

ID: 403971
Cookbook: browseurl.jbs
Time: 15:35:37
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report http://localcoronavirus.com 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 10
Contacted IPs 13
Public 13
Private 14
General Information 14
Simulations 16
Behavior and APIs 17
Joe Sandbox View / Context 17
IPs 17
Domains 17
ASN 17
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 17
Static File Info 51
No static file info 51
Network Behavior 51
Network Port Distribution 51
TCP Packets 52
UDP Packets 53
DNS Queries 57
DNS Answers 58
HTTP Request Dependency Graph 65
HTTP Packets 65
HTTPS Packets 66
Code Manipulations 85
Statistics 85
Behavior 85
System Behavior 85
Analysis Process: iexplore.exe PID: 2960 Parent PID: 792 85
General 85

Copyright Joe Security LLC 2021

File Activities 86
Registry Activities 86
Analysis Process: iexplore.exe PID: 5880 Parent PID: 2960 86
General 86
File Activities 86
Registry Activities 86
Analysis Process: OpenWith.exe PID: 4880 Parent PID: 792 86
General 86
Disassembly 87
Code Analysis 87

Copyright Joe Security LLC 2021

Analysis Report http://localcoronavirus.com

Overview

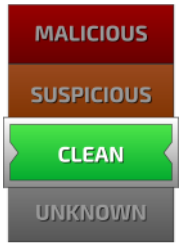
General Information

Sample URL:	http://localcoronavirus.com
Analysis ID:	403971
Infos:	

Most interesting Screenshot:



Detection

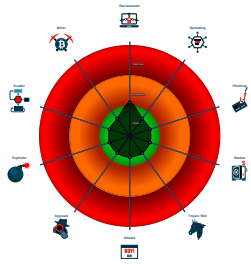


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 2960 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5880 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2960 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- OpenWith.exe (PID: 4880 cmdline: C:\Windows\system32\OpenWith.exe -Embedding MD5: D179D03728E95E040A889F760C1FC402)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

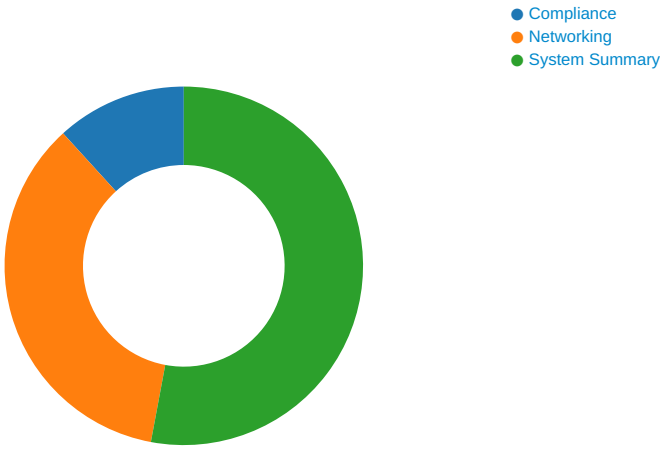
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



