAnwrth9h2X
MD5:	61A176B572FDE2D04094C822DBEDBC26
SHA1:	A5C9FE6D4DC51DD750EBC0F32AA08B4BC90B3E85
SHA-256:	C35EA487FE1E5ED8B8FB95BF5DE185DB988C317249A7943488B2E79F882C37D9
SHA-512:	D9A295652DBCB849BDEF2B270A1F52AAF856AD43539B679AF286C547CC4174154E5FD68C61052B8648A41E2D4F2DEDC66953F265C1B64906A20E6860A3C75C8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/css/settings.css
Preview:	./*----------.-.Revolution Slider 5.0 Default Style Settings -..Screen Stylesheet..version: .5.0.0.date: .18/03/15.author:..t hemepunch.email: .info@themepunch.com.website: .http://www.themepunch.com.----------*/...@font-face {. font-family 'revicons';. src: url('../fonts/revicons/revicons.eot?5510888');. src: url('../fonts/revicons/revicons.eot?5510888#iefix') format('embedded-opentype'),. url('../fonts/revic ons/revicons.woff?5510888') format('woff'),. url('../fonts/revicons/revicons.ttf?5510888') format('truetype'),. url('../fonts/revicons/revicons.svg?5510888#revicons') f ormat('svg');. font-weight: normal;. font-style: normal;.}.. [class^="revicon-"]:before, [class*=" revicon-"]:before {. font-family: "revicons";. font-style: normal;. font-weight: normal;. speak: none;. display: inline-block;. text-decoration

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\skin[1].less	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	3478
Entropy (8bit):	4.807484822489245
Encrypted:	false
SSDEEP:	96:HBVq1mcUmCr9K//Y6F//YvBCIHMYa93K1eX:hLcryCIH7yX
MD5:	8FF5158198DF09D0133C423698F81979
SHA1:	F4B748FB851B57792D4A1A2D0BF7ACFA79F49DDA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\skin[1].less	
SHA-256:	8107D881EB59AF129AC071A7234D22D75084746401DF5FF7EC23B4FA97254353
SHA-512:	5FEDEBE4688AF08E15454D2374446EC12506B9737F1769F8431F7F5BD865CB28DC1B8CC93134CDD83BE5DD480E27996CC528B297C9613F16293AD38627F6CCE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/css/skin.less
Preview:	/*!.. * Theme v1.0.0 .. * Copyright 2015-2016 theemon.com.. */..@skinColor:#bd242b; //Change here your theme Color..@fontFamily:'Raleway', sans-serif; //Change here your theme Font family.....transition_effect{.. -webkit-transition: all 0.2s ease-in-out;.. -moz-transition: all 0.2s ease-in-out;.. -ms-transition: all 0.2s ease-in-out;.. -o-transition: all 0.2s ease-in-out;.. transition: all 0.2s ease-in-out;..}....//==..//====================TEXT COLOR==================...header-three .icon-call-out,.header-three .calling:hover,.header-three .navbar-default .navbar-nav > li.active > a, ...navbar-default .navbar-nav > li.active > a,.header-three .navbar-default .navbar-nav > li > a:hover, .header-three .calling:hover,.foot-contact-form .btn-submit,.footer-two .foot-nav li i,.trans-btn, button.trans-btn,a.blog-read-btn,.blog-paging-list li.active a,.blog-paging-list li:hover a,.commenter-info-1 span,a.comm-back-btn i,.blog-list-sidebar li

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	74929
Entropy (8bit):	4.964492574931129
Encrypted:	false
SSDEEP:	1536:Tt1Jqx3ZcOqTR60mDRPXh4B49MCZ2CzYfCiQ4cL3Tsl+qnzmo39o8:XaZcfNs8+Ma3Y3Q4es/L91
MD5:	F15866C5D144019F33AD437DF111B048
SHA1:	197C991C8D13117E4A512BC54A226D8693203545
SHA-256:	1DF2EE66141D91889686AB94633B90E5F76A342F6F1CB57D0BDAACD0E31071D3
SHA-512:	302CAAF9FE1DE3596BAC1275F98625DAF005FC285CECAB483E4D6A0824034ECF2629EA1EDE780E178167E33C64C5F4DB266D5D3D7B29E16FDE6A87F508F86FD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/css/style.css
Preview:	/*. Table Of Contents.. 1.) Homepage. 1.1) Homepage_1 style. 2.) 404 page. 3.) About_Us page. 4.) Contact_Us page. 5.) Faq page. 6.) News page. 7.) Services page. 8.) blog page. 9.) blog_post page. 10.)blog_sidebar page. ==*/../*. 1.1) Homepage_1 style. ----------*/../*Slider style start here*/..tp-mask-wrap .tp-caption.first-label {. font-size: 14px;. text-transform: uppercase;. color: #fff;. font-family: "Catamaran", sans-serif;. font-weight: 800;. padding: 18px 30px;. background: #bd242b;.}..tp-mask-wrap .tp-caption.business-label {. background: #3b9dff;. padding: 20px 55px 50px 30px !important;. max-width: 458px !important;. min-width: auto !important;. width: 458px;. position: relative;. top: 31px;. height: 100%;.}..tp-mask-wrap .tp-caption.business-label strong {. font-size: 24px;. color: #fff;. font-family: "Catamaran", sans-serif;. font-weight: 800;. text-transform: uppercase;.}..tp-m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sync[1].gif	
SHA-256:	A065920DF8CC4016D67C3A464BE90099C9D28FFE7C9E6EE3A18F257EFC58CBD7
SHA-512:	49B8DAF1F5BA868BC8C6B224C787A75025CA36513EF8633D1D8F34E48EE0B578F466FCC104A7BED553404DDC5F9FAFF3FEF5F894B31CD57F32245E550FAD65 A
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sync[2].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:	49B8DAF1F5BA868BC8C6B224C787A75025CA36513EF8633D1D8F34E48EE0B578F466FCC104A7BED553404DDC5F9FAFF3FEF5F894B31CD57F32245E550FAD65 A
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\vacuna-astrazeneca-pfizer-moderna[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):	53869
Entropy (8bit):	7.885404492233788
Encrypted:	false
SSDEEP:	1536:ia28O4Ar/GybChP52s7+yll9fkJAHsdP/iRcdYM6g:D2XuHBz6uICJ6sdHi+dYM6g
MD5:	2A3AC58BEDF52AF2891EBAEADD999A53
SHA1:	9E1407FE8F93669E435F0857A424B3ACF9887963
SHA-256:	F6DA23458E436B61287429BE4B38EEF588A0BE83EAA87C5A9BC7A5A9D512F97F
SHA-512:	5E7E17B871260BC5B59751C3F13D916F924381EBC963DD4651A27C3FF93EAEED9147F58E4ECB62CFC2E77498620F401C3C4942C0AB77FFC3AE3D2A0687BDEB 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://imagenes.20minutos.es/files/og_thumbnail/uploads/imagenes/2021/05/07/vacuna-astrazeneca-pfizer-moderna.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...$4.%.....&'()*56789:CDEF GHIJSTUVWXYZcdefghijstuvwxyz.....?...(....(.....m..0.NI.U,.2I.....M\|L.....+.i.....\..z.....Le~.-r...W.D.m0.2p...^.iv.6."..3. .Y.E...{..<7.Y.Xmc...(.a#Q..:....r..$.*sR..J.)@....6i....F..2M+.C.<...d.....9.[6.`..p..Z.A.VB.Ijb.../..N.....jwK...c..5L..z.M....h...9y....S.....'vt.x...0.o..[.+.....7.v.x..K}.[.`.....R.[/;..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\vacunas-completas[1].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\2WF3MMUU\videoplayback[1].mp4	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ISO Media, MP4 v2 [ISO 14496-14]
Category:	dropped
Size (bytes):	1129766
Entropy (8bit):	7.966750545382506
Encrypted:	false
SSDEEP:	24576:C1LYie57mOwo1RgQfXxvWS967d8l7L9i1p6k0w1haE/decBFXMW:qhs7mhoYyv6ml7L9i6kL18E/deSF8W
MD5:	D1D082AE30D81FDD9F46ED9C39ABF8B5
SHA1:	E0F1917CE60FF295F0875CB7FE1563E684E02677
SHA-256:	54746379518BCBEC5CF17DB78A51059908B769F27B06A7B076DD828285B9D1EF
SHA-512:	992E29BBAA0B7E908AD60F2FDFCED3C29AC5E1761036AD516AE9AEC9FCE5C51C50641982D015A069AC0D13C4083649549C02C6EAD4D3653FC0A91828DF779E A
Malicious:	false
Reputation:	low
Preview:	....ftypmp42....isommp42....moov...lmvhd.....7.....@.....trak...\tkhd.....7x.....@..... ...h...../mdia... mdhd.....2.....U...._hdlr.....vide.....ISO Media file produced by Google Inc. Created on: 04/02/2019.....minf...$dinf....dref.....url .....hstb l....stsd.....avc1.....h.H...H.....2avcC.B.....gB.....Z..... ...A.....h.<.....stts.....c.....Xstsc..... .....stco.....b..%...}i.....nw.....a._8..1....X.....{_...X...E..N.....p...!.....V....Q...A..c{...L..9-....stsz.....c..#].....%.....>...A...I.....>... c.....2.....>.....A.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\1436723653-kos--1024x512@abc[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 34x34, segment length 16, baseline, precision 8, 1024x512, frames 3
Category:	downloaded
Size (bytes):	102718
Entropy (8bit):	7.978169539557044
Encrypted:	false
SSDEEP:	1536:GTmKKr5DA0ZAraqolmDIhp6gj5OrTHidpbmbyoshbVHY1GpJ8DUjdMxODLrb:GBKrDE2ls0pB5GTm+NshpFyUqEf
MD5:	D75AD78E511E69EAE31F61F2953E4AEB
SHA1:	3DD10B93ACBE5EEA8FF0DC243FCC8978282136DE
SHA-256:	19FFA44071E7AB1D0359C374026801CC50852BBFC7592E0C75C6130754D46720
SHA-512:	2C9434941329047427712 7FFD266BFF5BA954A035571127812E7C92CECEE6B128469C4B415AE073FEF30F26EE6B4876DEB4F80BEC60EC031EB55EEA697ABB8E5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static2.abc.es/media/espana/2021/05/10/1436723653-kos--1024x512@abc.jpg
Preview:	.....JFIF.....".".....,Photoshop 3.0.8BIM.....".....".....C.....C....."..... .....C.....!.1.."AQ.2a#q.BR...3...$Cb..4Sr..%.D..c.....*.....!.1.A.".2Q.B#aq.....?...J*#.BG..b.JQ.K..Vy.....+.r..U....N.A.....|.|..`... (.0...@W..72p.erHD.r{sF.....j.hZ0v.*..~..j.(.8.g.2..W..f....K..Q...)G...I.@Y..]..{mB.WV....*..z.^.Z=^..k.j.&.ZN.P8.C..z.^..!.R..m....;^.W.....].^^./u. .1^.}..>.VC...\.O.+..L.....q^...D=. {.....m.....Zt@]...A....Wd...t.....a.*9.7H.....u#/..H...M.....j>`....qJ...eu\.E,.W...(.$&2~i.^h.3.{SR.h.....M..h...j.j. .&.....zp.5..2*.pq....t.....`/ b..4e.r(rH.-...).F..O....".h.0c.... {.O4r8.6\aF1T.C...3~k.....O&v...Q.....\.5k.....9...7...xF...O\,.....Y...yK....zP..~s^..W.g.k..j..Y.{.....Lr.\T...-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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):	126
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEqjdfXPQE/xlEqjdfXPQE/xlEy:1QEoqh3QEoqh3QEoy
MD5:	7EDD19F8419144CEA07BFBE8887B944E
SHA1:	49D47C4F9EAFC111ED241D743F09D73C3A12F5C4
SHA-256:	605627E07A397426E1FDB473A8B69F252EB192CC953C266199DE9E5E63629F68
SHA-512:	19034777E93BFAAF0A80256EDFAED658D544E8EF9139C24C7FBBDE8CEAA9FFA5319558D33897DC692233784C147CAE7A9A5D80335A9206407ED0F15077BCE95 A
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;GIF89a.....!.....,.....D.;GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\6098cbc1260000e269b4296a[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 1200x630, frames 3
Category:	downloaded
Size (bytes):	143294
Entropy (8bit):	7.959815478538268
Encrypted:	false
SSDEEP:	3072:aVXUtVG6DzK+7HEq6GCCA+CHgibidLB7zJ8m603vKcQjHxu+IP:GXUt9D7gx+smVfKHjY+Y
MD5:	0B001090F5F7C32F2B78326674904E11
SHA1:	1B932B14C11EA7268740237A893ED7EA00B996A0
SHA-256:	90F84293AE4C2251B14DA8291099241517B97F1B51854272376E2A745DE31730
SHA-512:	8E80477586FF3DD7070ADBA057091637D4C8906481F73924D5BB71F1DE6F0669BFAD326AD606D6AEE6A1D13B512477A6A15ED33676D3D63B34F61C1FC0A85D6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img.huffingtonpost.com/asset/6098cbc1260000e269b4296a.jpg?ops=1200_630
Preview:	.....C..................................%...#... , #&')*)..-0-(0%()(...C..........(...(((......v...."......................................H......................!..1AQ.."aq... 2...#BR...3...$b.r%CS...&45.s..Dc.............................3.....................!.1A."Qa.2q....#B...R....3............?...\|W.3J...R.t.<..#4.O.v..>.^RO ..@ LriI.........)...R.=i ..J.....(..W..4 +.E8.29.."........$.s.M.lt...S.v.NE.#. ....4.@.G|......;......8BU....3..S..8.E..S'..FS......s...$I.:.m..`0L.........*N>i\|...O..."e....h..c.q'`.'.......x...w.D..<.\_..J}.2.U.GAm..5!....m..Ii.....C.E..^ .@3...A%]i+....[!4...h.s....BO=.I.$.@.;.F.:..^...+.....DKL..M.3.:Q.!I!b..0G.M.Q.ds^...m0I.+....U@'S.);.P=.{.. .).d.1.|S...G.:...2.FjW.P...0.T{.*..L..Z........H...$......O.!.(RS'..d .Gj%..>...2O5O.,..q^.............x....s^..Y=c....x..q.x..f.b{.x.I9...A q^..zs....z.BLH..&f)L..+.$u......&A......^9.i.A#...3....W..A.....{..\D.i#.M....S.h.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\9dzwlnlkvn11[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	11021
Entropy (8bit):	5.529480664951553
Encrypted:	false
SSDEEP:	192:Gty+VUOCRCLa232TiEoxfaQ0XRvhF6kjTkhmokp6H3Wtt9D8DuCyEjKGMk+1gdfo:SCRCLa232TG0XgT8EjBM1nU2
MD5:	6AED7723ABD59520D68572E2F62834E1
SHA1:	75AF6ABACCC4EBC8AF9BB456F5ED14270378ED02
SHA-256:	E1FE40B65D8F529E43256D900A30FDF8ADD5D1B9AE80949D7E0772613D866D5B
SHA-512:	F3E85BC3DCD463F93D978DE8A818AA614C09EE71216985DB41184C278233B6996C1045E34C7AFAABCE12AFE63A7C94EE63EBF18E198BA98EBF9216DF6A99DE E1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ad.ad-srv.net/zone/9dzwlnlkvn11? subid=&extVar[]=DOUBLEBORDER:1&extVar[]=ANIM_AFTER_30S:0&extVar[]=ACA_SSP:2&redirectClick=https%3A%2F%2Fadclick.g.doubleclick.net%2Faclk%3Fsa%3DL%26ai%3DCj9AgBOuYYPnJG9CPiM0PuOSeqAOfop6QXPrS2p2AAcCNtwEQASAAYPWVzoHgBIIBF2NhLXB1Yi00NjA3NDQzNTc1NzEwNzk1yAEJqQIIRrFXEWi0PqgDAaoE6QFP0CZxa56hn2EzEAqsg8hkteW4hm43U1bSikpKG_yRX86d-S-54AzuFX4bWu0bNbO7mxahshK4wP_t3lQGvGQzxrVn4SUtjrmZSxuENcvft0LNmylfk9-XxGenZ9loRpEo5D83L0BIba9hmqGAW0L4OAE5dyx2pqwMzj18SZaWGHPYatMsHPME73WshUwWBFEDuGnmKJgViXa6muHJzLf9XumqcNkBBXCSBpZZomz5iD4YRXjbIL8deYhqpuSiW2MMoqK0t-Usa4LZvCWsUi5KCxRd_p2ELmD0mxsqCwkyo-dEDxceyOMv4YAG5J6u4Kn55dxIoAYhqAemvhuoB_DZG6gH8tkbqAfs1RuoB5bYG6gHipyxAtgHANIIBQiAYRAB-gsCCAGADAHQFQGAFwE%26num%3D1%26sig%3DAOD64_1uStp1hdC4jEPdJdFJybJcOBUPag%26client%3Dca-pub-4607443575710795%26adurl%3Dhttps%253A%252F%252Fdspcluster.adfarm1.adition.com%252Fredi%253Flid%253D6960571630809711797%2526gdpr%253D0%2526gdpr%255Fconsent%253D%2526gdpr%255Fpd%253D0%2526userid%253D6959548101452429453%2526sid%253D3849937%2526kid%253D3023964%2526bid%253D941112%2526c%253D30643%2526keyword%253D%2526bidid%253D6960571626517735820%2526clickurl%253D
Preview:	if (typeof(tpAdtagBase) == 'undefined') {......function tpAdtagBase() {........function fp(o){var x=0;var y=0;if(o&&o.offsetParent){x=o.offsetLeft;y=o.offsetTop;while((o=o.offsetParent)){x+=o.offsetLeft;y+=o.offsetTop;}}return[x,y];}....function gcw(){return fr(window.innerWidth?window.innerWidth:0,document.documentElement?document.documentElement.clientWidth:0,document.body?document.body.clientWidth:0);}....function gch(){return fr(window.innerHeight?window.innerHeight:0,document.documentElement?document.documentElement.clientHeight:0,document.body?document.body.clientHeight:0);}....function gsl(){return fr(window.pageXOffset?window.pageXOffset:0,document.documentElement?document.documentElement.scrollLeft:0,document.body?document.body.scrollLeft:0);}....function gst(){return fr(window.pageYOffset?window.pageYOffset:0,document.documentElement?document.documentElement.scrollTop:0,document.body?document.body.scrollTop:0);}....function fr(n_win,n_docel,n_body){var n_result=n_win?n_wi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/ErrorPageTemplate.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ErrorPageTemplate[1]

Preview:

.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}..   ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\KFOmCnqEu92Fr1Mu4mxM[1].woff

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

Preview:

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\L24A1025[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 1280x720, frames 3
Category:	downloaded
Size (bytes):	76047
Entropy (8bit):	7.941288721439686
Encrypted:	false
SSDEEP:	1536:jarxD9M4fMRnB2yR6pqJeGtpAHQ8lXr7pEqxMY+F8CKl3xlP7x25e:jaD3OBVReqJeGkHDTEsMY+Ful3BOe
MD5:	083BD77AF7323845C4B9290EA44AAF8A
SHA1:	CADE805EDFEC79D9D3B77DD3CD2B6F450D7323A4
SHA-256:	846AC7B55916DE12DD87F4794FFB44A0B7F59425D22531C1AFEE884AB875D44F
SHA-512:	91D9A03F732F3BB2D1C31BB1E9E34CACAE9775B246B3287C32BA91186C928CA6D5DE06B2D5607E73035A075D66882D303F1DB6728AC2768E184FFC809160298
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.lavozdegalicia.es/default/2021/05/03/00121620068642701225646/Foto/L24A1025.jpg

Preview:

......JFIF.....H.H.....@ICC_PROFILE......0ADBE....mntrRGB XYZ ....acspAPPL....none...........................-ADBE..cprt.......2desc...0...kwtpt.. ......bkpt........rTRC........gTRC........bTRC........rXYZ........gXYZ........bXYZ........text....Copyright 1999 Adobe Systems Incorporated...desc........Adobe RGB (1998).......... ....XYZ ....Q........XYZ ....curv.........3..curv.........3..curv.........3..XYZ ....O.....XYZ ......4....,....XYZ ......&1.../.......C........ ....%...#... , #&')*)..-0-(0%()(...C...........(...((.........."...}........!1A..Qa."q.2....#B...R. .$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\NewErrorPageTemplate[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):	3224
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	48:5m73jcJqQep89TEw7UxkZCm73jcJqQep89TEw7Uxkk:5nqrehEw7U6ZCnqrehEw7U6k
MD5:	3A35614D9A6156057F7D30C91C1ED4F2
SHA1:	7DDE5D14A15F465C9BFD0B0C0B3416175E69D1BC
SHA-256:	D544FAC44B7B2CD937726C401B5C9C726F900CEF22980A7B39F8756581901B73
SHA-512:	8A31C0C90EF443E3B7AC5B930466CD8CEF1D540D2D436A7DC4D12F38686368303882A9610A57B2A1CF9AB973DB684FDA0B1831B116EAEB4D86BE816FDD627C 8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\NewErrorPageTemplate[1]	
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\S28A1086[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 1280x719, frames 3
Category:	downloaded
Size (bytes):	98929
Entropy (8bit):	7.9617153413841955
Encrypted:	false
SSDEEP:	3072:jb1wCSXlg5niLRCRVmikmjljn9HQpJqMS:j52QORqVkK9HnMS
MD5:	8065EBB30D9EA499DF925502A9E72CE4
SHA1:	B25A428EB293EDBF90D382FA8CEFE1CA96E1621A
SHA-256:	AEC735530A656E844ADFC5FF86A1B2B6B941B2CBCFC8982AAC4F28F8C7BB3E27
SHA-512:	A6A761FE35A57541AD9DB0EC113EFEAAC203823CC402D3D09369F6FEF3C1F776C129FC2F04B453A97F9A65A15EF99BC99575B2EBE98D04C953E4B44ACEF85A8A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.lavozdegalicia.es/default/2021/04/30/00121619797502369793300/Foto/S28A1086.jpg
Preview:	......JFIF.....H.H.....@ICC_PROFILE......0ADBE....mntrRGB XYZ ....acspAPPL....none..........................-ADBE...cprt.......2desc...0...kwtpt.. ......bkpt........rTRC........gTRC........bTRC........rXYZ........gXYZ........bXYZ........text....Copyright 1999 Adobe Systems Incorporated...desc........Adobe RGB (1998).......... ....XYZ ....Q........XYZ ....curv.........3..curv.........3..curv.........3..XYZ ....O.....XYZ ......4....,....XYZ ......&1.../.......C........ ....%...#... , #&')*)..-0-(0%()(...C...........(...((..........."...}........!1A..Qa."q.2....#B...R. .$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\activeview[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	168
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEqjdfXPQE/xlEqjdfXPQE/xlEqjdfXPQE/xlEy:1QEoqh3QEoqh3QEoqh3QEoy
MD5:	467516F9253EA731178FBAB3B642EF8A
SHA1:	7C72BB053990BA49D08DEF4C7B64B6174D56543A
SHA-256:	5A9C78173EE4289896C0FB6A2DC37F0BAB123B7514BD7CB79D71BB563A9ED8B0
SHA-512:	AEDAA2A5EAC835C5B514FDE2E2E50A2D7BBD0D88450321BEAC9BE9E08DA89606054D72780F2A5CF907B1F57DAB73B5FC8A4A36137E0FF380B88A8454E2629DDE
Malicious:	false
Reputation:	low
Preview:	GIF89a.............!.......,...........D.;GIF89a.............!.......,...........D.;GIF89a.............!.......,...........D.;GIF89a.............!.......,...........D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\activeview[2].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\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ads[1].htm	
Category:	downloaded
Size (bytes):	77988
Entropy (8bit):	6.099606296481587
Encrypted:	false
SSDEEP:	768:auuhUZAoMpWyoDGfRyzqO3SwjuMWFrXxwBVge3WcR1x9lj+DgC8smNmiCD5A:ZuhOTyoDGYHrV3xxDaDgtkm
MD5:	B9D927A948CEB6ACDF1442D2ED889C3D
SHA1:	3F5D93E468B765A960D1F18D59A2F0AFD2C2698C
SHA-256:	850D27A850290CDA9C46878255A9045B15C222BA2594A705C44D1DE0B5812E08
SHA-512:	D6A1B9475896594CB050AA40608D20EE0DD9D7AD913A87D05EF3F46522D2478B7F854AED8BF1C9C3606E9EE4D96A3D95E25CB630148ED421D88463BD345CFA2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&h=280&adk=167372081&adf=836702963&pi=t.aa~a.140049771~rp.4&w=1140&fwrn=4&fwrnh=100&lmt=1620634303&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&adsid=ChAI8LPjhAYQs5bl0v6R5aZiEi8ALyzY0Z1MNjQeS4bGKZBHI6mradXljywuj8DPvxqX09XAOv0Tz5mgMN0s6YhhFg&dt=1620634303652&bpp=4&bdt=8599&idt=-M&shv=r20210505&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3Dce7f47caa8065e01-22bebfc90bc800fd%3AT%3D1620634270%3ART%3D1620634270%3AS%3DALNI_MaPVA5E2E6UYS_tehOMD4IsHIcqpw&prev_fmts=0x0%2C1140x280&nras=3&correlator=4886060073280&frm=20&pv=1&ga_vid=2036550515.1620634268&ga_sid=1620634300&ga_hid=993524416&ga_fc=0&u_tz=120&u_his=1&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=70&ady=1724&biw=1280&bih=906&scr_x=0&scr_y=0&eid=44739524&oid=3&pvsid=3029286976782573&pem=269&eae=0&fc=1920&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=128&bc=1&ifi=3&uci=a!3&btvi=2&xpc=uMdtMpFs1M&p=https%3A//localcoronavirus.com&dtd=22
Preview:	<!DOCTYPE html><html lang=es><head><meta charset="UTF-8"><script>var jscVersion = 'r20210505';</script><script>var google_casm=[];</script><style>HTML,BODY{height:100%;width:100%;margin:0;padding:0;overflow:hidden;}#mys-wrapper{height:100%;width:100%;overflow:hidden;position:absolute;top:0;left:0;align-items:center;display:flex;justify-content:center;line-height:normal;}.mys-wrapper A,.mys-wrapper A:visited,.mys-wrapper A:hover,.mys-wrapper A:active{color:inherit;cursor:pointer;text-decoration:inherit;}[dir=rtl] .flip-on-rtl{transform:scale(-1,1);transform-origin:center;}#mys-content{flex-shrink:0;position:relative;overflow:hidden;z-index:0;}</style><style x-ns-k8y10-l="banner-large-vanilla" x-phase="assemble">.ns-k8y10-l-banner-large-vanilla{opacity:.01;position:absolute;top:0;left:0;display:block;width:1140px;height:280px;}.ns-k8y10-e-0{line-height:1.3;border-color:#e6e7e8;border-style:solid;border-width:1px;box-sizing:border-box;display:-ms-flexbox;display:flex;-ms-flex-direction:co

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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):	81594
Entropy (8bit):	6.1072627695414425
Encrypted:	false
SSDEEP:	1536:r9ruhOTyoDG/Q+Gg7X7fmfEfVfgf0fOf+fX0OVJktf8xmfdf99k6kBf+fKJY:hruh0G/QU7XjQiZuS4okHx1h9WTFon
MD5:	200B2D4E5659C092BDC1863A733601B7
SHA1:	35434835B335E2953A32E612CC10F0B05B4413EA
SHA-256:	872F2808636D828BDF117A44628904BB77663D5DEA40F472E92428573B0B6876
SHA-512:	EFFD5B52C3743FD50C28C1825D1C5B2654DFF90043D1586A664211C8065FEFC3F951D2FD25B2FAD710AE1B8E328A30A2CFBA09D37F5F7185C014A9FF7B2B8DB7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&h=600&adk=2325579370&adf=543082386&pi=t.aa~a.2521328022~rp.1&w=263&fwrn=4&fwrnh=100&lmt=1620634340&rafmt=1&to=qs&pwprc=4903144676&psa=1&format=263x600&url=https%3A%2F%2Flocalcoronavirus.com%2Fa-coruna-coronavirus&flash=29.0.0&fwr=0&pra=3&rpe=1&resp_fmts=4&wgl=1&fa=40&adsid=ChAI8LPjhAYQs5bl0v6R5aZiEi8ALyzY0S_Bbr6ZS2UxhaNSRAYEioSRSJHYtPM-fI7tVDu7Y2VSJ8NkNFKFwh3M3A&dt=1620634340533&bpp=5&bdt=9910&idt=-M&shv=r20210505&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3Dce7f47caa8065e01-22bebfc90bc800fd%3AT%3D1620634270%3ART%3D1620634270%3AS%3DALNI_MaPVA5E2E6UYS_tehOMD4IsHIcqpw&prev_fmts=0x0%2C379x280%2C263x600%2C263x600&nras=5&correlator=3073635131724&frm=20&pv=1&ga_vid=2036550515.1620634268&ga_sid=1620634338&ga_hid=862558432&ga_fc=0&u_tz=120&u_his=9&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=948&ady=3134&biw=1280&bih=906&scr_x=0&scr_y=0&eid=42530672%2C44739521&oid=3&pvsid=3872528305419811&pem=269&eae=0&fc=1920&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=128&bc=1&ifi=5&uci=a!5&btvi=4&xpc=gQ1ulIwqMu&p=https%3A//localcoronavirus.com&dtd=434
Preview:	<!DOCTYPE html><html lang=de><head><meta charset="UTF-8"><script>var jscVersion = 'r20210505';</script><script>var google_casm=[];</script><style>HTML,BODY{height:100%;width:100%;margin:0;padding:0;overflow:hidden;}#mys-wrapper{height:100%;width:100%;overflow:hidden;position:absolute;top:0;left:0;align-items:center;display:flex;justify-content:center;line-height:normal;}.mys-wrapper A,.mys-wrapper A:visited,.mys-wrapper A:hover,.mys-wrapper A:active{color:inherit;cursor:pointer;text-decoration:inherit;}[dir=rtl] .flip-on-rtl{transform:scale(-1,1);transform-origin:center;}#mys-content{flex-shrink:0;position:relative;overflow:hidden;z-index:0;}</style><style x-ns-eb5ag-l="skyscraper-default" x-phase="assemble">.ns-eb5ag-l-skyscraper-default{opacity:.01;position:absolute;top:0;left:0;display:block;width:263px;height:600px;}.ns-eb5ag-e-0{box-sizing:border-box;display:-ms-flexbox;display:flex;-ms-flex-direction:column;flex-direction:column;font-family:Google Sans,Roboto,Arial,sans-serif;fon

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ads[3].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):	119959
Entropy (8bit):	6.059685886419079
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ads[3].htm	
SSDEEP:	1536:u7zhOmhoDGD6mEvZtv8i84S/7MKAmmjlf6a0tkdUuVmPk/xg1WicNQbs34ay47UM:u7zh+GD6Zb8i8GcZGicl4y
MD5:	334A641B74DA1626D9643AA57CBDD881
SHA1:	AA7BA11B07A0F1BDD159AABC3DEDEE57FA205730
SHA-256:	4C6AE5F056D714FA9C1438885F66619544CE78A8801DEB51E23B221A45B219C7
SHA-512:	2BFD88C21BED2E8814A4F2EF3217111C9A28094F3A5E60CFD0D2FD6541A2C2E5E1BE27FE58EA1A1FF94569D32C81C228D5C312AEEEFEA14ED50CE0DEE8457D96
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&h=240&adk=1103059081&adf=4286448932&pi=t.aa~a.2521328022~rp.4&w=263&fwrn=4&fwrnh=100&lmt=1620634341&rafmt=1&to=qs&pwprc=4903144676&psa=1&format=263x240&url=https%3A%2F%2Flocalcoronavirus.com%2Fa-coruna-coronavirus&flash=29.0.0&fwr=0&pra=3&rpe=1&resp_fmts=4&wgl=1&fa=40&adsid=ChAI8LPjhAYQs5bl0v6R5aZiEi8ALyzY0S_Bbr6ZS2UxhaNSRAYEioSRSJHYtPM-fl7tVDu7Y2VSJ8NkNFKFwh3M3A&dt=1620634340533&bpp=4&bdt=9911&idt=-M&shv=r20210505&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3Dce7f47caa8065e01-22bebfc90bc800fd%3AT%3D1620634270%3ART%3D1620634270%3AS%3DALNI_MaPVA5E2E6UYS_tehOMD4IsHIcqpw&prev_fmts=0x0%2C379x280%2C263x600%2C263x600%2C263x600&nras=6&correlator=3073635131724&frm=20&pv=1&ga_vid=2036550515.1620634268&ga_sid=1620634338&ga_hid=862558432&ga_fc=0&u_tz=120&u_his=9&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=948&ady=3764&biw=1280&bih=906&scr_x=0&scr_y=0&eid=42530672%2C44739521&oid=3&pvsid=3872528305419811&pem=269&eae=0&fc=1920&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=128&bc=1&ifi=6&uci=a!6&btvi=5&xpc=48z6RFK0hS&p=https%3A//localcoronavirus.com&dtd=530
Preview:	<!DOCTYPE html><html lang=de><head><meta charset="UTF-8"><link rel="preload" href="https://www.gstatic.com/mysidia/a204a622610ec42c29322584ae03f5a9.js?tag=client_fast_engine" as="script"><link rel="preload" href="https://www.gstatic.com/mysidia/18d789d750418e20e0a7b56da835eb89.js?tag=video_mra/web_raspberry" as="script"><script>var jscVersion = 'r20210506';</script><script>var google_casm=[];</script><script>function a(b){this.t={};this.tick=function(b,f,d){this.t[b]=[void 0!=d?d:(new Date).getTime(),f]};this.tick("start",null,b)}var c=new a;window.jstiming={Timer:a,load:c};try{var e=null;null==e&&window.gtbExternal&&(e=window.gtbExternal.pageT());null==e&&window.external&&(e=window.external.pageT);e&&(window.jstiming.pt=e)}catch(g){}var h=window.onerror;window.onerror=function(){window.jstiming.jsError=1;"function"==typeof h&&h.apply(window,arguments)};</script><script class="lima-exp-data" type="application/json">{"experimentIds": "44714510,44729911,44730425,44730426,75259405,7525940

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ads[4].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):	81088
Entropy (8bit):	6.105063347028689
Encrypted:	false
SSDEEP:	1536:SsguhOTyoDGw7oT2/tXQR3DZpGRVuxyf2XW:nguh0Gw7W2/tX7fZ
MD5:	42FE9C1B0BB5C98824A4EF8D3C9D85E9
SHA1:	7664AEB3838FE5BBEF2956B09B2DBA16F90CE09A
SHA-256:	8CBFD6CDD48E3534E03DCF1461BF089EBDF99F50C01912EEE66B6F1E1AC4B072
SHA-512:	1392745B3A97D5425C9D1E0DD9DB4A570859C2F7339B7B3AFE08BDC4966E4ECF25C633911C5240463D333ABEEAB575FE25489BDD28082FDA150EDCC6248837E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&h=600&adk=2325579370&adf=1526419059&pi=t.aa~a.2521325828~rp.4&w=263&fwrn=4&fwrnh=100&lmt=1620634340&rafmt=1&to=qs&pwprc=4903144676&psa=1&format=263x600&url=https%3A%2F%2Flocalcoronavirus.com%2Fa-coruna-coronavirus&flash=29.0.0&fwr=0&pra=3&rpe=1&resp_fmts=4&wgl=1&fa=40&adsid=ChAI8LPjhAYQs5bl0v6R5aZiEi8ALyzY0S_Bbr6ZS2UxhaNSRAYEioSRSJHYtPM-fl7tVDu7Y2VSJ8NkNFKFwh3M3A&dt=1620634340533&bpp=8&bdt=9910&idt=-M&shv=r20210505&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3Dce7f47caa8065e01-22bebfc90bc800fd%3AT%3D1620634270%3ART%3D1620634270%3AS%3DALNI_MaPVA5E2E6UYS_tehOMD4IsHIcqpw&prev_fmts=0x0%2C379x280%2C263x600&nras=4&correlator=3073635131724&frm=20&pv=1&ga_vid=2036550515.1620634268&ga_sid=1620634338&ga_hid=862558432&ga_fc=0&u_tz=120&u_his=9&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=948&ady=2249&biw=1280&bih=906&scr_x=0&scr_y=0&eid=42530672%2C44739521&oid=3&pvsid=3872528305419811&pem=269&eae=0&fc=1920&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=128&bc=1&ifi=4&uci=a!4&btvi=3&xpc=VaVJtWhuYB&p=https%3A//localcoronavirus.com&dtd=326
Preview:	<!DOCTYPE html><html lang=de><head><meta charset="UTF-8"><script>var jscVersion = 'r20210505';</script><script>var google_casm=[];</script><style>HTML,BODY{height:100%;width:100%;margin:0;padding:0;overflow:hidden;}#mys-wrapper{height:100%;width:100%;overflow:hidden;position:absolute;top:0;left:0;align-items:center;display:flex;justify-content:center;line-height:normal;}.mys-wrapper A,.mys-wrapper A:visited,.mys-wrapper A:hover,.mys-wrapper A:active{color:inherit;cursor:pointer;text-decoration:inherit;}[dir=rtl] .flip-on-rtl{transform:scale(-1,1);transform-origin:center;}#mys-content{flex-shrink:0;position:relative;overflow:hidden;z-index:0;}</style><style x-ns-1bof9-l="skyscraper-default" x-phase="assemble">.ns-1bof9-l-skyscraper-default{opacity:.01;position:absolute;top:0;left:0;display:block;width:263px;height:600px;}.ns-1bof9-e-0{box-sizing:border-box;display:-ms-flexbox;display:flex;-ms-flex-direction:column;flex-direction:column;font-family:Google Sans,Roboto,Arial,sans-serif;fon