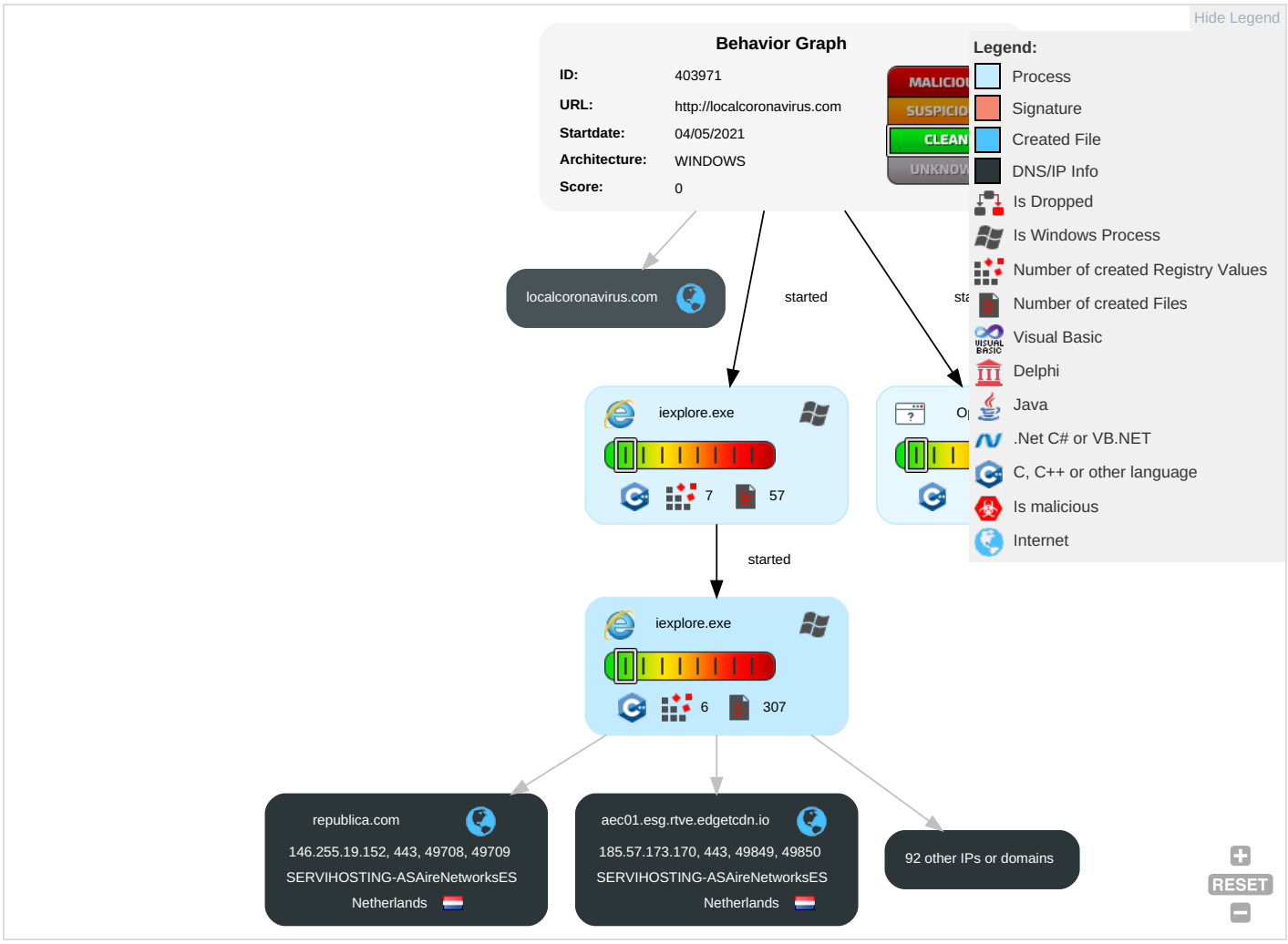
Click to jump to signature section

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

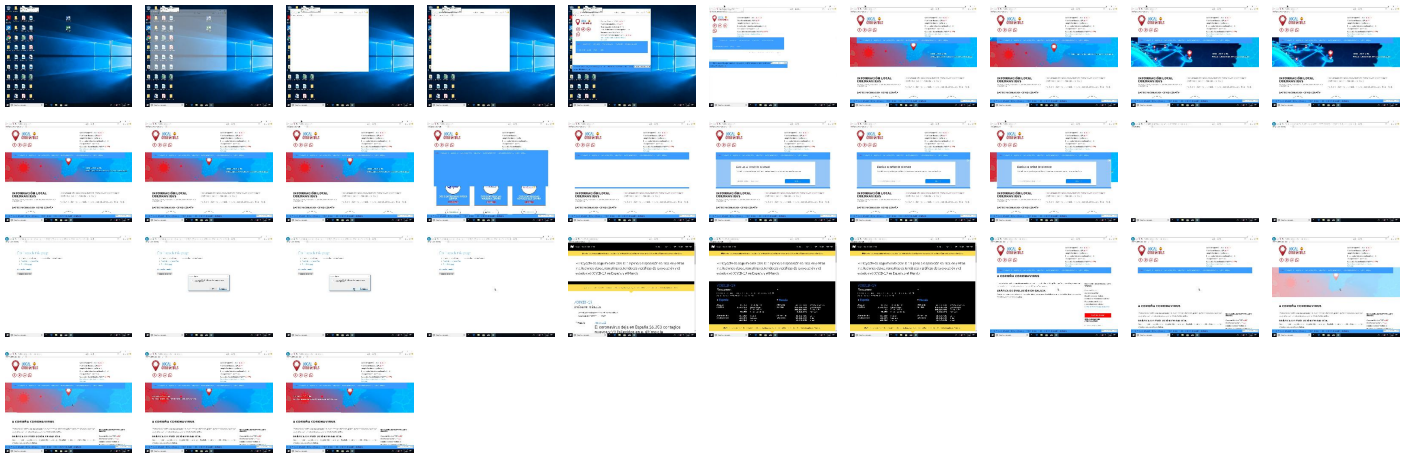
Behavior Graph

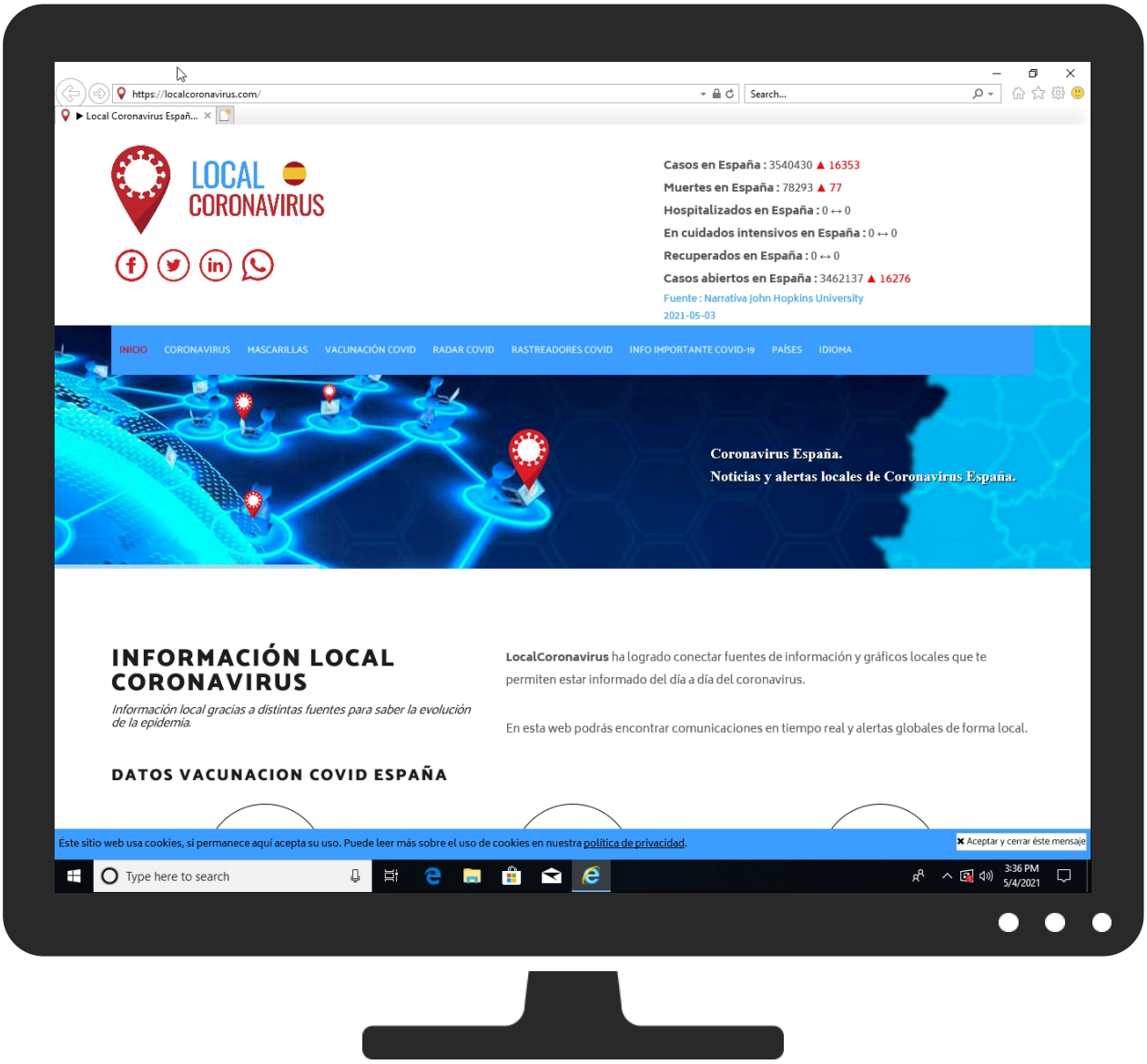


Screenshots

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	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://www.hotjarconsent.com/sv.html	0%	URL Reputation	safe	
http://https://help.narrativa.com/	0%	Avira URL Cloud	safe	
http://https://fontawesome.comhttps://fontawesome.comFont	0%	Avira URL Cloud	safe	
http://https://covid19tracking.narrativa.com/vProyecto	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http:// https://www.mscbs.gob.es/profesionales/saludPublica/ccayes/alertasActual/nCov/vacunaCovid19.htm	0%	Avira URL Cloud	safe	
http://https://covid19tracking.narrativa.com/img/infobae.png	0%	Avira URL Cloud	safe	
http://https://www.facebus.com/a-coruna-coronavirusRoot	0%	Avira URL Cloud	safe	
http://https://www.nwc10.com/politica-privacidad	0%	Avira URL Cloud	safe	
http://https://covid19tracking.narrativa.com/img/carto.png	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/pl.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/pl.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/pl.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fr.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fr.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fr.html	0%	URL Reputation	safe	
http://https://www.narrativa.com	0%	Avira URL Cloud	safe	
http://labs.skinkers.com/touchSwipe/	0%	URL Reputation	safe	
http://labs.skinkers.com/touchSwipe/	0%	URL Reputation	safe	
http://labs.skinkers.com/touchSwipe/	0%	URL Reputation	safe	
http://https://covid19tracking.narrativa.com/v2/bootstrap-4.4.1-dist/css/custom.css	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/el.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/el.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/el.html	0%	URL Reputation	safe	
http://https://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://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://narrativa.com	0%	Avira URL Cloud	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://covid19tracking.narrativa.com	0%	Avira URL Cloud	safe	
http://https://covid19tracking.narrativa.com/img/NarrativaLogoBlanco.png	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.googletagservices.com	142.250.186.34	true	false		high
www.meneame.net	108.128.145.3	true	false		high
di7juyclzlgyp.cloudfront.net	13.225.74.87	true	false		high
eu-u.openx.net	34.98.64.218	true	false		high
dbpabf0off7y1.cloudfront.net	13.224.193.117	true	false		high
prensaiberica.map.fastly.net	199.232.194.133	true	false		unknown
republica.com	146.255.19.152	true	false		high
scontent.xx.fbcdn.net	31.13.92.14	true	false		high
aec01.esg.rtve.edgetcdn.io	185.57.173.170	true	false		unknown

Copyright Joe Security LLC 2021

Name	IP	Active	Malicious	Antivirus Detection	Reputation
script.hotjar.com	13.224.193.122	true	false		high
tagr-gcp-odr-euw4.mookie1.com	34.98.67.61	true	false		high
d1j70itqjm2icu.cloudfront.net	13.225.74.97	true	false		high
cm.g.doubleclick.net	142.250.185.226	true	false		high
facebook.com	31.13.92.36	true	false		high
match-1943069928.eu-west-1.elb.amazonaws.com	54.76.6.247	true	false		high
localcoronavirus.com	104.21.18.245	true	false		unknown
d2dzdx91mh5kpx.cloudfront.net	13.224.193.96	true	false		high
ec2-34-243-184-100.eu-west-1.compute.amazonaws.com	34.243.184.100	true	false		high
id.rlcdn.com	35.244.174.68	true	false		high
static-cdn.hotjar.com	13.225.74.30	true	false		high
www.google.de	142.250.185.227	true	false		high
star-mini.c10r.facebook.com	31.13.92.36	true	false		high
pagead46.l.doubleclick.net	142.250.186.162	true	false		high
pugm22000nf.pubmatic.com	185.64.189.115	true	false		high
us-u.openx.net	35.244.159.8	true	false		high
d2jcax5o6gwtn6.cloudfront.net	143.204.98.33	true	false		high
cs491300.wpc.mucdn.net	192.229.220.196	true	false		unknown
stats.l.doubleclick.net	74.125.133.155	true	false		high
s.libertaddigital.com	213.149.255.231	true	false		high
cni-digital.map.fastly.net	151.101.2.133	true	false		unknown
akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com	52.210.129.255	true	false		high
cs41.wac.edgecastcdn.net	93.184.220.66	true	false		high
4i2g925ohj.execute-api.eu-west-3.amazonaws.com	13.225.74.124	true	false		high
proteccion10.net	193.32.242.105	true	false		unknown
vars.hotjar.com	13.224.193.73	true	false		high
cec01.eug.edgetcdn.io	51.255.81.138	true	false		unknown
partnerad.l.doubleclick.net	142.250.185.194	true	false		high
in-live.live.eks.hotjar.com	63.33.16.37	true	false		high
aec01.esg.eldiario.edgetcdn.io	84.17.62.22	true	false		unknown
googleads.g.doubleclick.net	142.250.185.194	true	false		high
d1gubrkaoxki64.cloudfront.net	13.225.74.27	true	false		high
m.facebook.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
img.europapress.es	unknown	unknown	false		high
estaticos-cdn.elperiodico.com	unknown	unknown	false		high
adservice.google.de	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
token.rubiconproject.com	unknown	unknown	false		high
static.hotjar.com	unknown	unknown	false		high
www.lavozdegalicia.es	unknown	unknown	false		high
i.blogs.es	unknown	unknown	false		high
static3.abc.es	unknown	unknown	false		high
platform.twitter.com	unknown	unknown	false		high
static1.abc.es	unknown	unknown	false		high
navarra.elespanol.com	unknown	unknown	false		high
static4.abc.es	unknown	unknown	false		high
match.adsrvr.org	unknown	unknown	false		high
www.ecestaticos.com	unknown	unknown	false		high
covid19tracking.narrativa.com	unknown	unknown	false		unknown
eldiariocantabria.publico.es	unknown	unknown	false		high
odr.mookie1.com	unknown	unknown	false		high
www.republica.com	unknown	unknown	false		high
kit.fontawesome.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
cronicaglobal.elespanol.com	unknown	unknown	false		high
phantom-elmundo.unidadeditorial.es	unknown	unknown	false		high
static.eldiario.es	unknown	unknown	false		high
static.hosteltur.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high
www.jornada.com.mx	unknown	unknown	false		unknown

Copyright Joe Security LLC 2021

Name	IP	Active	Malicious	Antivirus Detection	Reputation
in.hotjar.com	unknown	unknown	false		high
image6.pubmatic.com	unknown	unknown	false		high
s01.europapress.net	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
img.huffingtonpost.com	unknown	unknown	false		high
img2.rtve.es	unknown	unknown	false		high
media.revistagq.com	unknown	unknown	false		high