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ads[5].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	405
Entropy (8bit):	5.414951658162851
Encrypted:	false
SSDEEP:	12:hax/XKB0OoLu4UlJ2fRk3xtFiYSB0Fgdu43o9fFUhbhtFiYG:haoDCfJ2fCTF5Kpp3iWfF5G
MD5:	2820F561B105B51941AE380CC5823292
SHA1:	BF22111106188E52C8F1D7F25DC3E52E1AFADAEA
SHA-256:	2925CEDA9FA7DED8C1E87F1EB8F32F1C1D3A58C70040ACDB9D0263106B398513

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ads[5].htm	
SHA-512:	89E8D45A3314804645856E920EBE67B6AD173C499C493FE75C9D87BC5EEB97477C00AE9896D7D3F8830C961DF3A3E7E7B8161F0DD8C47E955AE34215420C784
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&h=240&adk=1103059081&adf=1526419059&pi=t.aa~a.2521325828~rp.4&w=263&fwrn=4&fwrnh=100&lmt=1620634372&rafmt=1&to=qs&pwprc=4903144676&psa=1&format=263x240&url=https%3A%2F%2Flocalcoronavirus.com%2Falava-coronavirus&flash=29.0.0&fwr=0&pra=3&rpe=1&resp_fmts=4&wgl=1&fa=40&adsid=ChAI8LPjhAYQs5bl0v6R5aZiEi8ALyzY0fePj5iV5335666DEG7LluCXoPom13u3QUjmmg1-r5kMbrNW2mJBcTbZkw&dt=1620634371641&bpp=9&bdt=14142&idt=10&shv=r20210505&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3Dce7f47caa8065e01-22bebfc90bc800fd%3AT%3D1620634270%3ART%3D1620634270%3AS%3DALNI_MaPVA5E2E6UYS_tehOMD4IsHIcqpw&prev_fmts=0x0%2C379x280%2C263x600&nras=4&correlator=2126365037244&frm=20&pv=1&ga_vid=2036550515.1620634268&ga_sid=1620634364&ga_hid=1692515415&ga_fc=0&u_tz=120&u_his=10&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=948&ady=2298&biw=1280&bih=906&scr_x=0&scr_y=0&eid=42530672%2C44739524%2C44739991&oid=3&pvsid=2412960947998l4&pem=269&eae=0&fc=1920&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=128&bc=1&ifi=4&uci=a!4&btvi=3&xpc=Xt0aPynW4S&p=https%3A//localcoronavirus.com&dtd=411
Preview:	<!DOCTYPE html><html><head><script>window.top.postMessage('{"msg_type":"resize-me","key_value":[{"key":"r_nh","value":"0"},{"key":"qid","value":"CMmH2MDVvvACFY4HogMd3yIMCg"}],"googMsgType":"sth"}', '*');</script><script>window.top.postMessage('{"msg_type":"adsense-labs","key_value":[{"key":"settings","value":"[\\\"ca-pub-4607443575710795\\\",[[1]]]"}],"googMsgType":"sth"}', '*');</script></head></html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\alexander-zverev-conclusiones-mutua-madrid-open-2021[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 449 x 282, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	261128
Entropy (8bit):	**7.994162397936518**
Encrypted:	**true**
SSDEEP:	6144:/tTLgXaMeCHcJ7vZF9hzx6EKj/WvyCdvjZ534Hi76Q3a/P:dbMeTjF6zMdvjZ5oHin3aH
MD5:	BC01687AD512BFD2CAD8CD5FD697E365
SHA1:	E306766109B568F5E7C56FA111B7D7D48F2497D5
SHA-256:	A078FEAA44EFC8D2C33918B46E50BEBC9ABCDB930AA140A368560F884D5856D2
SHA-512:	C1CC517A27F0C0AF78E660854ECA98C42FA4F5E5A512C47D330C7CA61CBFE249C6C8BFC4E510C2A73005C4F84C4CF24A2EEF766ECF3126659AA6F67EA95EC5E
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.puntodebreak.com/files/alexander-zverev-conclusiones-mutua-madrid-open-2021.png
Preview:	.PNG.....IHDR..... {S....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^....$.u.b.8.z.{...{o.....w.....A..).$E..D.....'.....?x....9...I.<...79.QYY.UY..vDd..~.)~.....C...R.....5...L.....Wn.....MHI..+**..nhn...56:1?. XX...".If...n..-..EF...4...c.....em...-i%UqY...i.....5..W.o]y....Y.....|jx.xs.O....[. >V....'....B...../3.\.r...7o...GGG.....UT446wv.....\XZ...j..4[u....1z6....i....<Z.Ke.K....$P...5.....zI.\.(.e.rE.Zf.s..D. .-.....E.ll*_.+!..e....j.e..m.$.-c....,...b,.l..:/..%..... ...sb.D.(..Je.fV(..D...d.K.hnM8.....~.....C...r.....6...{#P.i...c.A\.04..0../p.....%.dd....U..5.....\.Z.,.....J..!1..:+1T..[...v.m..S.1XP.YV..[.....u.....!p..#f..m9..../.W...y..iq.....Sk.....^.iqy._j|...`h91....xlbzayQ ^W..:..b{..m.{...C5v..l...B.q].e.%.*..2.0..L.*S/KU.y.#&..%X.J.R.rQ*....!p.....*g(.?..aQ...K..H:/....^.J.....n.D....:...]......?.....y..Y.j\z?._Up6}jpd|

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\aprende[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 600 x 600
Category:	downloaded
Size (bytes):	28596
Entropy (8bit):	7.965977078847451
Encrypted:	false
SSDEEP:	768:BtoUhf0p9YfaxP4qOzWy9agGocX4gNRIcF:foM0XpP8zjtGocX4aBF
MD5:	8800D16069E012C1542002AC1A5B3DF6
SHA1:	AC7946B532FBD98B52A8592B13DAB1AFBF7182FB
SHA-256:	1742A94A78BF4E65FBFAEBDA6714C3181031399B5E6890832B84FF91442E9BD5
SHA-512:	F387757E31D7D6A837135A90BD83CB13EAA9613382E6931F2D3A8CFE4066632A711807F09C9B00FE78D5AE19382B358491D300E75D51971408E38E8505982E73
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/images/aprende.gif
Preview:	GIF89aX.X..".ff..0.f.f..0.....f.t0...c...t00.f.....f.....0..0.ff.....ff.....000...00h...W..".....WC..t0hff...^.....!..NETSCAPE2.0.....!..XMP DataXMP<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2017 (Windows)" xmpMM:InstanceID="xmp.iid:9ED3DC88139711EBBA63BE46C6EA322D" xmpMM:DocumentID="xmp.did:9ED3DC89139711EBBA63BE46C6EA322D"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:9ED3DC86139711EBBA63BE46C6EA322D" stRef:documentID="xmp.did:9ED3DC87139711EBBA63BE46C6EA322D" /> </rdf:Description> </rdf:RDF> </x:xmpmet

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\casa-pedro-rabo-toro-madrid-kh8--1024x512@abc[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, baseline, precision 8, 1024x512, frames 3
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\casa-pedro-rabo-toro-madrid-kh8--1024x512@abc[1].jpg	
Size (bytes):	106982
Entropy (8bit):	7.962758453095419
Encrypted:	false
SSDEEP:	3072:W1jW+H+iFMxtSPzETymYdXLnwOdmOIoE3p4DeRNaIyCvidEo:4W+eiFMT3mHXLnwgmpyD/I1iqo
MD5:	87A60438469D8C57F22272E6978B8AC7
SHA1:	3B6DAC848988CB0C5D164027D3ABEFEC35A42D2B
SHA-256:	B73B6A1DC7E4D09B28868456E69D03D62B12BC52E3E2EB28D044F23A37702058
SHA-512:	7776596FAB375D904676874171B0E1414DEB046C022A999F816198A6023DEE32D9E7C110514F91E9A75B9A8EB5CFAF273D0327BF98BE7CD69C44FAA5C784180B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static4.abc.es/media/gastronomia/2021/05/10/casa-pedro-rabo-toro-madrid-kh8--1024x512@abc.jpg
Preview:	......JFIF.....d.d...,,Photoshop 3.0.8BIM.....d.....d.....C.....C.....".....B.....!.1A."Q.2a#q..BR.3...$Cb..%...4Sr..&.....*.....!..1."A.Q2a..#.3Bq.....?...e.-..$.W.....W.$0....TF6f.Q"}....U...Z.....OzW....]...2.....X....'.!.;$.....:....Km.....k&.d6B..+.....y.....r)B.....l..u. a. sFC..1A.:..g....V..|.0RW....Q.[Z.R.;...Ym}9....|.....j...Bt..T.P...+&#dgp..CehB..>h....\. a.V.....&..IXZ....Q..U.KDPq{d...j.....82.. ..|.i.<>#{e....r....5d6....j)....>..j../..T.yJ...}..iu.....IQmA' ...y....4.:.....M.V..Ulr..[{.7."...l.....8rwy...i/ ...l...5..-..Z.<..'n...rVr.....R....R....*'.....,_H..n3.D.....nZ.T.;....BP.....X.Z....lw.LaZ$>..pi..d0.jV.U..U.7m.....VyF.....H.j.b.d.;]<U....[.Pe....C.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\coronavirus_mapa_localcoronavirus_slide_1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop CC 2018 (Windows), datetime=2020:03:11 15:06:00], baseline, precision 8, 1920x300, frames 3
Category:	downloaded
Size (bytes):	206887
Entropy (8bit):	7.89260750102466
Encrypted:	false
SSDEEP:	3072:VdN9qam4QnzkdaxCkPVOGsHEE8jq59GZgvLfE8u1zXp9xQf7agf3Muf99qVhV:VNqaCpxCC4E/q5mi48uxNQz/hf992
MD5:	2AC5010CB1563099923B56C3476EA347
SHA1:	C56091141290A054F57C52FAE3C18C56F967F0A6
SHA-256:	D21E2127BFF9C55CFE6ED2EE9C702C506938210341D3719C6601961745F1C2B0
SHA-512:	D1BB0351916F52A47F08B5B18FC9489DEAAC3A33C6D8DBA7726DE016841BCDB38D15970DB1692995B6AC39E522113C1ACDD23F4657CFA950C1A9414754011F5D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/images/coronavirus_mapa_localcoronavirus_slide_1.jpg
Preview:	......Exif..MM.*.....b.....j.(.....1....."...r.2.....i.....-....'..-....'.Adobe Photoshop CC 2018 (Windows).2020:03:11 15:06:00.....,.....".....*.(.....2.....H.....H.....Adobe_CM.....Adobe.d.....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?..{.....u7z^.-i.:..>....kE..;...iR5V@.D...'"....1..I.g..e..9.....=...(0.8....f>^.....$...f..qq...y.,.$.F@..H....K.: .x..v.W..NST...?..~.F:.k....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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
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\9026IKNJ\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\dnserror[1]	
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.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\9026IKNJ\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, 2943x1541, frames 3
Category:	downloaded
Size (bytes):	202896
Entropy (8bit):	7.932591738870841
Encrypted:	false
SSDEEP:	3072:LAQlh/VybNlV+X06yaSlVz1QaKyShji5JY9QibjKJpX8uaHoQIIthIsh2up:cOcPVKGHrz17KJjH9BbmJ1pPQIIthhNp
MD5:	DAF9C2432C644BFC39720941B3C0598C
SHA1:	429FB3E2E139DE11871CF008B95AB944ED967EE0
SHA-256:	2D2C67E9238ADE66442271FCF14EACAEE4617FC95CE5A1D40D78D9A88EE705CF
SHA-512:	32FAD6B20BC9E346C187A1FD78C0F77D16F6B59A4937C64EBCD7617927E8A53F7441977FDF0B1EA626476FDBBF4E9AF74133E42DF05977E4E8A2A062E8E279B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/5618836558336947399/downsize_200k_v1
Preview:	......JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222....."..... .....B.....!1.A.."Qa2q.B...#R....3b....CS.$r...4%c.s.....'.....!.1.A."Q2aqB.3#.....?..tZfq-....$0).....Fr5fR.....f2 .FO.i.2..).....H..!.....F..H..h.H..F.F.GD....I....F,.YP.....V.PPTP.....(.#h.%.b...c..8.<6...&.H....U..a.a.....8.P...t.!U..F".M....E$U..CI..H...&.F.Ee.zMt..2.i6...J#.k.(..I.....K.....&...t'.J.@d....CE.I.I..Fr.G$.s.'l.a8....wN...W#.$n.N...k..`o.....@P....8@.E..m..8..1.Q.P.".E$.(.H...*.*.@E..B.%.Z-...Fm.2YF2F2F.2.....,..4sdC.....e..nX...7....X9e.....h...Ib2.?..H.K`9%.=..2Di&...c..k..8D.....*.GD..F.EV.F.FqF.".(.""..............b...0.....C....0.....1.....h.....0..F.....6..Mc.E.$E...e.....0.7J....:.....$u=Sw._..~..1.s..._..}..).....7z`...vx.W..l$J..._.dm.u...oda<...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ecd-logo-mini-2[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 133 x 44, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1054
Entropy (8bit):	7.595293083535915
Encrypted:	false
SSDEEP:	24:ciGmW8mMp4g/j1egOAaQscWHTd++CNpB3VizTZWUjWQocNWo:mNo4gbAJADHoTdBCjBiofXo
MD5:	495BA4EE6F48CE5DA74B8680E3CBFE79

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ecd-logo-mini-2[1].png	
SHA1:	5D1CC79496BAD4F0B69F2430538B5D9D783FE080
SHA-256:	F172A834DC46C93B5C1B028EB757EEFDC790652B3C178D9CE71ACEAA65CDBFD7
SHA-512:	990A432CC7A0242F517791B8C9B0FB73A1B600B09624EC2D56694AF2FE22B50EC827FD6877E56FA4F17B980D65EBEAD4E91CCE5248ABE9A377DFBBA78D009A2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.elconfidencialdigital.com/media/elconfidencialdigital/sections/ecd-logo-mini-2.png
Preview:	.PNG.....IHDR.....,.....|..(...cPLTE.....&;i...&;i...&;i...&;i...&;i...&;i...&;i...&;i...&;i...&;i...&;i...&;i...&;i...&;i...&;i...u....tRNS... 00@@PP``pp.....,T...KIDATx.... ..Q.0-*U..i.....<T..t..vo.+.)..D.!..T.J..0hU...m..$a...d...P..\|...y>...=6.m...`.g(h....v.h...k.6E,m-.....e..s...Z.q..B)R..L...HE,.:F.g,!.....G.!E.V.cC!.....ht...*..s=.l...3-..R.[.....\f..k... ....R.!.....0.-..X^.6.;o.-.Q...p..Q...1p..I>..E...N..D.RH..;..Q.....fVJ1=....Y.....<..h^.p^(`..Q.y.x..\|..g...Md..).;.!.<..!..S.J!.E==.x..Q....C%H.pSX..m..(`....E.y.4H...!.....ON.`Vy).V*.h.UH..c.....B....S<...j....oR..$.)..uJH..._.....|!>.#.A.).z#U~0R.*.t(.OR|#.1JA.E.TN`7.I..r.V|..b\....{I..]....x.W.}..{....!!..''7..r..G...X}.b.o...3....._k.]...0..I..{.1.....@.B..r'{.t....z.+.`...|.PE.....e....J.C.z...nKK.O...=r..S..e..!0.u.!'.q..,.+.;...'a...eq.....F.-..g.FhUF*....UNC.m.R.,- . .g1....(.9.[a..4=.L.M.).yc.....V_%..>8@d.....+._....At.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	9440
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	192:JsUOG1yNlX6ZzWpHOWLia16Cb7b4sUOG1yNlX6ZzWpHOWLia16Cb7bk:JsDhpNOWLiIb7b4sDhpNOWLiIb7bk
MD5:	9FDEE838E7C036092E81A4E7CC949643
SHA1:	364FC6C36972FFD803E5999AD501F3D7A2216FDF
SHA-256:	C6BF586821E13F7F6D6EF75AA82E69BD5E3E1336615C85AE513C70704F5C0787
SHA-512:	622BC3BD9F0615C191B03F2E8D018867C9D9ADCF1015DA5FB4D3462D71512B72558B32CA9F74A925C150B57FD232ABD48AFFC8D32128C50540DF02FCA8ECBB
Malicious:	false
Reputation:	low
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\es_local_coronavirus_LOGO[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1461 x 613, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	47133
Entropy (8bit):	7.86994529869928
Encrypted:	false
SSDEEP:	768:BtjJNt7Z6lzbFEsJINbPHJoSkmDUeNfqTLDSlDug3ueBdv5Cs6uSosJD/:LjboZEocbPH7kSUTSlDZ3ueH09PJD/
MD5:	646A7700594372DFC4D540A23B0D1CF5
SHA1:	EAA92CC75083639D88EC1C29084F553B4D6654F8
SHA-256:	4C87E0BBD9D09B0A036C07FBA7FB374530379C3BF92AFE8F49C0B6AAF7DB9FC9
SHA-512:	127E4FBF9C334438A2CCCC3C0B75EF1773D5B8BFFD1AEE0DB3EE7A688881884C452E117E7E8BECC1AA1384331BBA5906ED265C4A754AE48020DFAF19C8310DC1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/images/es_local_coronavirus_LOGO.png
Preview:	.PNG.....IHDR.....e.....pHYs.....&.?.. .IDATx..._|Uu...O...&.0$..L.....$.h.8.....&"\1...&..W &x.....b..wG.PM...3V<.../5.09.[K....o..f6]...|>.....|$.]...k...Z...4(.r.m.J..Y.\|.m..QJ...N.....1.....Bm$F...Y)U.K<S..:<x.....:...&.....A....Z.:.4.LU.F..&&.}3.../...../X.....0.P.^.. .:.~f..u.....:.f.....A.....[&.....5!...A..z..n.....$..6...5..]O`.`.S...D.....`..6.*...).....#.....P...Z.... !. .....6.km...R.....~..'.....+Bm.D/.....S..~_Oq..$.....@....Z..u..Av....A.n.....P.....,R.....!.F...~.j.,.nEl.....0.P.E..F.bK...^A.&t..V..:.;.....j.\...C/...}.cF$.....6.j.....S....R=..Lo.....B..)[...l.6..z.s\|t.=.....z.j.@.....}..M.j...l.....P.B.*[.q..#....,.....j.j'...w.....a..m.....T.P;\|r.m.e.?.f#DC:.....`>...a.>..D..n.....`^..".F..n..... .P;0tf#.$...9>:.....v .....v.r.m.j.9...PJ...v.....>.....u(.....}=r.....P.Cz.H..;./.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\f0234e85-9a07-ac77-5b5b-be7724994cd3[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.5257351171929923
Encrypted:	false
SSDEEP:	3:CUEIHh/:i4/
MD5:	13E1C7A2184E36D7AE519E99B1AA226F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\f0234e85-9a07-ac77-5b5b-be7724994cd3[1].gif	
SHA1:	355CCAD4EAC39838E1CC76FD0B670FD2EA1E5AA3
SHA-256:	48A33CA9F42B91902D57AD8AC52E1CE32B92C8C10C732F2DBB6FE960EBFD9438
SHA-512:	B1A6CFA7B21DBB0B281D241AF609F3BA7F3A63E5668095BBA912BF7CFD7F0320BAF7C3B0BFABD0F8609448F39902BAEB145BA7A2D8177FE22A6FCEA03DD29BE1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pr-bh.ybp.yahoo.com/sync/openx/f0234e85-9a07-ac77-5b5b-be7724994cd3?gdpr=0
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2213
Entropy (8bit):	5.4055823551793205
Encrypted:	false
SSDEEP:	48:ax0tF7QWGf8HFwiMPHAHF+lbPxOTbMnuNUofvof0:nsWGEHaHAHFPbMnuTO0
MD5:	8C97D8788EE127BD9111AC41A443DC09
SHA1:	BA87D83CB7A061EAAB7E37E5DCF962543490DB78
SHA-256:	23C061E7D440B7804C374DAE567E47162A04CACC44E35B5C35065629D8F2B3CE
SHA-512:	6DC3FF56C59B202CE869FB845C648E46DF29321C172A6704A203212E834EAABCFA107DF15B810AA514F223F1D6223235288102F95F2F6112EED9B6B74DA6963E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/pagead/js/r20210505/r20110914/client/window_focus.js
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .function e(a,b,d){a.addEventListener&&a.addEventListener(b,d,!1)};function g(a,b,d){if(Array.isArray(b))for(var c=0;c<b.length;c++)g(a,String(b[c]),d);else null!=b&&d.push(a+(""===b?"":"="+encodeURIComponent(String(b))))};function h(a,b){a.google_image_requests||(a.google_image_requests=[]);var d=a.document.createElement("img");d.src=b;a.google_image_requests.push(d)};function k(){var a=document.currentScript;return(a=void 0===a?null:a)&&"22"===a.getAttribute("data-jc")?a:document.querySelector('[data-jc="22"]')};var l=document,m=window;function n(){var a=p["gws-id"],b=p["qem-id"];this.l=p.url;this.m=a;this.o=b;this.i=!1;a=q(l.hidden)?{g:"hidden",h:"visibilitychange"}:q(l.mozHidden)?{g:"mozHidden",h:"mozvisibilitychange"}:q(l.msHidden)?{g:"msHidden",h:"msvisibilitychange"}:q(l.webkitHidden)?{g:"webkitHidden",h:"webkitvisibilitychange"}:{g:"hidden",h:"visibilitychange"};this.g=a.g;this.h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\f[2].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	15836
Entropy (8bit):	5.443481957824485
Encrypted:	false
SSDEEP:	384:KAkj7TW2wTyHtx41laMkYtviAFM+T3K24/amuaH:27TjwTT1lRXbT3K2oamus
MD5:	8BDC71E7FFC44A603ED7A63D908029AD
SHA1:	AC8860FC17606B38EC162787F2C93484684B33F6
SHA-256:	4D8470086B6A72C24D72AEBD855F89DA6D6A2E407164EC46014BE7E1465FAAF1
SHA-512:	A8945F406162C068E79777985AB08D6C1349FD368321DEF63D10DC4080D3FCCB8B3FD5A2DE8FEFA665C09F9F937A4238397C10E456DCBB8EE955D1C3CD0335
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/pagead/js/r20210505/r20110914/client/qs_click_protection.js
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .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 ea(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 k(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:aa(a)}}function fa(a){if(!(a instanceof Ar

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\font-awesome.min[1].css	
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\9026IKNJ\fotonoticia_20210506114015_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, 1024x576, frames 3
Category:	downloaded
Size (bytes):	93982
Entropy (8bit):	7.9568929539188975
Encrypted:	false
SSDEEP:	1536:Ia4Kc6hrSr+ysTTDlyk5NlfRsPGa++YIaTzWy5IfJGgIs6IIEzxFll:oKlu+ysf5yiHfRAQ+eWy5uGDsaEzf
MD5:	55A8B1037C759E24B1A2F8AB9637DBDE
SHA1:	53190B51262BACF43769788232D60D70E14D4458
SHA-256:	D7A30E1448D7F6743304384ADEB3DCE6F273ED9834E027ED41DB12E50DE3CF35
SHA-512:	34B3C193CA24189D9A596FA09BF074E17611BA11F94841B87B31D5D3939B16EB2E86A78C5090C039A421EAE7EBC899694B1FA0819F04D8E03F132E35351FE1D8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img.europapress.es/fotoweb/fotonoticia_20210506114015_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..... .....?....~0:._...X...q.^K...fa.w._.Ez.}.}.|./...wg.|Fb<ag..=...B5.....Goj..x.....?.*.i?....(..(...H.\&..c .U.....qn.....i=...Wo.....<..R.....fs...<5i.._K....q.....8...).>...'.@..5...|!.g .y..Z%.....?:3\G`.....Z.L.R(.....k.w.)..#..*....q.dq.G.*..t.....i{...w.....:X....z.....W.....>..2.....v.M..?1]X...s..y.h.....%...Ezq"...W.E..%~.=...+

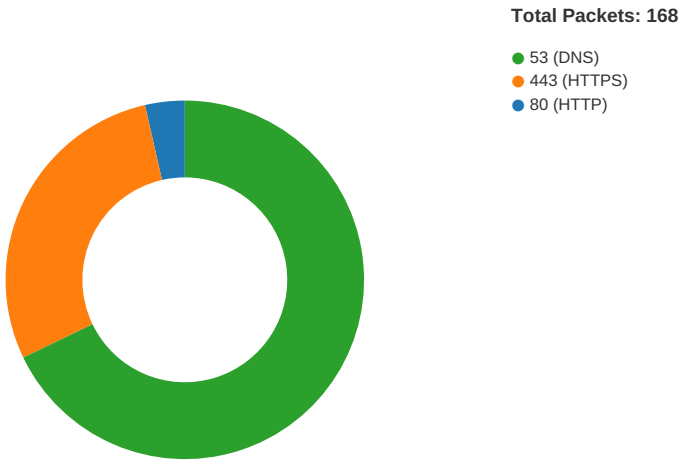
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\hotjar-2075733[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3502
Entropy (8bit):	5.250106220561627
Encrypted:	false
SSDEEP:	48:Z1f+Bmr4DDiIr/CpDuMY6wRQAQl07k5G8r4U4R5UETledeHtwWNxsTnOf3DZ:ORPi6/snIQg24U4bU4qO0qTZ
MD5:	0B42C46D0511566FB0AA2DDC34D6F585
SHA1:	09F69BFBB93271C43307D1EFEEFC547CF368E15E
SHA-256:	AC77F7A971CDA919D497BD657C41D77F3F342D49155D8936788B580481EF5A5F
SHA-512:	15062A19963273FEFFF9BD279581ABCCEB085C5EC68BC12AB334EFA05774CF854EA5EC68E1CDC466E866627CCDCCF22671021645FBE78B65A0D15D4836D123B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.hotjar.com/c/hotjar-2075733.js?sv=6
Preview:	window.hjSiteSettings = window.hjSiteSettings || {"site_id":2075733,"r":0.493100070271164,"rec_value":0.0,"state_change_listen_mode":"automatic","record":false,"continuous_capture_enabled":false,"recording_capture_keystrokes":false,"anonymize_digits":true,"anonymize_emails":true,"suppress_all":false,"suppress_text":false,"suppress_location":false,"user_attributes_enabled":false,"legal_name":null,"privacy_policy_url":null,"deferred_page_contents":[],"record_targeting_rules":[],"feedback_widgets":[],"heatmaps":[],"polls":[],"integrations":{"optimizely":{"tag_recordings":false}},"features":["heatmap.continuous_capture","recordings.filter_new_user","survey.impressions","feedback.widgetV2","feedback.full_screen_survey","settings.billing_v2","feedback.widget_telemetry"]};..!function(e){var t={};function n(o){if(t[o])return t[o].exports;var r=t[o]={i:o,l:!1,exports:{}};return e[o].call(r.exports,r,r.exports,n),r.l=!0,r.exports}n.m=e,n.c=t,n.d=function(e,t,o){n.o(e,t)||Object.defineProperty(e,

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2021 10:11:05.755146980 CEST	49733	80	192.168.2.4	172.67.183.244
May 10, 2021 10:11:05.755212069 CEST	49734	80	192.168.2.4	172.67.183.244
May 10, 2021 10:11:05.796180010 CEST	80	49733	172.67.183.244	192.168.2.4
May 10, 2021 10:11:05.796874046 CEST	49733	80	192.168.2.4	172.67.183.244
May 10, 2021 10:11:05.799077034 CEST	80	49734	172.67.183.244	192.168.2.4
May 10, 2021 10:11:05.799688101 CEST	49734	80	192.168.2.4	172.67.183.244
May 10, 2021 10:11:05.800451994 CEST	49734	80	192.168.2.4	172.67.183.244
May 10, 2021 10:11:05.841443062 CEST	80	49734	172.67.183.244	192.168.2.4
May 10, 2021 10:11:05.853977919 CEST	80	49734	172.67.183.244	192.168.2.4
May 10, 2021 10:11:05.854413986 CEST	49734	80	192.168.2.4	172.67.183.244
May 10, 2021 10:11:05.865199089 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:05.908385038 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:05.908504963 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:05.913888931 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:05.954883099 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:05.959644079 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:05.959687948 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:05.959773064 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.001758099 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.007802010 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.008085012 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.042622089 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.047151089 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.047179937 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.047211885 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.047240973 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.048244953 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.048563957 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.048648119 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.048724890 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.088057041 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.130987883 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.375900030 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.375926018 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.375957012 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.375977039 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.376008987 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.376030922 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.376075983 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.376133919 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.376302004 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.376319885 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.376358986 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.376406908 CEST	49735	443	192.168.2.4	172.67.183.244

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2021 10:11:06.376833916 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.376868010 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.376918077 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.376943111 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.404685974 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.404716969 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.404753923 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.404778004 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.404845953 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.404881001 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.405288935 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.405330896 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.405365944 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.405401945 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.406267881 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.406286001 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.406388998 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.407284975 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.407315969 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.407371044 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.407414913 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.408157110 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.408235073 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.509572029 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.510301113 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.510996103 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.511679888 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.512367964 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.513035059 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.515749931 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.516480923 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.517184019 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.517855883 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.550445080 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.550923109 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.551639080 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.552464008 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.553002119 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.553692102 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.556467056 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.557259083 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.557801962 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.559370995 CEST	443	49735	172.67.183.244	192.168.2.4
May 10, 2021 10:11:06.599277973 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.600400925 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.601111889 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.601799965 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.602727890 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.603420019 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.604135990 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.604823112 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.605494022 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.606164932 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.607810974 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.608606100 CEST	49735	443	192.168.2.4	172.67.183.244
May 10, 2021 10:11:06.609308958 CEST	49735	443	192.168.2.4	172.67.183.244