URLs from Memory and Binaries

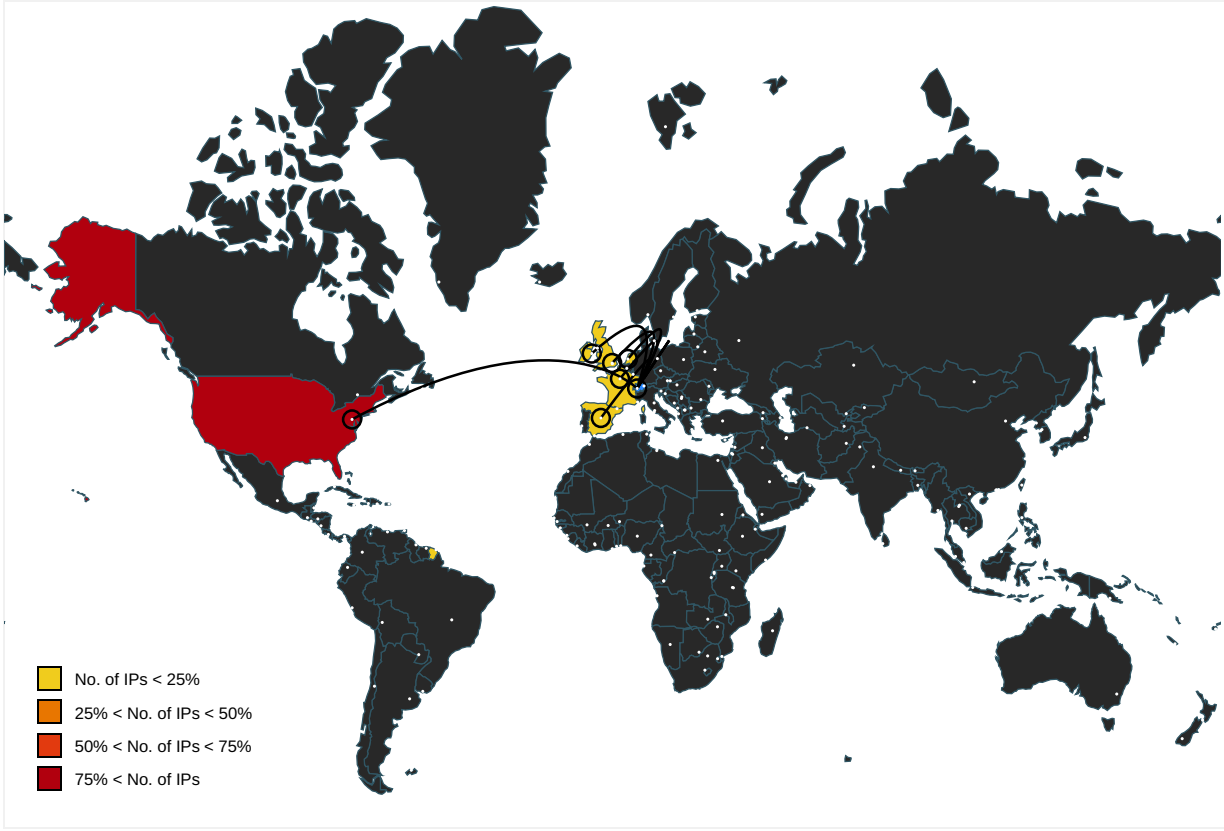
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.infosalus.com/asistencia/noticia-gobierno-asegura-espana-condiciones-vacunar-70-poblacio	13AB4AOQ.htm.2.dr	false		high
http://https://www.santepubliquefrance.fr/maladies-et-traumatismes/maladies-et-infections-respiratoires/inf	BFRV20U7.htm.2.dr	false		high
http://https://stats.g.doubleclick.net/g/collect	js[2].js.2.dr	false		high
http://https://www.hotjarconsent.com/sv.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.genbeta.com/actualidad/esta-web-puedes-comprobar-saturacion-aforo-tu-colegio-electoral-t	13AB4AOQ.htm.2.dr	false		high
http://https://img.huffingtonpost.com/asset/6090de5e210000bc497f0b00.jpeg?ops=1200_630	a-coruna-coronavirus[1].htm.2.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/interaction/%3Fai%3DCZ_nBNE6RYIq3CsvrgAeVpoTYCOzmuqNi5b2x	{293327BD-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr, ads[2].htm0.2.dr	false		high
http://https://www.huffingtonpost.es/entry/cuatro-tripulantes-de-un-buque-en-vigo-hospitalizados-por-la-cep	a-coruna-coronavirus[1].htm.2.dr	false		high
http://https://help.narrativa.com/	BFRV20U7.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://fontawesome.comhttps://fontawesome.comFont	free-fa-brands-400[1].eot.2.dr, free-fa-solid-900[1].eot.2.dr, free-fa-regular-400[1].eot.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.abc.es/espana/madrid/abci-elecciones-madrid-2021-directo-9-abren-colegios-electorales-y-	a-coruna-coronavirus[1].htm.2.dr	false		high
http://https://www.20minutos.es/noticia/4684721/0/las-farmacias-malaguenas-comenzaran-un-programa-de-seguim	13AB4AOQ.htm.2.dr	false		high
http://https://www.ecestaticos.com/imagestatic/clipping/1be/366/1be36630a456b11ca8b479d18a1daa04.jpg	a-coruna-coronavirus[1].htm.2.dr	false		high
http://https://phantom-elmundo.unidadeditorial.es/161a109e20f0c2eeae4b7737fead9341/resize/1200/f/jpg/assets	a-coruna-coronavirus[1].htm.2.dr	false		high
http://https://static1.abc.es/media/espana/2021/05/04/teruel_buj-k0zG--1024x512	13AB4AOQ.htm.2.dr	false		high
http://https://fontawesome.com	free.min[1].css.2.dr, free-fa-brands-400[1].eot.2.dr	false		high
http://https://covid19tracking.narrativa.com/vProyecto	{293327BD-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/interaction/%3Fai%3DCio2tN06RYIX2Hof2-galw5L4AtHl885i_K3g	ads[4].htm.2.dr	false		high
http://https://eldiariocantabria.publico.es/media/eldiariocantabria/images/2020/11/02/2020110212560140742.j	a-coruna-coronavirus[1].htm.2.dr	false		high
http://https://cronicaglobal.elespanol.com/uploads/s1/96/01/02/3/pablo-planas-cg-opinion_12_658x347.jpeg	a-coruna-coronavirus[1].htm.2.dr	false		high
http://getbootstrap.com)	bootstrap[1].js.2.dr, bootstrap[1].css.2.dr	false	• Avira URL Cloud: safe	low
http://https://www.abc.es/espana/aragon/abci-teruel-regala-115000-euros-bonos-para-gastar-comercios-bares-y	13AB4AOQ.htm.2.dr	false		high
http://https://4i2g925ohj.execute-api.eu-west-3.amazonaws.com/pro/coronavirus?confirmed_num=153.632.222&act	BFRV20U7.htm.2.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.2.dr	false		high
http://https://cdn.ampproject.org/amp4ads-host-v0.js	f[2].txt.2.dr	false		high
http://https://www.mscbs.gob.es/profesionales/saludPublica/ccayes/alertasActual/nCov/vacunaCovid19.htm	13AB4AOQ.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19tracking.narrativa.com/img/infobae.png	BFRV20U7.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.facebus.com/a-coruna-coronavirusRoot	{293327BD-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.nwc10.com/politica-privacidad	13AB4AOQ.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.lavozdegalicia.es/noticia/sociedad/2021/05/04/gobierno-aprobara-decreto-comunidades-pued	13AB4AOQ.htm.2.dr	false		high
http://https://covid19tracking.narrativa.com/img/carto.png	BFRV20U7.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.rtve.es/	BFRV20U7.htm.2.dr	false		high
http://https://www.lavozdegalicia.es/default/2021/05/03/00121620068642701225646/Foto/L24A1025.jpg	a-coruna-coronavirus[1].htm.2.dr	false		high
http://https://cdn.jsdelivr.net/npm/chart.js	13AB4AOQ.htm.2.dr, a-coruna-coronavirus[1].htm.2.dr	false		high
http://https://www.hotjarconsent.com/pl.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/images/mtad/back_blue.png	{293327BD-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr, ads[2].htm.2.dr	false		high
http://https://www.hotjarconsent.com/fr.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.libertaddigital.com/ciencia-tecnologia/salud/2021-05-04/portugal-suma-un-dia-mas-sin-mue	13AB4AOQ.htm.2.dr	false		high
http://https://www.narrativa.com	BFRV20U7.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/images/mtad/x_blue.png	{293327BD-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr, ads[3].htm.2.dr, ads[2].htm.2.dr, ads[2].htm0.2.dr, ads[1].htm1.2.dr, ads[1].htm0.2.dr, ads[5].htm.2.dr, ads[6].htm.2.dr, ads[1].htm2.2.dr, ads[1].htm.2.dr, ads[4].htm.2.dr	false		high
http://labs.skinkers.com/touchSwipe/	jquery.themepunch.tools.min[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.lavozdegalicia.es/noticia/sociedad/2021/05/03/xunta-decide-jueves-medidas-regiran-tras-e	a-coruna-coronavirus[1].htm.2.dr	false		high
http://https://systems.jhu.edu/research/public-health/ncov/	BFRV20U7.htm.2.dr	false		high
http://https://covid19tracking.narrativa.com/v2/bootstrap-4.4.1-dist/css/custom.css	BFRV20U7.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&h=600&adk=	{293327BD-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false		high
http://https://img.europapress.es/fotoweb/fotonoticia_20210504115714_1024.jpg	a-coruna-coronavirus[1].htm.2.dr	false		high
http://https://github.com/pcm-dpc/COVID-19	BFRV20U7.htm.2.dr	false		high
http://https://www.europapress.es/galicia/noticia-sube-165-poblacion-vacunar-galicia-pauta-completa-adminst	a-coruna-coronavirus[1].htm.2.dr	false		high
http://https://i.blogs.es/9fbb30/aforo-ios/840_560.jpg	13AB4AOQ.htm.2.dr	false		high
http://https://www.hotjarconsent.com/el.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/html/r20210429/r20190131/zrt_lookup.html#RS-0-&adk=181227	{293327BD-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false		high
http://https://proteccion10.net/compras.html	{293327BD-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr, 13AB4AOQ.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap[1].css0.2.dr	false		high
http://https://googleads.g.doubleclick.net/aclk?sa=L&ai=CMPQ-N06RYJSVForugAe6lIX4AdHl885i_K3glvEN1YTBrr	ads[3].htm.2.dr	false		high
http://https://stats.g.doubleclick.net/g/collect?v=2&	js[2].js.2.dr	false		high
http://googleads.g.doubleclick.net	f[1].txt2.2.dr, f[2].txt.2.dr	false		high
http://https://cronicaglobal.elespanol.com/primeras-planas/cinco-millones-vacunados-fin-toque-queda_478303_	a-coruna-coronavirus[1].htm.2.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/interaction/%3Fai%3DCUgKM4U2RYPqOC6_C7_UPn9CfyAjs5rqjYuW9	{293327BD-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr, ads[1].htm.2.dr	false		high
http://carto.com/	BFRV20U7.htm.2.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/interaction/%3Fai%3DCZjWROE6RYOmjBq6ux_AP_Ki7qA7ltZX_Ybju	ads[1].htm2.2.dr	false		high
http://https://twitter.com/in	{293327BD-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false		high
http://https://www.hotjarconsent.com/zh.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://stats.uptimerobot.com/Q6NlpspLQ	BFRV20U7.htm.2.dr	false		high
http://https://www.hotjar.com	box-5e3cec51ed8e99df6977c199d27812d7[1].htm.2.dr	false		high
http://https://www.hotjarconsent.com/fi.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/interaction/%3Fai%3DCQ65jN06RYJySN8yAgQfh7IqYDvL766Jijb6x	ads[5].htm.2.dr	false		high
http://https://platzi.com/r/nwc10/	a-coruna-coronavirus[1].htm.2.dr	false		high
http://https://ka-f.fontawesome.com	b745858f50[1].js.2.dr	false		high
http://www.greensock.com/club/	jquery.themepunch.tools.min[1].js.2.dr	false		high
http://https://fontawesome.com/license/free	free.min[1].css.2.dr	false		high
http://https://www.hotjarconsent.com/sq.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://media.revistagq.com/photos/60910fb6235a5910299c90f7/16:9/w_1920	13AB4AOQ.htm.2.dr	false		high
http://https://narrativa.com	BFRV20U7.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.hotjarconsent.com/it.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.hosteltur.com/143907_asi-van-las-reservas-de-hotel-en-comparacion-con-2019.html	a-coruna-coronavirus[1].htm.2.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/interaction/%3Fai%3DCyDxo402RYLG3Nr6A7_UPrfyGgATR5fPOYvyt	ads[1].htm0.2.dr	false		high
http://https://platform.twitter.com/widgets.js	13AB4AOQ.htm.2.dr, a-coruna-coronavirus[1].htm.2.dr	false		high
http://https://www.hotjarconsent.com	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.20minutos.es/noticia/4684770/0/la-consejeria-de-turismo-grupo-fuertes-y-hotel-puerto-jua	13AB4AOQ.htm.2.dr	false		high
http://https://www.lavozdegalicia.es/default/2021/05/03/00121620061682629287424/Foto/AY4C1F1_19641.jpg	a-coruna-coronavirus[1].htm.2.dr	false		high
http://https://www.rtve.es/noticias/20210504/elecciones-madrid-4m-2021-directo-ultima-hora-resultados/20883	a-coruna-coronavirus[1].htm.2.dr	false		high
http://https://www.hotjarconsent.com/pt_br.html	modules.7225c79fe4e29708c611[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://googleads.g.doubleclick.net/aclk?sa=L&ai=CYSNP-k2RYLm0EpG-3gOV3YCIBtHl885i_K3glvEN1YTBrr	ads[1].htm1.2.dr	false		high
http://https://kit.fontawesome.com/b745858f50.js	BFRV20U7.htm.2.dr	false		high
http://https://i.blogs.es/3d0f69/peugeot-concesionario-/840_560.jpeg	13AB4AOQ.htm.2.dr	false		high
http://https://covid19tracking.narrativa.com	BFRV20U7.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://amzn.to/31GOUWE	compras[1].htm.2.dr	false		high
http://https://img.europapress.es/fotoweb/fotonoticia_20210504124210_1024.jpg	13AB4AOQ.htm.2.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/html/r20210429/r20190131/zrt_lookup.html	{293327BD-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false		high
http://https://www.meneame.net//mnmstatic.net/img/mnm/logo-350x350.png	13AB4AOQ.htm.2.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/html/r20210429/r20190131/zrt_lookup.html#	{293327BD-AD29-11EB-90E6-ECF4BB82F7E0}.dat.1.dr, f[1].txt.2.dr	false		high
http://https://cdn.ampproject.org/rtv/%	f[2].txt.2.dr	false		high
http://https://googleads.g.doubleclick.net	f[1].txt2.2.dr, f[2].txt.2.dr	false		high
http://https://static.hotjar.com/c/hotjar-	13AB4AOQ.htm.2.dr	false		high
http://https://covid19tracking.narrativa.com/img/NarrativaLogoBlanco.png	BFRV20U7.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://img.europapress.es/fotoweb/fotonoticia_20210504121532_1024.jpg	13AB4AOQ.htm.2.dr	false		high
http://https://www.lavozdegalicia.es/default/2021/04/14/00121618386603074724936/Foto/efe_20210414_073806655	13AB4AOQ.htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://getbootstrap.com/)	bootstrap[1].css0.2.dr	false		high
http://www.github.com/mattbryson	jquery.themepunch.tools.min[1].js.2.dr	false		high
http://https://amzn.to/2XQwbGR	compras[1].htm.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
93.184.220.66	cs41.wac.edgecastcdn.net	European Union		15133	EDGECASTUS	false
31.13.92.36	facebook.com	Ireland		32934	FACEBOOKUS	false
13.225.74.124	4i2g925ohj.execute-api.eu-west-3.amazonaws.com	United States		16509	AMAZON-02US	false
142.250.185.226	cm.g.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.185.227	www.google.de	United States		15169	GOOGLEUS	false
13.225.74.27	d1gubrkaoxki64.cloudfront.net	United States		16509	AMAZON-02US	false
54.76.6.247	match-1943069928.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
13.224.193.122	script.hotjar.com	United States		16509	AMAZON-02US	false
13.224.193.73	vars.hotjar.com	United States		16509	AMAZON-02US	false
51.255.81.138	cec01.eug.edgetcdn.io	France		16276	OVHFR	false
52.210.129.255	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
142.250.186.34	www.googletagservices.com	United States		15169	GOOGLEUS	false
13.225.74.97	d1j70itqjm2icu.cloudfront.net	United States		16509	AMAZON-02US	false
192.229.220.196	cs491300.wpc.mucdn.net	United States		15133	EDGECASTUS	false
142.250.185.194	partnerad.l.doubleclick.net	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
84.17.62.22	aec01.esg.eldiario.edgetcdn.io	United Kingdom		60068	CDN77GB	false
74.125.133.155	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
213.149.255.231	s.libertaddigital.com	Spain		16371	ACENS_ASSpainHostinghousingandVPNservicesES	false

Copyright Joe Security LLC 2021

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
146.255.19.152	republica.com	Netherlands		29119	SERVIHOSTING-ASAireNetworksES	false
31.13.92.14	scontent.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false
13.225.74.87	di7juyclzlgyp.cloudfront.net	United States		16509	AMAZON-02US	false
35.244.159.8	us-u.openx.net	United States		15169	GOOGLEUS	false
199.232.194.133	prensaiberica.map.fastly.net	United States		54113	FASTLYUS	false
185.64.189.115	pugm22000nf.pubmatic.com	United Kingdom		62713	AS-PUBMATICUS	false
143.204.98.33	d2jcax5o6gwtn6.cloudfront.net	United States		16509	AMAZON-02US	false
13.224.193.96	d2dzdx91mh5kpx.cloudfront.net	United States		16509	AMAZON-02US	false
108.128.145.3	www.meneame.net	United States		16509	AMAZON-02US	false
34.243.184.100	ec2-34-243-184-100.eu-west-1.compute.amazonaws.com	United States		16509	AMAZON-02US	false
142.250.186.162	pagead46.l.doubleclick.net	United States		15169	GOOGLEUS	false
104.21.18.245	localcoronavirus.com	United States		13335	CLOUDFLARENETUS	false
13.225.74.30	static-cdn.hotjar.com	United States		16509	AMAZON-02US	false
151.101.2.133	cni-digital.map.fastly.net	United States		54113	FASTLYUS	false
34.98.64.218	eu-u.openx.net	United States		15169	GOOGLEUS	false
193.32.242.105	proteccion10.net	Spain		41705	GRUPOBALADIGES	false
185.57.173.170	aec01.esg.rtve.edgetcdn.io	Netherlands		29119	SERVIHOSTING-ASAireNetworksES	false
13.224.193.117	dbpabf0off7y1.cloudfront.net	United States		16509	AMAZON-02US	false
63.33.16.37	in-live.live.eks.hotjar.com	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403971
Start date:	04.05.2021
Start time:	15:35:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://localcoronavirus.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@4/237@54/40
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