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2021 10:10:56.152383089 CEST	49714	53	192.168.2.4	8.8.8.8
May 10, 2021 10:10:56.201565027 CEST	53	49714	8.8.8.8	192.168.2.4
May 10, 2021 10:10:56.452436924 CEST	58028	53	192.168.2.4	8.8.8.8
May 10, 2021 10:10:56.454364061 CEST	53097	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2021 10:10:56.503015995 CEST	53	58028	8.8.8.8	192.168.2.4
May 10, 2021 10:10:56.503040075 CEST	53	53097	8.8.8.8	192.168.2.4
May 10, 2021 10:10:56.672424078 CEST	49257	53	192.168.2.4	8.8.8.8
May 10, 2021 10:10:56.726994991 CEST	53	49257	8.8.8.8	192.168.2.4
May 10, 2021 10:10:56.779613972 CEST	62389	53	192.168.2.4	8.8.8.8
May 10, 2021 10:10:56.843008041 CEST	53	62389	8.8.8.8	192.168.2.4
May 10, 2021 10:10:58.471132040 CEST	49910	53	192.168.2.4	8.8.8.8
May 10, 2021 10:10:58.522819042 CEST	53	49910	8.8.8.8	192.168.2.4
May 10, 2021 10:11:04.370275974 CEST	55854	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:04.431668997 CEST	53	55854	8.8.8.8	192.168.2.4
May 10, 2021 10:11:05.675075054 CEST	64549	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:05.740120888 CEST	53	64549	8.8.8.8	192.168.2.4
May 10, 2021 10:11:06.523390055 CEST	63153	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:06.535115004 CEST	52991	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:06.552779913 CEST	53700	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:06.582114935 CEST	53	63153	8.8.8.8	192.168.2.4
May 10, 2021 10:11:06.592086077 CEST	53	52991	8.8.8.8	192.168.2.4
May 10, 2021 10:11:06.602277994 CEST	53	53700	8.8.8.8	192.168.2.4
May 10, 2021 10:11:06.832447052 CEST	51726	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:06.891803980 CEST	53	51726	8.8.8.8	192.168.2.4
May 10, 2021 10:11:07.430075884 CEST	56794	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:07.447062969 CEST	56534	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:07.489548922 CEST	53	56794	8.8.8.8	192.168.2.4
May 10, 2021 10:11:07.651459932 CEST	53	56534	8.8.8.8	192.168.2.4
May 10, 2021 10:11:07.800306082 CEST	56627	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:07.885482073 CEST	53	56627	8.8.8.8	192.168.2.4
May 10, 2021 10:11:08.158102989 CEST	56621	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:08.215462923 CEST	53	56621	8.8.8.8	192.168.2.4
May 10, 2021 10:11:08.264507055 CEST	63116	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:08.268613100 CEST	64078	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:08.286444902 CEST	64801	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:08.321952105 CEST	61721	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:08.324240923 CEST	53	63116	8.8.8.8	192.168.2.4
May 10, 2021 10:11:08.327593088 CEST	53	64078	8.8.8.8	192.168.2.4
May 10, 2021 10:11:08.339030981 CEST	51255	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:08.355464935 CEST	61522	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:08.381578922 CEST	53	61721	8.8.8.8	192.168.2.4
May 10, 2021 10:11:08.395881891 CEST	53	51255	8.8.8.8	192.168.2.4
May 10, 2021 10:11:08.409452915 CEST	52337	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:08.420522928 CEST	53	61522	8.8.8.8	192.168.2.4
May 10, 2021 10:11:08.434986115 CEST	55046	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:08.450695992 CEST	49612	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:08.455727100 CEST	49285	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:08.463519096 CEST	50601	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:08.466852903 CEST	53	52337	8.8.8.8	192.168.2.4
May 10, 2021 10:11:08.496784925 CEST	53	55046	8.8.8.8	192.168.2.4
May 10, 2021 10:11:08.511832952 CEST	53	49612	8.8.8.8	192.168.2.4
May 10, 2021 10:11:08.529650927 CEST	53	49285	8.8.8.8	192.168.2.4
May 10, 2021 10:11:08.534576893 CEST	60875	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:08.549181938 CEST	53	50601	8.8.8.8	192.168.2.4
May 10, 2021 10:11:08.575299025 CEST	56448	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:08.584857941 CEST	59172	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:08.589209080 CEST	53	60875	8.8.8.8	192.168.2.4
May 10, 2021 10:11:08.598861933 CEST	62420	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:08.633658886 CEST	53	59172	8.8.8.8	192.168.2.4
May 10, 2021 10:11:08.650402069 CEST	60579	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:08.658555984 CEST	53	62420	8.8.8.8	192.168.2.4
May 10, 2021 10:11:08.670881987 CEST	53	56448	8.8.8.8	192.168.2.4
May 10, 2021 10:11:08.703252077 CEST	53	60579	8.8.8.8	192.168.2.4
May 10, 2021 10:11:08.750960112 CEST	53	64801	8.8.8.8	192.168.2.4
May 10, 2021 10:11:08.790102959 CEST	50183	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:08.843393087 CEST	53	50183	8.8.8.8	192.168.2.4
May 10, 2021 10:11:09.100333929 CEST	61531	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:09.140696049 CEST	49228	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2021 10:11:09.168488026 CEST	53	61531	8.8.8.8	192.168.2.4
May 10, 2021 10:11:09.198414087 CEST	53	49228	8.8.8.8	192.168.2.4
May 10, 2021 10:11:09.252971888 CEST	59794	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:09.314805984 CEST	53	59794	8.8.8.8	192.168.2.4
May 10, 2021 10:11:09.694864988 CEST	55916	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:09.714507103 CEST	52752	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:09.754501104 CEST	53	55916	8.8.8.8	192.168.2.4
May 10, 2021 10:11:09.770504951 CEST	53	52752	8.8.8.8	192.168.2.4
May 10, 2021 10:11:09.995213032 CEST	60542	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:10.046838045 CEST	53	60542	8.8.8.8	192.168.2.4
May 10, 2021 10:11:10.253566980 CEST	60689	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:10.259859085 CEST	64206	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:10.266980886 CEST	50904	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:10.302212954 CEST	57525	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:10.310937881 CEST	53	60689	8.8.8.8	192.168.2.4
May 10, 2021 10:11:10.325153112 CEST	53	64206	8.8.8.8	192.168.2.4
May 10, 2021 10:11:10.328874111 CEST	53	50904	8.8.8.8	192.168.2.4
May 10, 2021 10:11:10.332792044 CEST	53814	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:10.341368914 CEST	53418	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:10.362452984 CEST	53	57525	8.8.8.8	192.168.2.4
May 10, 2021 10:11:10.389940977 CEST	53	53814	8.8.8.8	192.168.2.4
May 10, 2021 10:11:10.397775888 CEST	62833	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:10.398469925 CEST	53	53418	8.8.8.8	192.168.2.4
May 10, 2021 10:11:10.457544088 CEST	53	62833	8.8.8.8	192.168.2.4
May 10, 2021 10:11:10.894700050 CEST	59260	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:10.962385893 CEST	53	59260	8.8.8.8	192.168.2.4
May 10, 2021 10:11:12.295125008 CEST	49944	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:12.312375069 CEST	63300	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:12.352356911 CEST	53	49944	8.8.8.8	192.168.2.4
May 10, 2021 10:11:12.377706051 CEST	53	63300	8.8.8.8	192.168.2.4
May 10, 2021 10:11:16.085001945 CEST	61449	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:16.135000944 CEST	53	61449	8.8.8.8	192.168.2.4
May 10, 2021 10:11:18.837682009 CEST	51275	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:18.897881031 CEST	53	51275	8.8.8.8	192.168.2.4
May 10, 2021 10:11:18.992187977 CEST	63492	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:19.019793987 CEST	58945	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:19.059505939 CEST	53	63492	8.8.8.8	192.168.2.4
May 10, 2021 10:11:19.084827900 CEST	53	58945	8.8.8.8	192.168.2.4
May 10, 2021 10:11:19.105437040 CEST	60779	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:19.118227959 CEST	64014	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:19.125231981 CEST	57091	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:19.133028984 CEST	55904	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:19.154174089 CEST	53	60779	8.8.8.8	192.168.2.4
May 10, 2021 10:11:19.171276093 CEST	53	64014	8.8.8.8	192.168.2.4
May 10, 2021 10:11:19.174019098 CEST	53	57091	8.8.8.8	192.168.2.4
May 10, 2021 10:11:19.193526030 CEST	53	55904	8.8.8.8	192.168.2.4
May 10, 2021 10:11:19.675381899 CEST	52109	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:19.736304998 CEST	53	52109	8.8.8.8	192.168.2.4
May 10, 2021 10:11:21.316943884 CEST	54450	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:21.374099016 CEST	53	54450	8.8.8.8	192.168.2.4
May 10, 2021 10:11:22.431127071 CEST	49374	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:22.431883097 CEST	50436	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:22.480029106 CEST	53	49374	8.8.8.8	192.168.2.4
May 10, 2021 10:11:22.503618002 CEST	53	50436	8.8.8.8	192.168.2.4
May 10, 2021 10:11:23.006144047 CEST	62605	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:23.054935932 CEST	53	62605	8.8.8.8	192.168.2.4
May 10, 2021 10:11:26.712624073 CEST	54256	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:26.764581919 CEST	53	54256	8.8.8.8	192.168.2.4
May 10, 2021 10:11:27.993407011 CEST	52189	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:28.044136047 CEST	53	52189	8.8.8.8	192.168.2.4
May 10, 2021 10:11:28.531982899 CEST	56131	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:28.593698025 CEST	53	56131	8.8.8.8	192.168.2.4
May 10, 2021 10:11:28.913366079 CEST	62992	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:28.970820904 CEST	53	62992	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2021 10:11:34.493149996 CEST	54432	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:34.543857098 CEST	53	54432	8.8.8.8	192.168.2.4
May 10, 2021 10:11:34.633929014 CEST	57227	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:34.684443951 CEST	53	57227	8.8.8.8	192.168.2.4
May 10, 2021 10:11:35.100963116 CEST	58383	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:35.150938988 CEST	53	58383	8.8.8.8	192.168.2.4
May 10, 2021 10:11:35.518640041 CEST	54432	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:35.575788975 CEST	53	54432	8.8.8.8	192.168.2.4
May 10, 2021 10:11:36.106225967 CEST	58383	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:36.156625986 CEST	53	58383	8.8.8.8	192.168.2.4
May 10, 2021 10:11:36.733556032 CEST	54432	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:36.782164097 CEST	53	54432	8.8.8.8	192.168.2.4
May 10, 2021 10:11:37.121589899 CEST	58383	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:37.170114040 CEST	53	58383	8.8.8.8	192.168.2.4
May 10, 2021 10:11:38.733457088 CEST	54432	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:38.783945084 CEST	53	54432	8.8.8.8	192.168.2.4
May 10, 2021 10:11:39.269459963 CEST	58383	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:39.318358898 CEST	53	58383	8.8.8.8	192.168.2.4
May 10, 2021 10:11:42.590740919 CEST	63136	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:42.661628008 CEST	53	63136	8.8.8.8	192.168.2.4
May 10, 2021 10:11:42.738028049 CEST	54432	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:42.801831007 CEST	53	54432	8.8.8.8	192.168.2.4
May 10, 2021 10:11:43.284573078 CEST	58383	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:43.333467960 CEST	50911	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:43.341852903 CEST	53	58383	8.8.8.8	192.168.2.4
May 10, 2021 10:11:43.385581017 CEST	53	50911	8.8.8.8	192.168.2.4
May 10, 2021 10:11:44.442583084 CEST	63409	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:44.491322994 CEST	53	63409	8.8.8.8	192.168.2.4
May 10, 2021 10:11:45.204813957 CEST	59185	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:45.265201092 CEST	53	59185	8.8.8.8	192.168.2.4
May 10, 2021 10:11:47.043420076 CEST	64236	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:47.111886978 CEST	53	64236	8.8.8.8	192.168.2.4
May 10, 2021 10:11:51.824023008 CEST	56157	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:51.876101017 CEST	53	56157	8.8.8.8	192.168.2.4
May 10, 2021 10:11:56.491756916 CEST	55601	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:56.540539980 CEST	53	55601	8.8.8.8	192.168.2.4
May 10, 2021 10:11:58.431716919 CEST	52984	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:58.471838951 CEST	51141	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:58.495246887 CEST	53	52984	8.8.8.8	192.168.2.4
May 10, 2021 10:11:58.536025047 CEST	53	51141	8.8.8.8	192.168.2.4
May 10, 2021 10:11:59.321907997 CEST	53610	53	192.168.2.4	8.8.8.8
May 10, 2021 10:11:59.370601892 CEST	53	53610	8.8.8.8	192.168.2.4
May 10, 2021 10:12:00.439743996 CEST	61247	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:00.491259098 CEST	53	61247	8.8.8.8	192.168.2.4
May 10, 2021 10:12:01.622905970 CEST	65165	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:01.678461075 CEST	53	65165	8.8.8.8	192.168.2.4
May 10, 2021 10:12:02.961061954 CEST	52076	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:03.011034966 CEST	53	52076	8.8.8.8	192.168.2.4
May 10, 2021 10:12:04.696547985 CEST	54903	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:04.748171091 CEST	53	54903	8.8.8.8	192.168.2.4
May 10, 2021 10:12:05.931792974 CEST	55045	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:05.985574961 CEST	53	55045	8.8.8.8	192.168.2.4
May 10, 2021 10:12:06.747833014 CEST	54464	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:06.798368931 CEST	53	54464	8.8.8.8	192.168.2.4
May 10, 2021 10:12:10.586193085 CEST	50970	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:10.638082027 CEST	53	50970	8.8.8.8	192.168.2.4
May 10, 2021 10:12:10.836546898 CEST	55261	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:10.905545950 CEST	53	55261	8.8.8.8	192.168.2.4
May 10, 2021 10:12:20.686439991 CEST	59809	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:20.735290051 CEST	53	59809	8.8.8.8	192.168.2.4
May 10, 2021 10:12:24.880423069 CEST	51278	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:24.931936979 CEST	53	51278	8.8.8.8	192.168.2.4
May 10, 2021 10:12:26.656172037 CEST	51932	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:26.745511055 CEST	53	51932	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2021 10:12:30.213506937 CEST	59494	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:30.262245893 CEST	53	59494	8.8.8.8	192.168.2.4
May 10, 2021 10:12:30.540936947 CEST	55915	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:30.621968985 CEST	53	55915	8.8.8.8	192.168.2.4
May 10, 2021 10:12:31.214323044 CEST	49779	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:31.263120890 CEST	53	49779	8.8.8.8	192.168.2.4
May 10, 2021 10:12:31.893657923 CEST	49458	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:31.963289022 CEST	53	49458	8.8.8.8	192.168.2.4
May 10, 2021 10:12:41.112062931 CEST	57164	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:41.185616016 CEST	53	57164	8.8.8.8	192.168.2.4
May 10, 2021 10:12:41.238101959 CEST	49840	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:41.307003975 CEST	53	49840	8.8.8.8	192.168.2.4
May 10, 2021 10:12:52.665421963 CEST	57174	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:52.690781116 CEST	58531	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:52.727296114 CEST	53	57174	8.8.8.8	192.168.2.4
May 10, 2021 10:12:52.739433050 CEST	53	58531	8.8.8.8	192.168.2.4
May 10, 2021 10:12:53.035568953 CEST	49608	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:53.097819090 CEST	53	49608	8.8.8.8	192.168.2.4
May 10, 2021 10:12:53.375446081 CEST	55682	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:53.432614088 CEST	53	55682	8.8.8.8	192.168.2.4
May 10, 2021 10:12:57.022046089 CEST	62436	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:57.081319094 CEST	53	62436	8.8.8.8	192.168.2.4
May 10, 2021 10:12:58.850353956 CEST	61230	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:58.901453018 CEST	53	61230	8.8.8.8	192.168.2.4
May 10, 2021 10:12:59.026529074 CEST	64730	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:59.060745955 CEST	60624	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:59.089896917 CEST	53	64730	8.8.8.8	192.168.2.4
May 10, 2021 10:12:59.118630886 CEST	53	60624	8.8.8.8	192.168.2.4
May 10, 2021 10:12:59.333374023 CEST	62600	53	192.168.2.4	8.8.8.8
May 10, 2021 10:12:59.399159908 CEST	53	62600	8.8.8.8	192.168.2.4
May 10, 2021 10:13:02.479185104 CEST	53200	53	192.168.2.4	8.8.8.8
May 10, 2021 10:13:02.543340921 CEST	53	53200	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 10, 2021 10:11:05.675075054 CEST	192.168.2.4	8.8.8.8	0x12a	Standard query (0)	localcoronavirus.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:07.430075884 CEST	192.168.2.4	8.8.8.8	0x9004	Standard query (0)	phantom-expansion.unidadeditorial.es	A (IP address)	IN (0x0001)
May 10, 2021 10:11:07.447062969 CEST	192.168.2.4	8.8.8.8	0xace2	Standard query (0)	cdn2.excelsior.com.mx	A (IP address)	IN (0x0001)
May 10, 2021 10:11:07.800306082 CEST	192.168.2.4	8.8.8.8	0xa84b	Standard query (0)	static4.abc.es	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.158102989 CEST	192.168.2.4	8.8.8.8	0x4f29	Standard query (0)	www.lavozdegalicia.es	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.264507055 CEST	192.168.2.4	8.8.8.8	0xcf48	Standard query (0)	cronicaglobal.elespanol.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.268613100 CEST	192.168.2.4	8.8.8.8	0x98f8	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.286444902 CEST	192.168.2.4	8.8.8.8	0x7855	Standard query (0)	www.republica.com.uy	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.321952105 CEST	192.168.2.4	8.8.8.8	0x79ac	Standard query (0)	imagenes.20minutos.es	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.339030981 CEST	192.168.2.4	8.8.8.8	0xe504	Standard query (0)	ep00.epimg.net	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.355464935 CEST	192.168.2.4	8.8.8.8	0x220a	Standard query (0)	d3cra5ec8gdi8w.cloudfront.net	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.409452915 CEST	192.168.2.4	8.8.8.8	0x78cc	Standard query (0)	i.blogs.es	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.434986115 CEST	192.168.2.4	8.8.8.8	0x5479	Standard query (0)	img.huffingtonpost.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.450695992 CEST	192.168.2.4	8.8.8.8	0xd4df	Standard query (0)	as01.epimg.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 10, 2021 10:11:08.455727100 CEST	192.168.2.4	8.8.8.8	0xdfd	Standard query (0)	img2.rtve.es	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.463519096 CEST	192.168.2.4	8.8.8.8	0x482b	Standard query (0)	www.puntodebreak.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.534576893 CEST	192.168.2.4	8.8.8.8	0xbb97	Standard query (0)	phantom-elmundo.unidadeditorial.es	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.575299025 CEST	192.168.2.4	8.8.8.8	0x652c	Standard query (0)	static2.abc.es	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.584857941 CEST	192.168.2.4	8.8.8.8	0xf4d2	Standard query (0)	s1.eestatic.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.598861933 CEST	192.168.2.4	8.8.8.8	0x2b18	Standard query (0)	www.elconfidencialdigital.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.650402069 CEST	192.168.2.4	8.8.8.8	0x8788	Standard query (0)	platform.twitter.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.790102959 CEST	192.168.2.4	8.8.8.8	0x1ecf	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)
May 10, 2021 10:11:09.100333929 CEST	192.168.2.4	8.8.8.8	0xb06	Standard query (0)	static.hotjar.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:09.252971888 CEST	192.168.2.4	8.8.8.8	0xeac9	Standard query (0)	proteccion10.net	A (IP address)	IN (0x0001)
May 10, 2021 10:11:09.694864988 CEST	192.168.2.4	8.8.8.8	0x9847	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
May 10, 2021 10:11:09.714507103 CEST	192.168.2.4	8.8.8.8	0x38b5	Standard query (0)	script.hotjar.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:10.259859085 CEST	192.168.2.4	8.8.8.8	0x806a	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
May 10, 2021 10:11:10.266980886 CEST	192.168.2.4	8.8.8.8	0x3fe9	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
May 10, 2021 10:11:10.332792044 CEST	192.168.2.4	8.8.8.8	0x76fb	Standard query (0)	adservice.google.ch	A (IP address)	IN (0x0001)
May 10, 2021 10:11:10.397775888 CEST	192.168.2.4	8.8.8.8	0x6cd8	Standard query (0)	www.googletagservices.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:10.894700050 CEST	192.168.2.4	8.8.8.8	0x2ee0	Standard query (0)	vars.hotjar.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:12.312375069 CEST	192.168.2.4	8.8.8.8	0x4469	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
May 10, 2021 10:11:18.992187977 CEST	192.168.2.4	8.8.8.8	0x4956	Standard query (0)	vc.hotjar.io	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.019793987 CEST	192.168.2.4	8.8.8.8	0x7c5d	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.105437040 CEST	192.168.2.4	8.8.8.8	0xa87d	Standard query (0)	odr.mookie1.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.118227959 CEST	192.168.2.4	8.8.8.8	0xb1eb	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.125231981 CEST	192.168.2.4	8.8.8.8	0x57a5	Standard query (0)	image6.pubmatic.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.133028984 CEST	192.168.2.4	8.8.8.8	0x977b	Standard query (0)	cc.adingo.jp	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.675381899 CEST	192.168.2.4	8.8.8.8	0x1e0d	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
May 10, 2021 10:11:21.316943884 CEST	192.168.2.4	8.8.8.8	0xbb70	Standard query (0)	token.rubiconproject.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:22.431127071 CEST	192.168.2.4	8.8.8.8	0x415a	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
May 10, 2021 10:11:22.431883097 CEST	192.168.2.4	8.8.8.8	0x86e2	Standard query (0)	c1.adform.net	A (IP address)	IN (0x0001)
May 10, 2021 10:11:23.006144047 CEST	192.168.2.4	8.8.8.8	0xd1ef	Standard query (0)	eu-u.openx.net	A (IP address)	IN (0x0001)
May 10, 2021 10:11:28.531982899 CEST	192.168.2.4	8.8.8.8	0x13fa	Standard query (0)	localcoronavirus.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:42.590740919 CEST	192.168.2.4	8.8.8.8	0xbf32	Standard query (0)	pixel.quantserve.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:44.442583084 CEST	192.168.2.4	8.8.8.8	0xf580	Standard query (0)	sync.mathtag.com	A (IP address)	IN (0x0001)
May 10, 2021 10:11:45.204813957 CEST	192.168.2.4	8.8.8.8	0xcbce	Standard query (0)	match.prod.bidr.io	A (IP address)	IN (0x0001)
May 10, 2021 10:11:47.043420076 CEST	192.168.2.4	8.8.8.8	0x219d	Standard query (0)	facebook.com	A (IP address)	IN (0x0001)
May 10, 2021 10:12:24.880423069 CEST	192.168.2.4	8.8.8.8	0xe06d	Standard query (0)	x.bidswitch.net	A (IP address)	IN (0x0001)
May 10, 2021 10:12:26.656172037 CEST	192.168.2.4	8.8.8.8	0xe952	Standard query (0)	pool.admedo.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 10, 2021 10:12:30.213506937 CEST	192.168.2.4	8.8.8.8	0x2cf7	Standard query (0)	pm.w55c.net	A (IP address)	IN (0x0001)
May 10, 2021 10:12:31.214323044 CEST	192.168.2.4	8.8.8.8	0xa58d	Standard query (0)	pr-bh.ybp.yahoo.com	A (IP address)	IN (0x0001)
May 10, 2021 10:12:31.893657923 CEST	192.168.2.4	8.8.8.8	0xdd20	Standard query (0)	r6---sn-n02xgoxufvg3-2gbs.googlevideo.com	A (IP address)	IN (0x0001)
May 10, 2021 10:12:41.112062931 CEST	192.168.2.4	8.8.8.8	0x2401	Standard query (0)	img.europapress.es	A (IP address)	IN (0x0001)
May 10, 2021 10:12:41.238101959 CEST	192.168.2.4	8.8.8.8	0xb0c8	Standard query (0)	ficheracos.publico.es	A (IP address)	IN (0x0001)
May 10, 2021 10:12:52.665421963 CEST	192.168.2.4	8.8.8.8	0xe382	Standard query (0)	dsp.active-agent.com	A (IP address)	IN (0x0001)
May 10, 2021 10:12:52.690781116 CEST	192.168.2.4	8.8.8.8	0x7bce	Standard query (0)	dsp.adfarm1.adition.com	A (IP address)	IN (0x0001)
May 10, 2021 10:12:53.035568953 CEST	192.168.2.4	8.8.8.8	0x6d2e	Standard query (0)	dspcluster.adfarm1.adition.com	A (IP address)	IN (0x0001)
May 10, 2021 10:12:53.375446081 CEST	192.168.2.4	8.8.8.8	0x5d	Standard query (0)	ad.ad-srv.net	A (IP address)	IN (0x0001)
May 10, 2021 10:12:57.022046089 CEST	192.168.2.4	8.8.8.8	0x74b3	Standard query (0)	ad14.ad-srv.net	A (IP address)	IN (0x0001)
May 10, 2021 10:12:58.850353956 CEST	192.168.2.4	8.8.8.8	0x1428	Standard query (0)	rtb.openx.net	A (IP address)	IN (0x0001)
May 10, 2021 10:12:59.026529074 CEST	192.168.2.4	8.8.8.8	0x5689	Standard query (0)	www.awin1.com	A (IP address)	IN (0x0001)
May 10, 2021 10:12:59.060745955 CEST	192.168.2.4	8.8.8.8	0x55fb	Standard query (0)	cdn.contentspread.net	A (IP address)	IN (0x0001)
May 10, 2021 10:12:59.333374023 CEST	192.168.2.4	8.8.8.8	0x65f8	Standard query (0)	media.kaspersky.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:11:05.740120888 CEST	8.8.8.8	192.168.2.4	0x12a	No error (0)	localcoronavirus.com		172.67.183.244	A (IP address)	IN (0x0001)
May 10, 2021 10:11:05.740120888 CEST	8.8.8.8	192.168.2.4	0x12a	No error (0)	localcoronavirus.com		104.21.18.245	A (IP address)	IN (0x0001)
May 10, 2021 10:11:07.489548922 CEST	8.8.8.8	192.168.2.4	0x9004	No error (0)	phantom-expansion.unidadeditorial.es	dbpabf0off7y1.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:07.489548922 CEST	8.8.8.8	192.168.2.4	0x9004	No error (0)	dbpabf0off7y1.cloudfront.net		65.9.66.100	A (IP address)	IN (0x0001)
May 10, 2021 10:11:07.489548922 CEST	8.8.8.8	192.168.2.4	0x9004	No error (0)	dbpabf0off7y1.cloudfront.net		65.9.66.34	A (IP address)	IN (0x0001)
May 10, 2021 10:11:07.489548922 CEST	8.8.8.8	192.168.2.4	0x9004	No error (0)	dbpabf0off7y1.cloudfront.net		65.9.66.65	A (IP address)	IN (0x0001)
May 10, 2021 10:11:07.489548922 CEST	8.8.8.8	192.168.2.4	0x9004	No error (0)	dbpabf0off7y1.cloudfront.net		65.9.66.80	A (IP address)	IN (0x0001)
May 10, 2021 10:11:07.651459932 CEST	8.8.8.8	192.168.2.4	0xace2	No error (0)	cdn2.excelsior.com.mx	d37ub18b7ivraq.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:07.651459932 CEST	8.8.8.8	192.168.2.4	0xace2	No error (0)	d37ub18b7ivraq.cloudfront.net		99.86.2.109	A (IP address)	IN (0x0001)
May 10, 2021 10:11:07.651459932 CEST	8.8.8.8	192.168.2.4	0xace2	No error (0)	d37ub18b7ivraq.cloudfront.net		99.86.2.100	A (IP address)	IN (0x0001)
May 10, 2021 10:11:07.651459932 CEST	8.8.8.8	192.168.2.4	0xace2	No error (0)	d37ub18b7ivraq.cloudfront.net		99.86.2.5	A (IP address)	IN (0x0001)
May 10, 2021 10:11:07.651459932 CEST	8.8.8.8	192.168.2.4	0xace2	No error (0)	d37ub18b7ivraq.cloudfront.net		99.86.2.114	A (IP address)	IN (0x0001)
May 10, 2021 10:11:07.885482073 CEST	8.8.8.8	192.168.2.4	0xa84b	No error (0)	static4.abc.es	static.abc.es		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:07.885482073 CEST	8.8.8.8	192.168.2.4	0xa84b	No error (0)	static.abc.es	static-abc.akamaized.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:11:08.215462923 CEST	8.8.8.8	192.168.2.4	0x4f29	No error (0)	www.lavozdegalicia.es	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.215462923 CEST	8.8.8.8	192.168.2.4	0x4f29	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		52.211.67.210	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.215462923 CEST	8.8.8.8	192.168.2.4	0x4f29	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		52.211.217.51	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.215462923 CEST	8.8.8.8	192.168.2.4	0x4f29	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		54.194.190.147	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.215462923 CEST	8.8.8.8	192.168.2.4	0x4f29	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		54.194.71.119	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.215462923 CEST	8.8.8.8	192.168.2.4	0x4f29	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		34.249.141.22	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.215462923 CEST	8.8.8.8	192.168.2.4	0x4f29	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		52.210.129.255	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.324240923 CEST	8.8.8.8	192.168.2.4	0xcf48	No error (0)	cronicaglobal.elespanol.com	caching.elespanol.edge2befaster.io		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.324240923 CEST	8.8.8.8	192.168.2.4	0xcf48	No error (0)	caching.elespanol.edge2befaster.io	caching.meta-cluster-03.edge2befaster.io		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.324240923 CEST	8.8.8.8	192.168.2.4	0xcf48	No error (0)	caching.meta-cluster-03.edge2befaster.io	cec01.eug.edgetcdn.io		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.324240923 CEST	8.8.8.8	192.168.2.4	0xcf48	No error (0)	cec01.eug.edgetcdn.io		51.68.35.185	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.324240923 CEST	8.8.8.8	192.168.2.4	0xcf48	No error (0)	cec01.eug.edgetcdn.io		51.255.81.138	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.327593088 CEST	8.8.8.8	192.168.2.4	0x98f8	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.327593088 CEST	8.8.8.8	192.168.2.4	0x98f8	No error (0)	scontent.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.381578922 CEST	8.8.8.8	192.168.2.4	0x79ac	No error (0)	imagenes.20minutos.es	di7juyclzlgyp.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.381578922 CEST	8.8.8.8	192.168.2.4	0x79ac	No error (0)	di7juyclzlgyp.cloudfront.net		13.32.25.102	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.381578922 CEST	8.8.8.8	192.168.2.4	0x79ac	No error (0)	di7juyclzlgyp.cloudfront.net		13.32.25.43	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.381578922 CEST	8.8.8.8	192.168.2.4	0x79ac	No error (0)	di7juyclzlgyp.cloudfront.net		13.32.25.93	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.381578922 CEST	8.8.8.8	192.168.2.4	0x79ac	No error (0)	di7juyclzlgyp.cloudfront.net		13.32.25.126	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.395881891 CEST	8.8.8.8	192.168.2.4	0xe504	No error (0)	ep00.epimg.net	prisa-us-eu.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.395881891 CEST	8.8.8.8	192.168.2.4	0xe504	No error (0)	prisa-us-eu.map.fastly.net		199.232.194.133	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.395881891 CEST	8.8.8.8	192.168.2.4	0xe504	No error (0)	prisa-us-eu.map.fastly.net		199.232.198.133	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:11:08.420522928 CEST	8.8.8.8	192.168.2.4	0x220a	No error (0)	d3cra5ec8gdi8w.cloudfront.net		13.35.253.104	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.420522928 CEST	8.8.8.8	192.168.2.4	0x220a	No error (0)	d3cra5ec8gdi8w.cloudfront.net		13.35.253.186	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.420522928 CEST	8.8.8.8	192.168.2.4	0x220a	No error (0)	d3cra5ec8gdi8w.cloudfront.net		13.35.253.12	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.420522928 CEST	8.8.8.8	192.168.2.4	0x220a	No error (0)	d3cra5ec8gdi8w.cloudfront.net		13.35.253.176	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.466852903 CEST	8.8.8.8	192.168.2.4	0x78cc	No error (0)	i.blogs.es	d1j70itqjm2icu.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.466852903 CEST	8.8.8.8	192.168.2.4	0x78cc	No error (0)	d1j70itqjm2icu.cloudfront.net		13.32.25.9	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.466852903 CEST	8.8.8.8	192.168.2.4	0x78cc	No error (0)	d1j70itqjm2icu.cloudfront.net		13.32.25.35	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.466852903 CEST	8.8.8.8	192.168.2.4	0x78cc	No error (0)	d1j70itqjm2icu.cloudfront.net		13.32.25.109	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.466852903 CEST	8.8.8.8	192.168.2.4	0x78cc	No error (0)	d1j70itqjm2icu.cloudfront.net		13.32.25.47	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.496784925 CEST	8.8.8.8	192.168.2.4	0x5479	No error (0)	img.huffingtonpost.com	cs491300.wpc.mucdn.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.496784925 CEST	8.8.8.8	192.168.2.4	0x5479	No error (0)	cs491300.wpc.mucdn.net		192.229.220.196	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.511832952 CEST	8.8.8.8	192.168.2.4	0xd4df	No error (0)	as01.epimg.net	prisa-us-eu.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.511832952 CEST	8.8.8.8	192.168.2.4	0xd4df	No error (0)	prisa-us-eu.map.fastly.net		199.232.194.133	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.511832952 CEST	8.8.8.8	192.168.2.4	0xd4df	No error (0)	prisa-us-eu.map.fastly.net		199.232.198.133	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.529650927 CEST	8.8.8.8	192.168.2.4	0xdfd	No error (0)	img2.rtve.es	caching.c251.edge2befaster.io		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.529650927 CEST	8.8.8.8	192.168.2.4	0xdfd	No error (0)	caching.c251.edge2befaster.io	aec01.esg.rtve.edgetcdn.io		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.529650927 CEST	8.8.8.8	192.168.2.4	0xdfd	No error (0)	aec01.esg.rtve.edgetcdn.io		51.195.63.237	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.529650927 CEST	8.8.8.8	192.168.2.4	0xdfd	No error (0)	aec01.esg.rtve.edgetcdn.io		185.103.37.62	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.529650927 CEST	8.8.8.8	192.168.2.4	0xdfd	No error (0)	aec01.esg.rtve.edgetcdn.io		185.103.37.59	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.529650927 CEST	8.8.8.8	192.168.2.4	0xdfd	No error (0)	aec01.esg.rtve.edgetcdn.io		51.195.63.235	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.529650927 CEST	8.8.8.8	192.168.2.4	0xdfd	No error (0)	aec01.esg.rtve.edgetcdn.io		51.89.172.162	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.529650927 CEST	8.8.8.8	192.168.2.4	0xdfd	No error (0)	aec01.esg.rtve.edgetcdn.io		51.210.220.45	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.529650927 CEST	8.8.8.8	192.168.2.4	0xdfd	No error (0)	aec01.esg.rtve.edgetcdn.io		51.89.235.116	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.529650927 CEST	8.8.8.8	192.168.2.4	0xdfd	No error (0)	aec01.esg.rtve.edgetcdn.io		185.103.37.61	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.529650927 CEST	8.8.8.8	192.168.2.4	0xdfd	No error (0)	aec01.esg.rtve.edgetcdn.io		51.210.220.43	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.549181938 CEST	8.8.8.8	192.168.2.4	0x482b	No error (0)	www.puntodebreak.com	puntodebreak.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:11:08.549181938 CEST	8.8.8.8	192.168.2.4	0x482b	No error (0)	puntodebreak.com		185.125.78.79	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.589209080 CEST	8.8.8.8	192.168.2.4	0xbb97	No error (0)	phantom-elmundo.unidadeditorial.es	dbpabf0off7y1.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.589209080 CEST	8.8.8.8	192.168.2.4	0xbb97	No error (0)	dbpabf0off7y1.cloudfront.net		65.9.66.80	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.589209080 CEST	8.8.8.8	192.168.2.4	0xbb97	No error (0)	dbpabf0off7y1.cloudfront.net		65.9.66.65	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.589209080 CEST	8.8.8.8	192.168.2.4	0xbb97	No error (0)	dbpabf0off7y1.cloudfront.net		65.9.66.34	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.589209080 CEST	8.8.8.8	192.168.2.4	0xbb97	No error (0)	dbpabf0off7y1.cloudfront.net		65.9.66.100	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.633658886 CEST	8.8.8.8	192.168.2.4	0xf4d2	No error (0)	s1.eestatic.com	caching.elespanol.edge2befaster.io		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.633658886 CEST	8.8.8.8	192.168.2.4	0xf4d2	No error (0)	caching.elespanol.edge2befaster.io	caching.meta-cluster-03.edge2befaster.io		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.633658886 CEST	8.8.8.8	192.168.2.4	0xf4d2	No error (0)	caching.meta-cluster-03.edge2befaster.io	cec01.eug.edgetcdn.io		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.633658886 CEST	8.8.8.8	192.168.2.4	0xf4d2	No error (0)	cec01.eug.edgetcdn.io		51.68.35.185	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.633658886 CEST	8.8.8.8	192.168.2.4	0xf4d2	No error (0)	cec01.eug.edgetcdn.io		51.255.81.138	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.658555984 CEST	8.8.8.8	192.168.2.4	0x2b18	No error (0)	www.elconfidencialdigital.com		172.67.82.88	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.658555984 CEST	8.8.8.8	192.168.2.4	0x2b18	No error (0)	www.elconfidencialdigital.com		104.25.57.34	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.658555984 CEST	8.8.8.8	192.168.2.4	0x2b18	No error (0)	www.elconfidencialdigital.com		104.25.56.34	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.670881987 CEST	8.8.8.8	192.168.2.4	0x652c	No error (0)	static2.abc.es	static.abc.es		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.670881987 CEST	8.8.8.8	192.168.2.4	0x652c	No error (0)	static.abc.es	static-abc.akamaized.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.703252077 CEST	8.8.8.8	192.168.2.4	0x8788	No error (0)	platform.twitter.com	platform.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.703252077 CEST	8.8.8.8	192.168.2.4	0x8788	No error (0)	platform.twitter.map.fastly.net		199.232.136.157	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.750960112 CEST	8.8.8.8	192.168.2.4	0x7855	No error (0)	www.republica.com.uy	republica.com.uy		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:08.750960112 CEST	8.8.8.8	192.168.2.4	0x7855	No error (0)	republica.com.uy		108.170.35.187	A (IP address)	IN (0x0001)
May 10, 2021 10:11:08.843393087 CEST	8.8.8.8	192.168.2.4	0x1ecf	No error (0)	cdn.jsdelivr.net	dualstack.f3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:09.168488026 CEST	8.8.8.8	192.168.2.4	0xb06	No error (0)	static.hotjar.com	static-cdn.hotjar.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:09.168488026 CEST	8.8.8.8	192.168.2.4	0xb06	No error (0)	static-cdn.hotjar.com		13.32.25.105	A (IP address)	IN (0x0001)
May 10, 2021 10:11:09.168488026 CEST	8.8.8.8	192.168.2.4	0xb06	No error (0)	static-cdn.hotjar.com		13.32.25.20	A (IP address)	IN (0x0001)
May 10, 2021 10:11:09.168488026 CEST	8.8.8.8	192.168.2.4	0xb06	No error (0)	static-cdn.hotjar.com		13.32.25.2	A (IP address)	IN (0x0001)
May 10, 2021 10:11:09.168488026 CEST	8.8.8.8	192.168.2.4	0xb06	No error (0)	static-cdn.hotjar.com		13.32.25.35	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:11:09.314805984 CEST	8.8.8.8	192.168.2.4	0xeac9	No error (0)	proteccion10.net		193.32.242.105	A (IP address)	IN (0x0001)
May 10, 2021 10:11:09.754501104 CEST	8.8.8.8	192.168.2.4	0x9847	No error (0)	googleads.g.doubleclick.net		216.58.214.194	A (IP address)	IN (0x0001)
May 10, 2021 10:11:09.770504951 CEST	8.8.8.8	192.168.2.4	0x38b5	No error (0)	script.hotjar.com		13.32.25.86	A (IP address)	IN (0x0001)
May 10, 2021 10:11:09.770504951 CEST	8.8.8.8	192.168.2.4	0x38b5	No error (0)	script.hotjar.com		13.32.25.118	A (IP address)	IN (0x0001)
May 10, 2021 10:11:09.770504951 CEST	8.8.8.8	192.168.2.4	0x38b5	No error (0)	script.hotjar.com		13.32.25.17	A (IP address)	IN (0x0001)
May 10, 2021 10:11:09.770504951 CEST	8.8.8.8	192.168.2.4	0x38b5	No error (0)	script.hotjar.com		13.32.25.19	A (IP address)	IN (0x0001)
May 10, 2021 10:11:10.325153112 CEST	8.8.8.8	192.168.2.4	0x806a	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:10.325153112 CEST	8.8.8.8	192.168.2.4	0x806a	No error (0)	stats.l.doubleclick.net		74.125.140.155	A (IP address)	IN (0x0001)
May 10, 2021 10:11:10.325153112 CEST	8.8.8.8	192.168.2.4	0x806a	No error (0)	stats.l.doubleclick.net		74.125.140.157	A (IP address)	IN (0x0001)
May 10, 2021 10:11:10.325153112 CEST	8.8.8.8	192.168.2.4	0x806a	No error (0)	stats.l.doubleclick.net		74.125.140.154	A (IP address)	IN (0x0001)
May 10, 2021 10:11:10.325153112 CEST	8.8.8.8	192.168.2.4	0x806a	No error (0)	stats.l.doubleclick.net		74.125.140.156	A (IP address)	IN (0x0001)
May 10, 2021 10:11:10.328874111 CEST	8.8.8.8	192.168.2.4	0x3fe9	No error (0)	www.google.ch		172.217.19.99	A (IP address)	IN (0x0001)
May 10, 2021 10:11:10.362452984 CEST	8.8.8.8	192.168.2.4	0xd6cb	No error (0)	partnerad.l.doubleclick.net		216.58.214.226	A (IP address)	IN (0x0001)
May 10, 2021 10:11:10.389940977 CEST	8.8.8.8	192.168.2.4	0x76fb	No error (0)	adservice.google.ch	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:10.389940977 CEST	8.8.8.8	192.168.2.4	0x76fb	No error (0)	pagead46.l.doubleclick.net		172.217.19.98	A (IP address)	IN (0x0001)
May 10, 2021 10:11:10.457544088 CEST	8.8.8.8	192.168.2.4	0x6cd8	No error (0)	www.googletagservices.com		172.217.19.98	A (IP address)	IN (0x0001)
May 10, 2021 10:11:10.962385893 CEST	8.8.8.8	192.168.2.4	0x2ee0	No error (0)	vars.hotjar.com		99.86.2.91	A (IP address)	IN (0x0001)
May 10, 2021 10:11:10.962385893 CEST	8.8.8.8	192.168.2.4	0x2ee0	No error (0)	vars.hotjar.com		99.86.2.115	A (IP address)	IN (0x0001)
May 10, 2021 10:11:10.962385893 CEST	8.8.8.8	192.168.2.4	0x2ee0	No error (0)	vars.hotjar.com		99.86.2.129	A (IP address)	IN (0x0001)
May 10, 2021 10:11:10.962385893 CEST	8.8.8.8	192.168.2.4	0x2ee0	No error (0)	vars.hotjar.com		99.86.2.113	A (IP address)	IN (0x0001)
May 10, 2021 10:11:12.377706051 CEST	8.8.8.8	192.168.2.4	0x4469	No error (0)	www.google.de		172.217.16.99	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.059505939 CEST	8.8.8.8	192.168.2.4	0x4956	No error (0)	vc.hotjar.io	vc-live-cf.hotjar.io		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:19.059505939 CEST	8.8.8.8	192.168.2.4	0x4956	No error (0)	vc-live-cf.hotjar.io		65.9.66.63	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.059505939 CEST	8.8.8.8	192.168.2.4	0x4956	No error (0)	vc-live-cf.hotjar.io		65.9.66.36	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.059505939 CEST	8.8.8.8	192.168.2.4	0x4956	No error (0)	vc-live-cf.hotjar.io		65.9.66.111	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.059505939 CEST	8.8.8.8	192.168.2.4	0x4956	No error (0)	vc-live-cf.hotjar.io		65.9.66.34	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:11:19.084827900 CEST	8.8.8.8	192.168.2.4	0x7c5d	No error (0)	id.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.154174089 CEST	8.8.8.8	192.168.2.4	0xa87d	No error (0)	odr.mookie1.com	tagr-gcp-odr-euw4.mookie1.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:19.154174089 CEST	8.8.8.8	192.168.2.4	0xa87d	No error (0)	tagr-gcp-odr-euw4.mookie1.com		34.98.67.61	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.171276093 CEST	8.8.8.8	192.168.2.4	0xb1eb	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.171276093 CEST	8.8.8.8	192.168.2.4	0xb1eb	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.174019098 CEST	8.8.8.8	192.168.2.4	0x57a5	No error (0)	image6.pubmatic.com	pugm22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:19.174019098 CEST	8.8.8.8	192.168.2.4	0x57a5	No error (0)	pugm22000nfc.pubmatic.com	pugm22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:19.174019098 CEST	8.8.8.8	192.168.2.4	0x57a5	No error (0)	pugm22000nf.pubmatic.com		185.64.189.115	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.193526030 CEST	8.8.8.8	192.168.2.4	0x977b	No error (0)	cc.adingo.jp		54.178.254.210	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.193526030 CEST	8.8.8.8	192.168.2.4	0x977b	No error (0)	cc.adingo.jp		52.68.53.67	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.193526030 CEST	8.8.8.8	192.168.2.4	0x977b	No error (0)	cc.adingo.jp		35.72.120.200	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.193526030 CEST	8.8.8.8	192.168.2.4	0x977b	No error (0)	cc.adingo.jp		18.180.1.224	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.193526030 CEST	8.8.8.8	192.168.2.4	0x977b	No error (0)	cc.adingo.jp		54.178.184.38	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.193526030 CEST	8.8.8.8	192.168.2.4	0x977b	No error (0)	cc.adingo.jp		54.250.196.226	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.193526030 CEST	8.8.8.8	192.168.2.4	0x977b	No error (0)	cc.adingo.jp		18.179.240.58	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.193526030 CEST	8.8.8.8	192.168.2.4	0x977b	No error (0)	cc.adingo.jp		52.69.69.122	A (IP address)	IN (0x0001)
May 10, 2021 10:11:19.736304998 CEST	8.8.8.8	192.168.2.4	0x1e0d	No error (0)	cm.g.doubleclick.net		216.58.214.226	A (IP address)	IN (0x0001)
May 10, 2021 10:11:21.374099016 CEST	8.8.8.8	192.168.2.4	0xbb70	No error (0)	token.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:22.480029106 CEST	8.8.8.8	192.168.2.4	0x415a	No error (0)	match.adsrvr.org	match-1943069928.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:22.480029106 CEST	8.8.8.8	192.168.2.4	0x415a	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.30.50.112	A (IP address)	IN (0x0001)
May 10, 2021 10:11:22.480029106 CEST	8.8.8.8	192.168.2.4	0x415a	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		34.240.192.98	A (IP address)	IN (0x0001)
May 10, 2021 10:11:22.480029106 CEST	8.8.8.8	192.168.2.4	0x415a	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		34.252.153.38	A (IP address)	IN (0x0001)
May 10, 2021 10:11:22.480029106 CEST	8.8.8.8	192.168.2.4	0x415a	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		63.33.11.43	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:11:22.480029106 CEST	8.8.8.8	192.168.2.4	0x415a	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.49.220.169	A (IP address)	IN (0x0001)
May 10, 2021 10:11:22.480029106 CEST	8.8.8.8	192.168.2.4	0x415a	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.18.54.41	A (IP address)	IN (0x0001)
May 10, 2021 10:11:22.480029106 CEST	8.8.8.8	192.168.2.4	0x415a	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.210.202.173	A (IP address)	IN (0x0001)
May 10, 2021 10:11:22.480029106 CEST	8.8.8.8	192.168.2.4	0x415a	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		54.220.204.72	A (IP address)	IN (0x0001)
May 10, 2021 10:11:22.503618002 CEST	8.8.8.8	192.168.2.4	0x86e2	No error (0)	c1.adform.net	track.adformnet.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:23.054935932 CEST	8.8.8.8	192.168.2.4	0xd1ef	No error (0)	eu-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
May 10, 2021 10:11:23.054935932 CEST	8.8.8.8	192.168.2.4	0xd1ef	No error (0)	eu-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
May 10, 2021 10:11:28.593698025 CEST	8.8.8.8	192.168.2.4	0x13fa	No error (0)	localcoronavirus.com		104.21.18.245	A (IP address)	IN (0x0001)
May 10, 2021 10:11:28.593698025 CEST	8.8.8.8	192.168.2.4	0x13fa	No error (0)	localcoronavirus.com		172.67.183.244	A (IP address)	IN (0x0001)
May 10, 2021 10:11:42.661628008 CEST	8.8.8.8	192.168.2.4	0xbf32	No error (0)	pixel.quantserve.com	px2.px.quantserve.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:42.661628008 CEST	8.8.8.8	192.168.2.4	0xbf32	No error (0)	px2.px.quantserve.com		91.228.74.133	A (IP address)	IN (0x0001)
May 10, 2021 10:11:42.661628008 CEST	8.8.8.8	192.168.2.4	0xbf32	No error (0)	px2.px.quantserve.com		91.228.74.198	A (IP address)	IN (0x0001)
May 10, 2021 10:11:42.661628008 CEST	8.8.8.8	192.168.2.4	0xbf32	No error (0)	px2.px.quantserve.com		91.228.74.189	A (IP address)	IN (0x0001)
May 10, 2021 10:11:42.661628008 CEST	8.8.8.8	192.168.2.4	0xbf32	No error (0)	px2.px.quantserve.com		91.228.74.226	A (IP address)	IN (0x0001)
May 10, 2021 10:11:42.661628008 CEST	8.8.8.8	192.168.2.4	0xbf32	No error (0)	px2.px.quantserve.com		91.228.74.134	A (IP address)	IN (0x0001)
May 10, 2021 10:11:44.491322994 CEST	8.8.8.8	192.168.2.4	0xf580	No error (0)	sync.mathtag.com	pixel-origin.mathtag.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:11:44.491322994 CEST	8.8.8.8	192.168.2.4	0xf580	No error (0)	pixel-origin.mathtag.com		185.29.132.68	A (IP address)	IN (0x0001)
May 10, 2021 10:11:44.491322994 CEST	8.8.8.8	192.168.2.4	0xf580	No error (0)	pixel-origin.mathtag.com		185.29.133.199	A (IP address)	IN (0x0001)
May 10, 2021 10:11:44.491322994 CEST	8.8.8.8	192.168.2.4	0xf580	No error (0)	pixel-origin.mathtag.com		185.29.135.234	A (IP address)	IN (0x0001)
May 10, 2021 10:11:44.491322994 CEST	8.8.8.8	192.168.2.4	0xf580	No error (0)	pixel-origin.mathtag.com		185.29.133.58	A (IP address)	IN (0x0001)
May 10, 2021 10:11:45.265201092 CEST	8.8.8.8	192.168.2.4	0xcbce	No error (0)	match.prod.bidr.io		52.209.246.140	A (IP address)	IN (0x0001)
May 10, 2021 10:11:45.265201092 CEST	8.8.8.8	192.168.2.4	0xcbce	No error (0)	match.prod.bidr.io		52.215.139.246	A (IP address)	IN (0x0001)
May 10, 2021 10:11:45.265201092 CEST	8.8.8.8	192.168.2.4	0xcbce	No error (0)	match.prod.bidr.io		52.48.151.83	A (IP address)	IN (0x0001)
May 10, 2021 10:11:45.265201092 CEST	8.8.8.8	192.168.2.4	0xcbce	No error (0)	match.prod.bidr.io		52.19.106.86	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:11:45.265201092 CEST	8.8.8.8	192.168.2.4	0xcbce	No error (0)	match.prod.bidr.io		52.49.40.147	A (IP address)	IN (0x0001)
May 10, 2021 10:11:45.265201092 CEST	8.8.8.8	192.168.2.4	0xcbce	No error (0)	match.prod.bidr.io		52.210.44.111	A (IP address)	IN (0x0001)
May 10, 2021 10:11:47.111886978 CEST	8.8.8.8	192.168.2.4	0x219d	No error (0)	facebook.com		31.13.92.36	A (IP address)	IN (0x0001)
May 10, 2021 10:12:24.931936979 CEST	8.8.8.8	192.168.2.4	0xe06d	No error (0)	x.bidswitch.net	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:12:24.931936979 CEST	8.8.8.8	192.168.2.4	0xe06d	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		18.195.54.133	A (IP address)	IN (0x0001)
May 10, 2021 10:12:24.931936979 CEST	8.8.8.8	192.168.2.4	0xe06d	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		52.58.102.227	A (IP address)	IN (0x0001)
May 10, 2021 10:12:24.931936979 CEST	8.8.8.8	192.168.2.4	0xe06d	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		3.120.242.149	A (IP address)	IN (0x0001)
May 10, 2021 10:12:24.931936979 CEST	8.8.8.8	192.168.2.4	0xe06d	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		52.57.230.211	A (IP address)	IN (0x0001)
May 10, 2021 10:12:24.931936979 CEST	8.8.8.8	192.168.2.4	0xe06d	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		35.156.223.207	A (IP address)	IN (0x0001)
May 10, 2021 10:12:24.931936979 CEST	8.8.8.8	192.168.2.4	0xe06d	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		52.59.81.87	A (IP address)	IN (0x0001)
May 10, 2021 10:12:24.931936979 CEST	8.8.8.8	192.168.2.4	0xe06d	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		18.195.177.11	A (IP address)	IN (0x0001)
May 10, 2021 10:12:24.931936979 CEST	8.8.8.8	192.168.2.4	0xe06d	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		52.58.182.33	A (IP address)	IN (0x0001)
May 10, 2021 10:12:26.745511055 CEST	8.8.8.8	192.168.2.4	0xe952	No error (0)	pool.admedo.com	pool-com.adizio.iponweb.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:12:26.745511055 CEST	8.8.8.8	192.168.2.4	0xe952	No error (0)	pool-com.adizio.iponweb.net	adizio.geo.iponweb.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:12:26.745511055 CEST	8.8.8.8	192.168.2.4	0xe952	No error (0)	adizio.geo.iponweb.net		35.210.53.219	A (IP address)	IN (0x0001)
May 10, 2021 10:12:30.262245893 CEST	8.8.8.8	192.168.2.4	0x2cf7	No error (0)	pm.w55c.net	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:12:30.262245893 CEST	8.8.8.8	192.168.2.4	0x2cf7	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.125.99.7	A (IP address)	IN (0x0001)
May 10, 2021 10:12:30.262245893 CEST	8.8.8.8	192.168.2.4	0x2cf7	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.127.92.82	A (IP address)	IN (0x0001)
May 10, 2021 10:12:30.262245893 CEST	8.8.8.8	192.168.2.4	0x2cf7	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		18.185.192.106	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:12:30.262245893 CEST	8.8.8.8	192.168.2.4	0x2cf7	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.127.88.255	A (IP address)	IN (0x0001)
May 10, 2021 10:12:30.262245893 CEST	8.8.8.8	192.168.2.4	0x2cf7	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		35.157.48.14	A (IP address)	IN (0x0001)
May 10, 2021 10:12:30.262245893 CEST	8.8.8.8	192.168.2.4	0x2cf7	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		18.159.187.109	A (IP address)	IN (0x0001)
May 10, 2021 10:12:30.262245893 CEST	8.8.8.8	192.168.2.4	0x2cf7	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		18.197.133.56	A (IP address)	IN (0x0001)
May 10, 2021 10:12:30.262245893 CEST	8.8.8.8	192.168.2.4	0x2cf7	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		18.159.182.76	A (IP address)	IN (0x0001)
May 10, 2021 10:12:31.263120890 CEST	8.8.8.8	192.168.2.4	0xa58d	No error (0)	pr-bh.ybp.yahoo.com	ds-pr-bh.ybp.gysm.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:12:31.263120890 CEST	8.8.8.8	192.168.2.4	0xa58d	No error (0)	ds-pr-bh.ybp.gysm.yahoodns.net		212.82.100.176	A (IP address)	IN (0x0001)
May 10, 2021 10:12:31.963289022 CEST	8.8.8.8	192.168.2.4	0xdd20	No error (0)	r6---sn-n02xgoxufvg3-2gbs.googlevideo.com	r6.sn-n02xgoxufvg3-2gbs.googlevideo.com		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:12:31.963289022 CEST	8.8.8.8	192.168.2.4	0xdd20	No error (0)	r6.sn-n02xgoxufvg3-2gbs.googlevideo.com		95.168.222.145	A (IP address)	IN (0x0001)
May 10, 2021 10:12:41.185616016 CEST	8.8.8.8	192.168.2.4	0x2401	No error (0)	img.europapress.es	d2dzdx91mh5kpx.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:12:41.185616016 CEST	8.8.8.8	192.168.2.4	0x2401	No error (0)	d2dzdx91mh5kpx.cloudfront.net		65.9.66.66	A (IP address)	IN (0x0001)
May 10, 2021 10:12:41.185616016 CEST	8.8.8.8	192.168.2.4	0x2401	No error (0)	d2dzdx91mh5kpx.cloudfront.net		65.9.66.100	A (IP address)	IN (0x0001)
May 10, 2021 10:12:41.185616016 CEST	8.8.8.8	192.168.2.4	0x2401	No error (0)	d2dzdx91mh5kpx.cloudfront.net		65.9.66.35	A (IP address)	IN (0x0001)
May 10, 2021 10:12:41.185616016 CEST	8.8.8.8	192.168.2.4	0x2401	No error (0)	d2dzdx91mh5kpx.cloudfront.net		65.9.66.113	A (IP address)	IN (0x0001)
May 10, 2021 10:12:41.307003975 CEST	8.8.8.8	192.168.2.4	0xb0c8	No error (0)	ficheracos.publico.es	www.publico.es.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:12:52.727296114 CEST	8.8.8.8	192.168.2.4	0xe382	No error (0)	dsp.active-agent.com		85.114.159.66	A (IP address)	IN (0x0001)
May 10, 2021 10:12:52.739433050 CEST	8.8.8.8	192.168.2.4	0x7bce	No error (0)	dsp.adfarm1.adition.com		85.114.159.93	A (IP address)	IN (0x0001)
May 10, 2021 10:12:52.739433050 CEST	8.8.8.8	192.168.2.4	0x7bce	No error (0)	dsp.adfarm1.adition.com		85.114.159.118	A (IP address)	IN (0x0001)
May 10, 2021 10:12:53.097819090 CEST	8.8.8.8	192.168.2.4	0x6d2e	No error (0)	dspcluster.adfarm1.adition.com		85.114.159.67	A (IP address)	IN (0x0001)
May 10, 2021 10:12:53.432614088 CEST	8.8.8.8	192.168.2.4	0x5d	No error (0)	ad.ad-srv.net		46.4.10.47	A (IP address)	IN (0x0001)
May 10, 2021 10:12:53.432614088 CEST	8.8.8.8	192.168.2.4	0x5d	No error (0)	ad.ad-srv.net		138.201.63.149	A (IP address)	IN (0x0001)
May 10, 2021 10:12:53.432614088 CEST	8.8.8.8	192.168.2.4	0x5d	No error (0)	ad.ad-srv.net		138.201.84.244	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:12:53.432614088 CEST	8.8.8.8	192.168.2.4	0x5d	No error (0)	ad.ad-srv.net		138.201.63.117	A (IP address)	IN (0x0001)
May 10, 2021 10:12:53.432614088 CEST	8.8.8.8	192.168.2.4	0x5d	No error (0)	ad.ad-srv.net		138.201.84.245	A (IP address)	IN (0x0001)
May 10, 2021 10:12:53.432614088 CEST	8.8.8.8	192.168.2.4	0x5d	No error (0)	ad.ad-srv.net		138.201.135.164	A (IP address)	IN (0x0001)
May 10, 2021 10:12:53.432614088 CEST	8.8.8.8	192.168.2.4	0x5d	No error (0)	ad.ad-srv.net		46.4.10.49	A (IP address)	IN (0x0001)
May 10, 2021 10:12:53.432614088 CEST	8.8.8.8	192.168.2.4	0x5d	No error (0)	ad.ad-srv.net		138.201.63.157	A (IP address)	IN (0x0001)
May 10, 2021 10:12:53.432614088 CEST	8.8.8.8	192.168.2.4	0x5d	No error (0)	ad.ad-srv.net		78.46.111.106	A (IP address)	IN (0x0001)
May 10, 2021 10:12:53.432614088 CEST	8.8.8.8	192.168.2.4	0x5d	No error (0)	ad.ad-srv.net		138.201.63.165	A (IP address)	IN (0x0001)
May 10, 2021 10:12:53.432614088 CEST	8.8.8.8	192.168.2.4	0x5d	No error (0)	ad.ad-srv.net		176.9.26.250	A (IP address)	IN (0x0001)
May 10, 2021 10:12:53.432614088 CEST	8.8.8.8	192.168.2.4	0x5d	No error (0)	ad.ad-srv.net		78.46.90.238	A (IP address)	IN (0x0001)
May 10, 2021 10:12:53.432614088 CEST	8.8.8.8	192.168.2.4	0x5d	No error (0)	ad.ad-srv.net		138.201.64.38	A (IP address)	IN (0x0001)
May 10, 2021 10:12:53.432614088 CEST	8.8.8.8	192.168.2.4	0x5d	No error (0)	ad.ad-srv.net		88.99.219.174	A (IP address)	IN (0x0001)
May 10, 2021 10:12:53.432614088 CEST	8.8.8.8	192.168.2.4	0x5d	No error (0)	ad.ad-srv.net		138.201.84.253	A (IP address)	IN (0x0001)
May 10, 2021 10:12:57.081319094 CEST	8.8.8.8	192.168.2.4	0x74b3	No error (0)	ad14.ad-srv.net		176.9.26.250	A (IP address)	IN (0x0001)
May 10, 2021 10:12:58.901453018 CEST	8.8.8.8	192.168.2.4	0x1428	No error (0)	rtb.openx.net		35.186.253.211	A (IP address)	IN (0x0001)
May 10, 2021 10:12:58.901453018 CEST	8.8.8.8	192.168.2.4	0x1428	No error (0)	rtb.openx.net		35.227.252.103	A (IP address)	IN (0x0001)
May 10, 2021 10:12:59.089896917 CEST	8.8.8.8	192.168.2.4	0x5689	No error (0)	www.awin1.com	www.awin1.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 10, 2021 10:12:59.118630886 CEST	8.8.8.8	192.168.2.4	0x55fb	No error (0)	cdn.contentspread.net		85.114.131.233	A (IP address)	IN (0x0001)
May 10, 2021 10:12:59.118630886 CEST	8.8.8.8	192.168.2.4	0x55fb	No error (0)	cdn.contentspread.net		88.99.65.215	A (IP address)	IN (0x0001)
May 10, 2021 10:12:59.118630886 CEST	8.8.8.8	192.168.2.4	0x55fb	No error (0)	cdn.contentspread.net		188.138.57.20	A (IP address)	IN (0x0001)
May 10, 2021 10:12:59.118630886 CEST	8.8.8.8	192.168.2.4	0x55fb	No error (0)	cdn.contentspread.net		62.138.14.19	A (IP address)	IN (0x0001)
May 10, 2021 10:12:59.118630886 CEST	8.8.8.8	192.168.2.4	0x55fb	No error (0)	cdn.contentspread.net		88.99.70.21	A (IP address)	IN (0x0001)
May 10, 2021 10:12:59.118630886 CEST	8.8.8.8	192.168.2.4	0x55fb	No error (0)	cdn.contentspread.net		85.114.131.234	A (IP address)	IN (0x0001)
May 10, 2021 10:12:59.118630886 CEST	8.8.8.8	192.168.2.4	0x55fb	No error (0)	cdn.contentspread.net		188.138.33.34	A (IP address)	IN (0x0001)
May 10, 2021 10:12:59.118630886 CEST	8.8.8.8	192.168.2.4	0x55fb	No error (0)	cdn.contentspread.net		88.99.69.161	A (IP address)	IN (0x0001)
May 10, 2021 10:12:59.118630886 CEST	8.8.8.8	192.168.2.4	0x55fb	No error (0)	cdn.contentspread.net		85.114.131.235	A (IP address)	IN (0x0001)
May 10, 2021 10:12:59.399159908 CEST	8.8.8.8	192.168.2.4	0x65f8	No error (0)	media.kaspersky.com	multisite-support.geo.kaspersky.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2021 10:12:59.399159908 CEST	8.8.8.8	192.168.2.4	0x65f8	No error (0)	multisite-support.geo.kaspersky.com		185.85.15.23	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- localcoronavirus.com
- www.puntodebreak.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49734	172.67.183.244	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 10, 2021 10:11:05.800451994 CEST	2351	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: localcoronavirus.com Connection: Keep-Alive
May 10, 2021 10:11:05.853977919 CEST	2352	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 10 May 2021 08:11:05 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Mon, 10 May 2021 09:11:05 GMT Location: https://localcoronavirus.com/ cf-request-id: 09f6ed80e600004a685086e000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=KNJDmP5Mv1KYq6DqMAb4bQScfg5kPkrbz%2FKYFsYHz793NlvtiHl9yhlC3mzW9xUwO6wHlYXHt1VlYaT0eq1w1I1gqziu5QP7yb4sqvJecZUYN%2B4Www%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Vary: Accept-Encoding Server: cloudflare CF-RAY: 64d1b1e16d5d4a68-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49786	185.125.78.79	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 10, 2021 10:11:09.207783937 CEST	6403	OUT	GET /files/alexander-zverev-conclusiones-mutua-madrid-open-2021.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.puntodebreak.com

Timestamp	kBytes transferred	Direction	Data
May 10, 2021 10:11:09.275537968 CEST	6426	IN	HTTP/1.1 200 OK Connection: Keep-Alive Cache-Control: public, max-age=604800 Expires: Mon, 17 May 2021 08:11:09 GMT Content-Type: image/png Last-Modified: Sun, 09 May 2021 08:35:54 GMT Accept-Ranges: bytes Content-Length: 261128 Date: Mon, 10 May 2021 08:11:09 GMT Server: LiteSpeed Access-Control-Allow-Origin: * Access-Control-Allow-Headers: origin, x-requested-with, content-type Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 c1 00 00 01 1a 08 02 00 00 00 e6 20 7b 53 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 0e c3 00 00 0e c3 01 c7 6f a8 64 00 00 ff a5 49 44 41 54 78 5e ec fd 87 97 24 cb 75 de 8b 62 91 38 e3 7a da 7b ef bd f7 de 7b 6f a6 bb a7 a7 bd 77 e5 bd f7 ae bd ef 1e ef e7 f8 03 ef 41 18 92 20 29 01 24 45 8a 94 44 91 a2 ae a4 ab cb 27 dd f7 96 de ba ef 3f 78 df 8e a8 ee e9 39 e7 00 04 49 00 3c a0 b0 d7 37 39 91 51 59 59 d9 55 59 bf fa 76 44 64 e4 e7 7e eb 9f 29 7e fb b7 7f fb a2 f0 b1 f2 c7 e2 f2 43 97 cb ff 52 e3 f3 9f ff bc b7 c4 02 ab 17 35 ac f4 e6 a3 4c 17 c1 b6 a5 f8 d8 ea 95 ab 57 6e dc f4 09 0c 0a 89 8c 8e 4d 48 49 cf ca 2b 2a 2a ab aa 6e 68 6e e9 ec ed bb 35 36 3a 31 3f b9 20 58 58 97 af ca b4 22 b5 49 66 b0 ab ac 6e 85 d5 2d b7 ba 45 46 c7 9a d6 b2 a4 34 cc 08 95 63 cb e2 c1 e9 95 ce d1 99 86 be db 65 6d fd b9 b5 2d 69 25 55 71 59 05 91 89 69 81 91 d1 d8 fb 35 9f 9b 57 11 6f 5d 79 8b 85 f7 b5 59 f0 e3 b9 1c 1f ab ff 19 db 7c 6a 78 b7 78 73 9b 4f d6 fc 8c e0 5b f2 a7 20 3e 56 e6 f1 b1 f2 a7 c6 27 1f e2 db ff 42 e2 f2 0e 7f f6 9e f9 96 08 ef fa 2f 33 ae 5c b9 72 ed da b5 9b 37 6f 06 07 07 47 47 47 a7 a4 a4 e4 e4 e6 96 55 54 34 34 36 77 76 f7 de 1a 9b 98 5c 58 5a 10 8a d7 95 6a 89 ce a0 34 5b 75 0e a7 c1 ed 31 7a 36 8d 9e 1d 13 69 d3 e8 de d0 bb 3c 5a 87 4b 65 b5 4b 0d 16 a1 c6 24 50 eb d6 94 9a 35 a5 1a c b 15 b9 7a 49 aa 5c 94 28 a0 65 89 72 45 aa 5a 66 ab 73 12 d9 bc 44 b6 20 95 2d ca e4 10 15 c4 d2 45 89 6c 49 2a 5f 91 2b 21 14 e6 65 b4 c1 92 8c 6a 96 65 d8 03 6d b3 24 91 2d 63 1b 99 02 1b 2c 88 a5 0b 62 2c e5 6c ff b4 3a 2f 16 cf 8b 25 f 3 12 da 15 b4 20 91 cd 8a c4 73 62 f1 82 44 b2 28 95 2e 4a 65 d8 66 56 28 86 e6 44 e2 05 91 64 01 4b 81 68 6e 4d 38 b7 2e 9c 17 8a 7f 15 0c f5 7e b6 8c 80 de d2 af 43 f0 d3 c5 bb 72 e9 d4 f4 ae ff 94 f8 e4 36 bc 06 ec 7b 23 50 7f 69 9f 97 e3 63 f4 41 5c d4 30 34 bd f1 30 ca a4 bf 2f 70 c6 fb f8 fa 86 84 86 c7 c4 25 a6 64 64 e7 15 96 95 55 d6 d5 35 b7 b5 f7 0c f4 0f df 19 9d 5c 98 5a 14 2c 08 bc 0c 95 1b 89 a1 4a eb 86 c2 ba 21 31 b9 04 3a 2b 31 54 ac 1a 5b 96 0c ce ac 76 dd 9e 6d 1a b8 53 d9 31 58 50 df 96 59 56 93 9c 5b 1c 9b 9e 19 16 97 10 10 16 e6 e3 ef 7f dd e7 c6 75 bc 18 0b e2 e9 d5 ab f8 be 21 70 0c de 23 66 f1 fa 6d 39 7f af 2e 97 2f 82 57 fe b4 f8 79 b6 f9 69 71 f1 dc 8b c2 a7 c6 e5 87 2e ca ec 19 af e3 53 6b fe e9 e1 dd 17 8b 8b 1a 5e f8 69 71 79 e3 5f 6a 7c 92 a1 b9 60 68 39 31 b4 ab a7 7f 78 6c 62 7a 61 79 51 20 5e 57 a8 a4 3a 83 ca 62 7b 83 a1 ee 6d a3 7b 13 18 05 43 35 76 a7 c2 6c 93 e8 cd 42 8d 71 5d a5 65 00 25 ad 2a d4 cb 32 15 30 8a e5 8a 4c bd 2a 53 2f 4b 55 1c 79 1f 23 26 00 87 25 58 b9 4a cf 52 a1 72 51 2a e7 00 05 c1 21 70 13 f4 e4 00 bd a0 2a 67 28 db 3f c3 2e 61 51 02 d4 2e 4b e4 a0 ed a2 48 Data Ascii: PNGIHDR {SsRGBgAMAapHYsodIDATx^$ub8z{{owA)$ED'?x9I<79QYYUYvDd~)~CR5LWnMHI+**nhn56:1?XX"Ifn-EF4cem-i%UqYi5Wo]yY|jxxsO[>V'B/3\r7oGGGUT446wv\XZj4[u1z6i<ZKeK$P5zI\(erEZfsD -EII*_+!ejem$-c,b,I:/%sbD(.JefV(DdKhnM8.~Cr6{#PicA\040/p%ddU5\Z,J!1:+1T[vmS1XPYV[u!p#fm9./Wyiq.Sk^iqy_j|`h91xlbzayQ ^W:b{m{C5vlBq]e%*20L*S/KUy#&%XJRrQ*!p*g(?.aQ.KH