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 104.42.151.234, 92.122.145.220, 88.221.62.148, 40.88.32.150, 142.250.185.72, 142.250.184.234, 142.250.185.110, 142.250.184.226, 92.122.213.154, 92.122.213.162, 151.101.2.109, 151.101.66.109, 151.101.130.109, 151.101.194.109, 142.250.185.67, 142.250.185.142, 142.250.186.66, 142.250.184.196, 13.88.21.125, 142.250.186.161, 142.250.186.67, 69.173.144.139, 69.173.144.165, 69.173.144.138, 184.30.24.56, 152.199.19.161, 2.20.142.210, 2.20.142.209, 52.255.188.83, 20.82.210.154, 104.18.23.52, 104.18.22.52, 172.64.100.17, 172.64.101.17, 104.22.5.10, 172.67.27.228, 104.22.4.10, 104.22.3.54, 172.67.21.145, 104.22.2.54, 104.20.86.24, 104.20.85.24, 37.157.2.236, 37.157.6.242, 37.157.4.23, 37.157.6.252, 37.157.4.41, 37.157.2.237, 37.157.4.28, 37.157.6.246, 92.122.213.194, 92.122.213.247 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, arc.msn.com.nsatc.net, ka-f.fontawesome.com.cdn.cloudflare.net, partner.googleadservices.com, fs-wildcard.microsoft.com.edgekey.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, www.google-analytics.com, www.bing.com, fonts.googleapis.com, fs.microsoft.com, dual-a-0001.a-msedge.net, pagead2.googlesyndication.com, www.jornada.com.mx.cdn.cloudflare.net, www3.l.google.com, store-images.s-microsoft.com, eldiariocantabria.publico.es.cdn.cloudflare.net, blobcollector.events.data.trafficmanager.net, wac.apr-8315.edgecastdns.net, cs9.wpc.v0cdn.net, a1972.g2.akamai.net, au.download.windowsupdate.com.edgesuite.net, pixel.rubiconproject.net.akadns.net, store-images.s-microsoft.com-c.edgekey.net, adservice.google.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, track.adformnet.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, www.googletagmanager.com, arc.trafficmanager.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, dualstack.f3.shared.global.fastly.net, kit.fontawesome.com.cdn.cloudflare.net, static-abc.akamaized.net, www-google-analytics.l.google.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, tpc.googlesyndication.com, go.microsoft.com.edgekey.net, analytics.google.com, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, navarra.elespanol.com.cdn.cloudflare.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
15:37:47	API Interceptor	1x Sleep call for process: OpenWith.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\IUHEMSR9\googleads.g.doubleclick[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\T8DRMTJ1\localcoronavirus[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	525220
Entropy (8bit):	5.35075526310324
Encrypted:	false
SSDEEP:	12288:U6D6ff555weQe6yyWW888vEPPPllJ3333FUUUUUzR77+QpR:U6D6ff555weQe6yyWW888vEPPPllJ33s
MD5:	1E358F3E62C5F89657D0B5DE855F4987
SHA1:	6C02AF68CD3E2B988C3010D48214B8ED7F51C6F6
SHA-256:	4C12E5D81C9228868A246E2124C3CF6DA2D9006C6DD78968107911C9148D4219
SHA-512:	33AB200F361FCF0A30795A723F8BB896A78385EC3D59F54D36A20B935603B5490DC716FBA19E1E6CEF72F244AFD948D45F9CEF9308C59177ADABF5C0E1E0FF1

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\T8DRMTJ1\localcoronavirus[1].xml	
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="goog_pem_mod" value="123" ltime="3991618896" htime="30884149" /><item name="google_experiment_mod34" value="660" ltime="3991778896" htime="30884149" /><item name="google_experiment_mod53" value="165" ltime="3991778896" htime="30884149" /><item name="google_experiment_mod36" value="393" ltime="3991778896" htime="30884149" /><item name="google_experiment_mod37" value="671" ltime="3991778896" htime="30884149" /><item name="google_experiment_mod44" value="689" ltime="3992238896" htime="30884149" /></root><root><item name="goog_pem_mod" value="123" ltime="3991618896" htime="30884149" /><item name="google_experiment_mod34" value="660" ltime="3991778896" htime="30884149" /><item name="google_experiment_mod53" value="165" ltime="3991778896" htime="30884149" /><item name="google_experiment_mod36" value="393" ltime="3991778896" htime="30884149" /><item name="google_experiment_mod37" value="671" ltime="3991778896" htime="30884149" /><item name="google_experiment_mod

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{293327BB-AD29-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.876354156509451
Encrypted:	false
SSDEEP:	192:rtZGZ72XW3tGifDKQzMbYB3+DssfWK9jrkFl:rDiSmdXKEc7n0
MD5:	6E2BB8593971184F6DDF84DB8C7E5C50
SHA1:	C63C3C4DEC29C25B2C3786AF6F3A587AF6B9074F
SHA-256:	C44D375B976D58794B41665024C935FD28FBC8F86C232E7E9F02E33FF92E4B83
SHA-512:	3F74DBD20E733954EBA3029D3631A6365F24BA154E5E057674417A1BB6FD6084559092C0C414652F3CCD53D2CC8D6DF79AEBBAC77DF1F45D007B61F700059C1
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\{293327BD-AD29-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	1501802
Entropy (8bit):	4.0396569027209095
Encrypted:	false
SSDEEP:	6144:lQ7qrKefJyQgeg6gjQbqrKefJyQgeg6gM/wzjef1wzjef50Ql0nDceff:iCJylrXsCJylrXER1RuQl0Jf
MD5:	945EDB44C4D4C73B70CB0984D1BD9B8F
SHA1:	6FC547EF2E13532EC6FDB9C24439EDD1B10CCD51
SHA-256:	0977F8D5FD8D0297CBC4E62C8F01413CA2F511C20960AC98A631FD1BC4CA4C8A
SHA-512:	635EB3BBC151856BFE0BB811B2002CBB263BAE0A003BD0C79BB94EA099E00290A66E06A96B94C25A37998F813952669F6C27A2CDC1B25EDCC4D1A21D5F134DD6
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\{313467C4-AD29-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.565846287161575
Encrypted:	false
SSDEEP:	48:IwOGcpr/GwpaVJG4pQ7GrapbSWZGQpK8G7HpR8aTGIpG:rSZJQN6vBSWzAXT8eA
MD5:	085031FB71BF11E006AE60C3026BFB3C
SHA1:	692F0ACFA99266BF67A7FA2F990BCE25C0567561
SHA-256:	8D5D03AF64CB31EFCBF1FDD2E80478F89C402F5E559E402369621E4F04C0088C
SHA-512:	1F2D04C507D4A29F042F197DCB1B6A64B64B1E943B1DC243D80266658B4C96BF238995A8672D106EB410C2DFC5EB36D8B3BA176C01CB2A01625808C8B732CE7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{313467C4-AD29-11EB-90E6-ECF4BB82F7E0}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\po60zt0\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	5893
Entropy (8bit):	7.724698219430442
Encrypted:	false
SSDEEP:	96:ohuQ5Vo7FhknmWpYOxYbOLMHfmH0mgzdtsfNFeC933ktunIOys60yiiLEgY4yJVx:oEQ07FhknOuM/muPs1Fqmd9nyiiZqL
MD5:	5F9E22F5B15EDA5BD5849EB90800B813
SHA1:	631DCD0710036D3ACBC3F1F6D50BD117A0A21D2D
SHA-256:	C2D017C74F83D9239DDBCC5BF540648C9E9C57AF29036CB951A0B693D054ED2A
SHA-512:	E4D7D73A8B14624D34509E3DC3461D649DB0E7BEF66DCEA6B58AC5D176AA2DD00F52EF7C232A2ED3796FCEEFFB4D597FAB8E10283E08916B21633844A7B737 5E
Malicious:	false
Reputation:	low
Preview:	(.h.t.t.p.s.:././.l.o.c.a.l.c.o.r.o.n.a.v.i.r.u.s...c.o.m./.f.a.v.i.c.o.n...p.n.g.....PNG.....IHDR...@...A.....a5.{...7iCCPAdobe RGB (1998)..(....J.P....E.V...p'QPl...I[. X.C..IC.b.n.... .n.\.}.'G.A..|...C.....9....b..Q..X.v.....f...N..v.u..'q.....M..4...2..J.#`..e!....1...j....N.5.O@....P.r..J..|._..s=..9..r_.L.]k.Z...Y.T.eY..&A$.....3....J...Q....`1.l7..V.....=...en.G.@,=.YA x...U.;..b.p...azTd.7p....E.Z...<.....O..S?.....pHYs...#...#.x.?v....iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xm lns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xap/1.0 /sType/ResourceEvent#" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\-F63fjptAgt5VM-kVkqdyU8n1i8q0Q[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17868, version 1.1
Category:	downloaded
Size (bytes):	17868
Entropy (8bit):	7.9664031905869646
Encrypted:	false
SSDEEP:	384:9gXBQFQmgBnaQTyky3exU+qwRmwoL2ydtNz1NWTWiVgFCQ:CXBQm9nJT/KldLvHNznckh
MD5:	0C3DB5C13D8FFB2DDD28B9A42A59DC65
SHA1:	B93182204F3E0C0F69AC5085D55325A212A1FC1E
SHA-256:	21DBCB97EE4D5E7F34F98E87A5FAEF3B26CBF3B9A082C32A367E3480F2057E2F
SHA-512:	E5F9F0129B9E9BCC0D9BED6FAC626768BA9E6740DAD0B8B32024FC113E93B1EA9C60AB50BD1DC39B24946C29A81E74B348CA32FFFCE68DE52A4082042BA68 8C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/ibmplexmono/v6/-F63fjptAgt5VM-kVkqdyU8n1i8q0Q.woff
Preview:	wOFF.....E.....GDEF.....@...R.d.RGPOS..... ... DvLuGSUB.....*...P.J..OS/2.....Y...`i. vcmap...h...v...,^...cvt .....@...@.6..fpgm... .....s.Y.7gasp..... ...!glyf...,..7...|.J.^head..>....5...6.h.xhhea..>H.....$...Ehmtx..>h...&....3.-.loca..?.....$..maxp..A.... ... .;.Oname..A.....x..9epost..B....U.....Vprep..D.....'F.x.....@ @...}.27.1B.....Z.Z....W...Q..d..U..f..Q.q.k<5^.....DFLT.....x.M..npa.E..o...6.._m7n.6....v...F/.'...p.D.p.#..]..P....~.....g=...9.ms..\(....WMCA..^.i.n ...-Ej.p.. pe...8.M....[?.l....PbI%.B*h..N..a.....eQ.cY.gU.`S.d[.bG..@.Q.A..T.A..T.A..T.A..Bp..M..%..kh.l#[.8.U..|./+hO.Q6.b....1.k...7P....L.Bw.'..6....(*..Z...._..'. ,@..6...,..X.'...h.a...x.c`f.`.... .....l.M.....L..L.....@.l.(.t.U`p``P.b.....(...8.$....H)00.....x.m.3.U.....m../.q.m.m.m.s..%....~.F.YE..U4.....#.b.....h....f....'.gA. w.?..E..A.`x.?...$nY,... .@qeU.N..l...o.>....9.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\13AB4AOQ.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	122780
Entropy (8bit):	5.194205309063521
Encrypted:	false
SSDEEP:	1536:fL83LI+7/nygB7DmzSrkYt/hILtbt2C+kMVvXy3Qqa0MH1w0SB:fY35ygNDmzStZVvXy3QqaJOB
MD5:	95E45D927FC2A54B04AD4A2517D273EE
SHA1:	A3EF26247A15478EF41C6D0D801FF6CD40E22125
SHA-256:	3F1B82120B58995872F8B294611D22F56CC5A96F99EE78069FB56E604F6505AC
SHA-512:	511764E9107A0665DD2362CF7F0F49DA3C146A7F57BDBE2B49D4FF09D6803E96F2E957CC97C4DDECC2126D1E15716A2E2F4E90C31F1D7372946FD98BADC2F2 D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\13AB4AOQ.htm	
Preview:	<!DOCTYPE html>.<html lang="es-ES">.<head>.<meta charset="utf-8">.<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no">.<title>. Local Coronavirus Espa.a . .ltima hora .</title>.<meta name="description" content=". Coronavirus Espa.a. . .ltimas Noticias y . alertas locales de Coronavirus Espa.a.">.<meta name="keywords" content="Espa.a Coronavirus, informaci.n Espa.a Coronavirus, alertas Espa.a Coronavirus, estad.sticas Espa.a C oronavirus, .ltima hora de las noticias en Espa.a Coronavirus">.<link rel="shortcut icon" type="image/png" href="/favicon.png">.<link href='https://fonts.googleapis.com/css?family=Catamaran:100,400,200,300,500,600,700,800,900%7CBiryani:100,200,400,300italic,300,400italic,600,600italic,700,700italic,800,800italic' rel='stylesheet' type='text/css'>.<link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.css" media="screen">.<link rel="stylesheet" type="text/css" href="/assets/css/f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\16201019236086[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1200x683, frames 3
Category:	downloaded
Size (bytes):	77891
Entropy (8bit):	7.9651588905943616
Encrypted:	false
SSDEEP:	1536:TQOeWEXLDCOcDnhXikXK6ywIBIzWW0stzUTxT9LUES:sOeNbmBbhyugiSnstzUTxTS
MD5:	7BB52F359CF323ED5A12D210F8CD5716
SHA1:	F2706EFBB3560BD1C420F63504AB27C56ABFD21D
SHA-256:	8C53AEF68ABC3BB2445A588FE56FAF6A80B9F49D85253A54B54AA3E51B754458
SHA-512:	1FB00C1E49EA68548DDE2061F9EBFFAA94F23E5472D7741934FCC8FCD8359B0397929251CFF1FF6580E3C67738E7DFD372AE89E126024179C55C550E5F27DA05
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://phantom-elmundo.unidadeditorial.es/161a109e20f0c2eeae4b7737fead9341/resize/1200/f/jpg/assets/multimedia/imagenes/2021/05/04/16201019236086.jpg
Preview:	.....JFIF.....`.`.....C.....%...#... , #&')*)..-0-(0%()(...C.....(...(((((((

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\4UabrENHsxJlGDuGo1OIlLU94YtzCwA[1].woff	
Preview:	wOFF.....g`.....d.....GDEF.....q.....GPOS.....$..+..K.MGSUB.....OS/2.....U...`i`..cmap.....~n..cvt .....fpgm...T.....uo..gasp.....glyf...(..>W..mNU!.)head..[....6...6..'.hhea..[.... ...$...4hmtx..[.....1'jloca..^....~.....t.maxp..a.... ... ....name..a4.....V..4.post..a.....O...prep..e.....^....x.D...Q...3..I.=D.@@....@...."...}.....`.%.....x.....umW...g.WwO.....J..^?.Jci^N{.Nr..Jw@.n(.....t4....i...x..Z...6.=r.....q`.>....m.....fy.g..y4N...tAg.."KWWW.j.....8...n.3..:..1....9.+.}...b]....0..6V..).G.r.....N...,R(.o.t.LU....;.{.l.y....i..w.{F..;p'.....,.....:3...|...,.`pGPAV.?....q!.....=.(cn.'<.....sK_...]..U.W.....b....E|.o..Jp.n.uX....*J.q'SFy...l..Cd..XZ..RP...#.w...C)..s../..D..1.G...Sx...e.....x.o.mJ...~./L..r...Y..sD./.....>$R`..&.v.....D..w.). .f.Y."<..V/.zQ{.8./...X*.....B..Jp#%.7.e>+L.Q.1..hd..k._...f..u....+....Q...N..|....$Lv.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\6090de5e210000bc497f0b00[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):	142245
Entropy (8bit):	7.9618443927362
Encrypted:	false
SSDEEP:	3072:kdnscqZ98HEZWRry9awO8Efr0iWByU5ENR2P6+5eJ:kdvqj8HEZT8r09By1H85W
MD5:	ABD331EB9B1E98071CEA34FE66E6ED5F
SHA1:	5CE5D23ED955471CD35A8A354F86AE26F2C32C33
SHA-256:	434EE202ADFCB559471863F8BE4101F4D07D644175EC2E8CF6B7306EC076704A
SHA-512:	CA196DFE930C738719C64F34E30F140E344DA3E4242E97FEB16E291F7AFAFDEBBBA3339AE6A35E01E68504747F0A3CFA05AB2F933FE9FD45A6D8816A56BC07E1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img.huffingtonpost.com/asset/6090de5e210000bc497f0b00.jpeg?ops=1200_630
Preview:	.....C.....%...#... , #&')*)..-0-(0%()(...C.....(...(((((((

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\77YWRDV3.htm	
Preview:	<!DOCTYPE html>.<html lang="es-ES">.<head>.<meta charset="utf-8">.<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no">.<title>. Local Coronavirus Espa.a . .ltima hora .</title>.<meta name="description" content=". Coronavirus Espa.a. . .ltimas Noticias y . alertas locales de Coronavirus Espa.a.">.<meta name="keywords" content="Espa.a Coronavirus, informaci.n Espa.a Coronavirus, alertas Espa.a Coronavirus, estad.sticas Espa.a C oronavirus, .ltima hora de las noticias en Espa.a Coronavirus">.<link rel="shortcut icon" type="image/png" href="/favicon.png">.<link href='https://fonts.googleapis.com/css?family=Catamaran:100,400,200,300,500,600,700,800,900%7CBiryani:100,200,400,300italic,300,400italic,600,600italic,700,700italic,800,800italic' rel='stylesheet' type='text/css'>.<link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.css" media="screen">.<link rel="stylesheet" type="text/css" href="/assets/css/f

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BFRV20U7.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):	19049
Entropy (8bit):	4.883999510292044
Encrypted:	false
SSDEEP:	384:ceb5Dipw8H1O7mhROvv2hbv3jvQ7bWXDd63q1OOigM:9dDinGsv8uXDo3O+D
MD5:	452B43AA8D0C80EBF27E9D1B66667909
SHA1:	BF9042725C1A522F9AE209DB352CF0EE973AB89E
SHA-256:	3FE5A78F7D2D3FF8E8865E0055C565DABD9481DBF88B9A845B52C44C46B2BF47
SHA-512:	BFA52632CFEF780829D9D59C9A5188D5F25DE294BD91B31997763B0717A650FE16411DCB8AA00EF8F938B63BD5E75856A351F4691141F086047621250BA40F0A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19tracking.narrativa.com/
Preview:	<!doctype html>.<html lang="en">..<head>. <meta charset="utf-8">. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">. <meta name="description" content="Proyecto de seguimiento del COVID19. Narrativa">. <meta name="author" content="Narrativa">.. <title>Proyecto de Seguimiento del Coronavrius COVID-19. Narrativa</title>.. <link rel="canonical" href="https://covid19tracking.narrativa.com">.. Bootstrap core CSS -->. <link rel="stylesheet" href="https://fonts.googleapis.com/css?family=IBM+Plex+Mono">. <link rel="stylesheet" href="https://fonts.googleapis.com/css?family=IBM+Plex+Sans">. <link rel="stylesheet" href="https://covid19tracking.narrativa.com/v2/bootstrap-4.4.1-dist/css/bootstrap.css">. <link rel="stylesheet" href="https://covid19tracking.narrativa.com/v2/bootstrap-4.4.1-dist/css/custom.css">. <link rel="stylesheet" href="bootstrap-4.4.1-dist/css/custom.css"> -->... <script src="https://kit.fontawe