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:11:05.959687948 CEST	172.67.183.244	443	192.168.2.4	49735	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	Tue Oct 26 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
						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		
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US					
May 10, 2021 10:11:07.659926891 CEST	65.9.66.100	443	192.168.2.4	49744	CN=*.unidadeditorial.es CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Jun 19 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jul 19 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 10, 2021 10:11:07.660763979 CEST	65.9.66.100	443	192.168.2.4	49745	CN=*.unidadeditorial.es CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Jun 19 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jul 19 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 10, 2021 10:11:07.827109098 CEST	99.86.2.109	443	192.168.2.4	49746	CN=excelsior.com.mx CN=excelsior.com.mx CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Apr 24 15:00:02 CEST 2021 Sat Apr 24 15:00:02 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jul 23 15:00:02 CEST 2021 Fri Jul 23 15:00:02 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=excelsior.com.mx	CN=R3, O=Let's Encrypt, C=US	Sat Apr 24 15:00:02 CEST 2021	Fri Jul 23 15:00:02 CEST 2021		
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:11:07.929847956 CEST	99.86.2.109	443	192.168.2.4	49747	CN=excelsior.com.mx CN=excelsior.com.mx CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Apr 24 15:00:02 CEST 2021 Sat Apr 24 15:00:02 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jul 23 15:00:02 CEST 2021 Fri Jul 23 15:00:02 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=excelsior.com.mx	CN=R3, O=Let's Encrypt, C=US	Sat Apr 24 15:00:02 CEST 2021	Fri Jul 23 15:00:02 CEST 2021		
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 10, 2021 10:11:08.358701944 CEST	52.211.67.210	443	192.168.2.4	49750	CN=*.lavozdegalicia.es, OU=PremiumSSL Legacy Wildcard, O=LA VOZ DE GALICIA S.A., STREET="RONDA DE OUTEIRO, 1 - 3 BAJO", L=A CORUNA, ST=La Corua, OID.2.5.4.17=15006, C=ES CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Thu Oct 17 02:00:00 CEST 2019 Fri Nov 02 01:00:00 CET 2018	Tue Jan 18 01:00:00 CET 2022 Wed Jan 01 00:59:59 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
May 10, 2021 10:11:08.369658947 CEST	52.211.67.210	443	192.168.2.4	49751	CN=*.lavozdegalicia.es, OU=PremiumSSL Legacy Wildcard, O=LA VOZ DE GALICIA S.A., STREET="RONDA DE OUTEIRO, 1 - 3 BAJO", L=A CORUNA, ST=La Corua, OID.2.5.4.17=15006, C=ES CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Thu Oct 17 02:00:00 CEST 2019 Fri Nov 02 01:00:00 CET 2018	Tue Jan 18 01:00:00 CET 2022 Wed Jan 01 00:59:59 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
May 10, 2021 10:11:08.414133072 CEST	31.13.92.14	443	192.168.2.4	49755	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:11:08.420509100 CEST	31.13.92.14	443	192.168.2.4	49754	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 10, 2021 10:11:08.431910992 CEST	51.68.35.185	443	192.168.2.4	49753	CN=cronicaglobal.elespanol.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Mar 28 11:00:43 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Sat Jun 26 11:00:43 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 10, 2021 10:11:08.432492018 CEST	51.68.35.185	443	192.168.2.4	49752	CN=cronicaglobal.elespanol.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Mar 28 11:00:43 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Sat Jun 26 11:00:43 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 10, 2021 10:11:08.470937014 CEST	13.32.25.102	443	192.168.2.4	49756	CN=*.20minutos.es CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Apr 05 02:00:00 CEST 2021 Mon Nov 06 13:23:52 CET 2017	Mon Apr 25 01:59:59 CEST 2022 Sat Nov 06 13:23:52 CET 2027	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:52 CET 2017	Sat Nov 06 13:23:52 CET 2027		
May 10, 2021 10:11:08.471843958 CEST	13.32.25.102	443	192.168.2.4	49757	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:11:08.488728046 CEST	199.232.194.133	443	192.168.2.4	49758	CN=*.epimg.net CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon May 03 13:44:46 CEST 2021	Sun Aug 01 13:44:46 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 10, 2021 10:11:08.490027905 CEST	199.232.194.133	443	192.168.2.4	49759	CN=*.epimg.net CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon May 03 13:44:46 CEST 2021	Sun Aug 01 13:44:46 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 10, 2021 10:11:08.532871008 CEST	13.35.253.104	443	192.168.2.4	49761	CN=*.cloudfront.net CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Feb 22 01:00:00 CET 2021	Tue Feb 22 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
							Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
							Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
					CN=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
May 10, 2021 10:11:08.534128904 CEST	13.35.253.104	443	192.168.2.4	49760	CN=*.cloudfront.net CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Feb 22 01:00:00 CET 2021	Tue Feb 22 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
							Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
							Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
					CN=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
May 10, 2021 10:11:08.590262890 CEST	192.229.220.196	443	192.168.2.4	49762	CN=img.huffingtonpost.com, O="Verizon Digital Media Services, Inc.", L=Los Angeles, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon May 04 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Wed Jun 08 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 10, 2021 10:11:08.599950075 CEST	192.229.220.196	443	192.168.2.4	49763	CN=img.huffingtonpost.com, O="Verizon Digital Media Services, Inc.", L=Los Angeles, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon May 04 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Wed Jun 08 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 10, 2021 10:11:08.602276087 CEST	13.32.25.9	443	192.168.2.4	49764	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 10, 2021 10:11:08.602385044 CEST	13.32.25.9	443	192.168.2.4	49765	CN=*.blogs.es CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Feb 05 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Mar 07 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 10, 2021 10:11:08.615134001 CEST	199.232.194.133	443	192.168.2.4	49767	CN=*.epimg.net CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon May 03 13:44:46 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Sun Aug 01 13:44:46 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 10, 2021 10:11:08.615906000 CEST	199.232.194.133	443	192.168.2.4	49766	CN=*.epimg.net CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon May 03 13:44:46 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Sun Aug 01 13:44:46 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:11:08.620538950 CEST	51.195.63.237	443	192.168.2.4	49768	CN=*.rtve.es, O=Corporacion de Radio y Television Espanola SA SME, OU=Digital, L=Madrid, ST=Madrid, C=ES CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Thu Feb 20 15:36:50 CET 2020 Wed Nov 21 01:00:00 CET 2018	Sun Apr 17 10:58:42 CEST 2022 Tue Nov 21 01:00:00 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
						CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
May 10, 2021 10:11:08.621421099 CEST	51.195.63.237	443	192.168.2.4	49769	CN=*.rtve.es, O=Corporacion de Radio y Television Espanola SA SME, OU=Digital, L=Madrid, ST=Madrid, C=ES CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Thu Feb 20 15:36:50 CET 2020 Wed Nov 21 01:00:00 CET 2018	Sun Apr 17 10:58:42 CEST 2022 Tue Nov 21 01:00:00 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
						CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
May 10, 2021 10:11:08.722399950 CEST	185.125.78.79	443	192.168.2.4	49771	CN=puntodebreak.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun May 02 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Aug 01 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 10, 2021 10:11:08.769563913 CEST	185.125.78.79	443	192.168.2.4	49770	CN=puntodebreak.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun May 02 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Aug 01 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:11:08.778326035 CEST	65.9.66.80	443	192.168.2.4	49772	CN=*.unidadeditorial.es CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Jun 19 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jul 19 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 10, 2021 10:11:08.780289888 CEST	65.9.66.80	443	192.168.2.4	49773	CN=*.unidadeditorial.es CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Jun 19 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jul 19 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:11:08.793231964 CEST	172.67.82.88	443	192.168.2.4	49774	CN=elconfidencialdigital.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 30 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Jul 30 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
May 10, 2021 10:11:08.800103903 CEST	172.67.82.88	443	192.168.2.4	49775	CN=elconfidencialdigital.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 30 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Jul 30 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
May 10, 2021 10:11:08.843977928 CEST	51.68.35.185	443	192.168.2.4	49779	CN=*.elespanol.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Nov 18 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Sun Dec 19 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 10, 2021 10:11:08.849025965 CEST	199.232.136.157	443	192.168.2.4	49780	CN=platform.twitter.com, OU=Twitter Security, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 13 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 18 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:11:08.852350950 CEST	199.232.136.157	443	192.168.2.4	49781	CN=platform.twitter.com, OU=Twitter Security, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 13 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 18 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 10, 2021 10:11:08.866602898 CEST	51.68.35.185	443	192.168.2.4	49778	CN=*.elespanol.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Nov 18 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Sun Dec 19 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 10, 2021 10:11:09.209976912 CEST	108.170.35.187	443	192.168.2.4	49783	CN=republica.com.uy CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Mar 29 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Jun 28 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