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\LOGO-WEB-MIN[1].png	
Preview:	.PNG.....IHDR...i.....<.I&....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....$.....r...8...!.5m....._.+!..y....l.....^i.;.....T..1p]._..._..~.s.`v.;...a..3a.....m&..P@Y...g.....].....n.....LH.....e..{..{.q.....0'!m...%.L:...*..7+.M9....:+.}.>>:e}.....KH.`..0.@....06.v!6n...i.{..... ...@Y.....Aal..B..Oy.....(.!m...J;._.....-q=.n..L..>>:e.....IH....!{`V.{..3.....6P9Y...A.o.....Wf....W.....@..i....d..d.XqJd*.m.4.m_.....'....P._.}V.....SN.....P6<..6.....@..i.]E(..m&..a}|.q.....6PxY.....b.R.g.l_1Z.....'o..f.B.6.gZ.....,..6P....c.U.B..l....^.$.....#..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\0MX4YUS9\NarrativaLogoBlancoOnlyLogo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 83 x 86, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1616
Entropy (8bit):	7.786782588316121
Encrypted:	false
SSDEEP:	24:5W2OYbSUEtMd5FjZu4aCkZ/YxczlylXhc9X9OJvcFaJtyp7INBY1466gWvgwwr+N:5+Yb1J5hk4MBYxDXkAJwDoeFVhaN
MD5:	66C7E78AAFF8202A6C8ED6E6AA08AD24
SHA1:	EBDABE808FCCE99A59F3BBD98F195FCEC8CE3D64
SHA-256:	422D01C20525BD018E94DF7DF4DAC522A2F584856B9DCFACD8BE853E73B772B3
SHA-512:	C1A7AA678F31C61F760BAA08F8F538530374158EC02FB9E37F8B9C9F20AD43A50F0089F807E756D8B0AD1AEDE2BE325508FF8C224B6A60C67BB4264FF94894D1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19tracking.narrativa.com/img/NarrativaLogoBlancoOnlyLogo.png
Preview:	.PNG.....IHDR...S...V.....bKGD.....pHYs.....~.....tIME.....,...:!....IDATx..Oh\E.....H.K/9..=X.J....E....K/.%...I.C....C..z.Rz.RZ(x....JAH,.1X,jw..i.....{o6.`.o7...o....f2%"...yGyx.....|.l.1.m....z....2.-...k..sw..l.W.....U.3`F_.\.l....'..y.....@.....".."...p5.H.&p.hL..k#@.....d.....0P..3I..G...m.t.F....L....j^.$.....L.....L.Le.y..H#s..Y.9..7.....=.7=5..m.5..G.S.L. .|.F#..MPf-..s.3H..7z..aD..Y..y.....G+ .N..l.F.+..[.....^.P.....A.....S..}..KDa.2@:..l.....x.O...`..6.^.@..=<{.x...O2.a...Jd.....vJD..O..p8.0.....^&...]N...Ty..Y..?k.....2Q.&...T...{..@F.4.S...g.]=2{D..P.....eY....c..2@....M...i.Q\....M...."Qz6.9....|T..<%"]...;..;(.Z.b.y.g.....F.4B../.kz./MFE.....b`@....Ke.U.Dm:..m....J...6.@..:.....=.V...|....k..5...Q...h..d<.....1.M.n.0..+.zx....P.C.I.R.3KT.i".....BPy.x[6g-...L|1....b..U.....=....t%.<..v....C.i.v7D.....)"2....6..4..<.*].;....}.....].E....r.e+...^..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
Reputation:	low
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\0MX4YUS9\OpenGraph_EP_1024x512[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 CS6 (Windows), datetime=2016:02:08 14:29:41], baseline, precision 8, 1024x512, frames 3
Category:	downloaded
Size (bytes):	74328
Entropy (8bit):	7.845383000016866
Encrypted:	false
SSDEEP:	1536:2ujS0WapwPoPLeEC2lD5Rr2mivOJmV3UoNcm5OtFA:k7apXPLeEh5B2mimJGUkP5Ok
MD5:	9822CF2166091AF83CD844DE78186FD8
SHA1:	9695C76926E7D5B23315E0FFDE22B0A4E36BBFBD
SHA-256:	6DE1769729B44995A08673850B8C7E1B342551B30553A43388F3479D1F98267D
SHA-512:	76CEC0A7878C84E9347DD9B6B0E044531418C00D2E10BB2ADA4488DB6D6B4000060EC5C1AD96A15D209E4470337321D1FCF80DA98E5DA5411338A50A288A824
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s01.europapress.net/imagenes/estaticos/OpenGraph_EP_1024x512.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\OpenGraph_EP_1024x512[1].jpg	
Preview:	.....JFIF.....H.H.....Exif..MM.*.....b.....j.(.....1.....r.2.....i.....'.....'.Adobe Photoshop CS6 (Windows).2016:02:08 14:29:41..... .....&.(.....H.....H.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!22222222 2222222222222222222222222222222222222222222222.....P....!.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJ STUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:C DEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..T}.C8....}..H'.jeb.....y.....fcU.....;.xTQ.5Dz..f]...}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\a-coruna-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):	114782
Entropy (8bit):	5.194706189580743
Encrypted:	false
SSDEEP:	1536:yL83LI+7DC+gBvNyQOJOsi0brYj9ROvXy3Qqa0MH1w0en:yY3lfgtNyQORi0brvvXy3QqaJ6n
MD5:	DC7B8012A06F4BCEF4B5F5983802D98A
SHA1:	0396C8FA7166F23D430B3EFA6111DDEC8D3B15F8
SHA-256:	A1F752CD84F17A5FAEF840F9DD0904C54172DCA1C6CE465595A0A19CAABAE763
SHA-512:	6C6647548A55D73EABCE3CFC5BA1C53B4ADB056CE327A54A4AA425C9130AEB62310E15A2FBB9028280CB18643EA332FB9E23B719A803982238A9E9B2A29E040 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/a-coruna-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>. A Coru.a Coronavirus . .ltima hora .</title><meta name="description" content=". Datos de la evoluci.n del Coronavirus . A Coru.a Casos de Coronavirus A Coru.a . Muertes por Coronavirus A Coru.a."><meta name="keywords" content="A Coru.a Coronavirus, informaci.n A Coru.a Coronavirus, alertas A Coru.a Coronavirus, estad.sticas A Coru.a Coronavirus, .ltima hora de las noticias en A Coru.a Coronavirus">.<link rel="shortcut icon" type="image/png" href="/favicon.png">.<link href='https://fonts.googleapis.com/css?family=Catamaran:100,400,200,300,500,600,700,800,900%7CBiryani:100,200,400,300italic,300,400italic,600,600italic,700,700italic,800,800italic' rel='stylesheet' type='text/css'>.<link rel="stylesheet" type="text/css" href="/assets/css/bootstrap.css" media="screen">.<link rel="styleshe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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):	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\0MX4YUS9\ads[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	166043
Entropy (8bit):	5.743779986719533
Encrypted:	false
SSDEEP:	3072:hyXtVYiTw1sTSNwrubkV4Sj2sdw9DAOyWRE:hybYiTcsTswrubG4Sj2sdw9DAOnE
MD5:	0F3AEDE4BDFC5FBC6E822944F5F5DC6C
SHA1:	98256F83B6ABDF4C34BBF7AB92DD63DB7ABB1D5D
SHA-256:	D5F9C4234E9BDFBC2E3C291C7CCC470926AF103E64F15EA265E842AF19DE9A24
SHA-512:	8EF3914F1452F1B4305856D0FB6F845B8FEC1AE8974E4E9231C80EC67E51B64C1EF51D9CDA1ADF060C60AC00CAE4428248A6A66AB1C83E17F0DBD044E03C76 9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\ads[1].htm	
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4607443575710795&output=html&adk=1812271804&adf=3025194257&lmt=1620167792&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=1620167791222&bpp=60&bdt=2078&idt=332&shv=r20210429&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&nras=1&correlator=6289338029669&frm=20&pv=2&ga_vid=1286235738.1620167791&ga_sid=1620167792&ga_hid=540570788&ga_fc=0&u_tz=-420&u_his=1&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=-12245933&ady=-12245933&biw=784&bih=554&scr_x=0&scr_y=0&eid=44740387&oid=3&pvsid=3005462665899052&pem=123&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=1081
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/css?family\x3dRoboto\x27 rel\x3d\x27stylesheet\x27 type\x3d\x27text/css\x27\x3e\x3cstyle\x3e* {margin: 0;padding: 0;outline: none;}body {background: rgba(15%,15%,15%,1);height: 100%;}#ad_iframe {box-shadow: 0px 0px 5px 0 rgba(0,0,0,0.2);display: block;left: auto;margin: 0 auto;position: relative;top: auto;}html {height: 100%;}.toprow {width: 100%;font-family: \x27Roboto\x27, arial, sans-serif;display: table;height: 30px;font-size: 18px;background-color: #424242;}.btn {display: table;transition: opacity 1s, background .75s;-webkit-transition: opacity 1s, background .75s;-moz-transition: opacity 1s, background .75s;-o-transition: opacity 1s, background .75s;height: 30px;padding-top: 15px;padding-bottom: 15px;background: transparent;padding-right: 0.25em;color: #FFF;}#dismiss-button {padding-left: 0.5em;padd