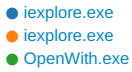
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 10, 2021 10:11:09.211082935 CEST	108.170.35.187	443	192.168.2.4	49782	CN=republica.com.uy CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Mar 29 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Jun 28 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 10, 2021 10:11:09.264686108 CEST	13.32.25.105	443	192.168.2.4	49787	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 10, 2021 10:11:09.270106077 CEST	13.32.25.105	443	192.168.2.4	49788	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 10, 2021 10:11:09.594213963 CEST	193.32.242.105	443	192.168.2.4	49796	CN=proteccion10.net CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Mar 24 02:05:17 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 22 03:05:17 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 10, 2021 10:11:09.596097946 CEST	193.32.242.105	443	192.168.2.4	49795	CN=proteccion10.net CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Mar 24 02:05:17 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 22 03:05:17 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 10, 2021 10:11:09.860039949 CEST	13.32.25.86	443	192.168.2.4	49799	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		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5964 Parent PID: 800

General

Start time:	10:11:03
Start date:	10/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff62b360000
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: 5132 Parent PID: 5964

General

Start time:	10:11:04
Start date:	10/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5964 CREDAT:17410 /prefetch:2
Imagebase:	0x1070000
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: 5748 Parent PID: 800

General

Start time:	10:12:07
Start date:	10/05/2021
Path:	C:\Windows\System32\OpenWith.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\OpenWith.exe -Embedding
Imagebase:	0x7ff791d00000
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