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\ads[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	145072
Entropy (8bit):	5.693976177908565
Encrypted:	false
SSDEEP:	1536:QatBHXs+cHhy52nSNwru5BjJJyn94/ta28AOQjJ+VG1dmvxW7MWRE:Qat1s3SNwrub09wAuwWRE
MD5:	442C001AA6BBB5D797F87FC466AC9722
SHA1:	76A65F06D7A3D7679F9A2E37F859E58B03F76C2D
SHA-256:	BB4F06F1B2A1F4B1366695503B11BE71DD2C4BA6EF3E862D2F2FEB14D7CF3404
SHA-512:	EB3844C87C2D95309A92B30A71F491F8934D4215D36C2D607117597C377787ABBFB7E53040993A78EC2C5064B38E49E0D98EB3A13E5F57BD81DDF03A17BD045(
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=1620167874&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=1620167872605&bpp=742&bdt=894&idt=985&shv=r20210429&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D3308cfb7e7eaafa7-22cef212c3c700a1%3AT%3D1620135393%3ART%3D1620135393%3AS%3DALNI_MZvA0xUxZ4sGmu8lOwjMKzhvLszwQ&nras=1&correlator=2496065476927&frm=20&pv=2&ga_vid=1286235738.1620167791&ga_sid=1620167875&ga_hid=1189571962&ga_fc=0&u_tz=-420&u_his=8&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%2C31060956&oid=3&pvsid=3915826362476766&pem=123&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=2703
Preview:	<script>window.sra_later_blocks = [];</script><script>window.sra_later_blocks.push({creative:'\x3c!doctype html\x3e\x3chtml \x3e\x3chead\x3e\x3clink href\x3d\x27//fonts.googleapis.com/css2?family\x3dRoboto:wght@400;700\x26display\x3dswap\x27 rel\x3d\x27stylesheet\x27 type\x3d\x27text/css\x27\x3e\x3cstyle\x3e* {margin: 0;padding: 0;outline: none;}body {background: rgba(52, 58, 65, 0.600000);backdrop-filter: blur(15px); /*potential issue: minimal browser support*/-webkit-backdrop-filter: blur(15px); /*for safari*/height: 100%;}#ad_iframe {box-shadow: 0 !important;display: block;left: auto;margin: 0 auto;position: relative;top: auto;}.creative {transition: opacity 1s;-webkit-transition: opacity 1s;position: relative;}#card {background-color: #fff;border-radius: 6px;padding: 0 6px 1px;position: relative;box-shadow: 0px 8px 12px rgba(60, 64, 67, 0.15), 0px 4px 4px rgba(60, 64, 67, 0.3);}html {height: 100%;}.toprow {width: 100%;display: table;height: 24px;background-color: #fff;}.btn {displa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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):	83460
Entropy (8bit):	6.073201195588352
Encrypted:	false
SSDEEP:	768:GVx1rhUZ1/MpxRoDGVGWm4tAuVyV7/rc7BVgeWR1xBumvCHA:YrhOuRoDGLmUc7/oVoxBf3
MD5:	F843A31AC800EB1D324AD2C9BC7E3CC1
SHA1:	3CA1E4555940A84BE71877FB95495980F47C8230
SHA-256:	477C3926FEA1E58955C37352CA2F50C7A0C737BE8F019FBD87DF498E21E03016
SHA-512:	AA3B624C7F140C2E734D4971311AA923327045895391713132083055 6B9C08819D451D71B1E80B668AEA64375004FDEF5BB749D9016463F9DC1B8DA7F4C9B850
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=928288379&pi=t.aa~a.3257539417~i.8~rp.4&w=379&fwrn=4&fwrnh=100&lmt=1620167878&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%2Fa-coruna-coronavirus&flash=29.0.0&fwr=0&pra=3&rh=315&rw=378&rpe=1&resp_fmts=3&wgl=1&fa=27&dt=1620167878401&bpp=5&bdt=6690&idt=-M&shv=r20210429&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D3308cfb7e7eaafa7-22cef212c3c700a1%3AT%3D1620135393%3ART%3D1620135393%3AS%3DALNI_MZvA0xUxZ4sGmu8lOwjMKzhvLszwQ&prev_fmts=0x0%2C1280x906&nras=3&correlator=2496065476927&frm=20&pv=1&ga_vid=1286235738.1620167791&ga_sid=1620167875&ga_hid=1189571962&ga_fc=0&u_tz=-420&u_his=8&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=5658&biw=1280&bih=906&scr_x=0&scr_y=0&eid=42530672%2C31060956&oid=3&pvsid=3915826362476766&pem=123&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=3&uci=a!3&btvi=1&xpc=K1xRDvjwFy&p=https%3A//localcoronavirus.com&dtd=107

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\ads[3].htm	
Preview:	<!DOCTYPE html><html lang=fr><head><meta charset="UTF-8"><link rel="preload" href="https://www.gstatic.com/mysidia/a204a622610ec42c29322584ae03f5a9.js?tag=client_fast_engine" as="script"><script>var jscVersion = 'r20210429';</script><script>var google_casm=[];</script><script src="https://www.gstatic.com/mysidia/f27a2327937451811f326a3c5359709a.js?tag=pingback"></script><script>mys.pingback.init("CNSM8f2SsPACFQo34AodOkoBHw", [4,1],"text/vanilla_rda", {2:"server",1:"square-eta-vanilla",4:"mysidia_upscale,mysidia_analytics"},3);</script><style>HTML,BODY{height:100%;width:100%;margin:0;padding:0;overflow:hidden;}#mys-wrapper{height:100%;width:100%;overflow:hidden;position:absolute;top:0;left:0;align-items:center;display:flex;justify-content:center;line-height:normal;}.mys-wrapper A,.mys-wrapper A:visited,.mys-wrapper A:hover,.mys-wrapper A:active{color:inherit;cursor:pointer;text-decoration:inherit;}[dir=rtl] .flip-on-rtl{transform:scale(-1,1);transform-origin:center;}#mys-content{flex-sh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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):	84479
Entropy (8bit):	6.071077391344047
Encrypted:	false
SSDEEP:	768:hVxNrhUZ1/MpxRoDGQXsolSXwMrcqBVgelR1x3umWOCq3t:jrhOuRoDG6soAXwM3Vhx3fnd
MD5:	5FF24FD6E4CF1F04C077E4689AF6B979
SHA1:	B494E68C2982CDD0886797CCC14BB8884B1A6124
SHA-256:	9713C242D18C5F0C702D221FCA5B41C7F8F86A10ADAEFCD043FD6A3653003769
SHA-512:	676C98EA3E633A6DFC9923E89CF95ADBB83F68909D2C1A8DA87C419E6484030C65B2DA7D6BF3A1C5803257C009410A61D6A1FC69F0A33F79F12EBB5039A85D6B
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=1572976528&pi=t.aa~a.3655020510~rp.4&w=263&fwrn=4&fwrnh=100&lmt=1620167878&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&dt=1620167878401&bpp=5&bdt=6691&idt=-M&shv=r20210429&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D3308cfb7e7eaafa7-22cef212c3c700a1%3AT%3D1620135393%3ART%3D1620135393%3AS%3DALNI_MZvA0xUxZ4sGmu8lOwjMKzhvLszwQ&prev_fmts=0x0%2C1280x906%2C379x280&nras=4&correlator=2496065476927&frm=20&pv=1&ga_vid=1286235738.1620167791&ga_sid=1620167875&ga_hid=1189571962&ga_fc=0&u_tz=-420&u_his=8&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=1052&biw=1280&bih=906&scr_x=0&scr_y=0&eid=42530672%2C31060956&oid=3&pvsid=3915826362476766&pem=123&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=2&xpc=ZCPcU2XX9p&p=https%3A//localcoronavirus.com&dtd=249
Preview:	<!DOCTYPE html><html lang=fr><head><meta charset="UTF-8"><link rel="preload" href="https://www.gstatic.com/mysidia/a204a622610ec42c29322584ae03f5a9.js?tag=client_fast_engine" as="script"><script>var jscVersion = 'r20210429';</script><script>var google_casm=[];</script><script src="https://www.gstatic.com/mysidia/f27a2327937451811f326a3c5359709a.js?tag=pingback"></script><script>mys.pingback.init("CMXt-f2SsPACFQe73godpaEELw", [4,1],"text/vanilla_rda", {2:"server",1:"skyscraper-eta-vanilla",4:"mysidia_upscale,mysidia_analytics"},3);</script><style>HTML,BODY{height:100%;width:100%;margin:0;padding:0;overflow:hidden;}#mys-wrapper{height:100%;width:100%;overflow:hidden;position:absolute;top:0;left:0;align-items:center;display:flex;justify-content:center;line-height:normal;}.mys-wrapper A,.mys-wrapper A:visited,.mys-wrapper A:hover,.mys-wrapper A:active{color:inherit;cursor:pointer;text-decoration:inherit;}[dir=rtl] .flip-on-rtl{transform:scale(-1,1);transform-origin:center;}#mys-content{fle

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\ads[5].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):	84603
Entropy (8bit):	6.07910638736484
Encrypted:	false
SSDEEP:	1536:ucrhOpRoDGhtVNqKGgUmZO2yJuFcVCxR31j:ucrhJGhtVN3ZO2yJulZ
MD5:	7922D0F39746C45CC592EFB9D39A7E10
SHA1:	9A8D8F0DF31AADA7D5C3EEE3C56D7ACEACA3B48D
SHA-256:	C2B2F6DD4529F435CB54F150017D0B1C9B073D1CFC6A8498D9BED06E5B77CD7C
SHA-512:	F3B1A6E3BCB763760ECA81B5B34C732F9A24B94472B7839108392351E82EB040F5A8D61C24B23CAC81B068A7C3BBED80890D861098F499CA63E5C6C64D98363
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.2521325055~rp.4&w=263&fwrn=4&fwrnh=100&lmt=1620167878&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&dt=1620167878401&bpp=4&bdt=6689&idt=-M&shv=r20210429&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D3308cfb7e7eaafa7-22cef212c3c700a1%3AT%3D1620135393%3ART%3D1620135393%3AS%3DALNI_MZvA0xUxZ4sGmu8lOwjMKzhvLszwQ&prev_fmts=0x0%2C1280x906%2C379x280%2C263x600%2C263x600&nras=6&correlator=2496065476927&frm=20&pv=1&ga_vid=1286235738.1620167791&ga_sid=1620167875&ga_hid=1189571962&ga_fc=0&u_tz=-420&u_his=8&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=3155&biw=1280&bih=906&scr_x=0&scr_y=0&eid=42530672%2C31060956&oid=3&pvsid=3915826362476766&pem=123&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=4&xpc=diSoFowrDM&p=https%3A//localcoronavirus.com&dtd=611

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\ads[5].htm	
Preview:	<!DOCTYPE html><html lang=fr><head><meta charset="UTF-8"><link rel="preload" href="https://www.gstatic.com/mysidia/a204a622610ec42c29322584ae03f5a9.js?tag=client_fast_engine" as="script"><script>var jscVersion = 'r20210429';</script><script>var google_casm=[];</script><script src="https://www.gstatic.com/mysidia/f27a2327937451811f326a3c5359709a.js?tag=pingback"></script><script>mys.pingback.init("CNyJkv6SsPACFUxA4AodYbYC4w", [4,1],"scream/throne_image_logo_och", {2:"server",1:"towerAThrone",4:"mysidia_upscale,mysidia_analytics"},17);</script><style>HTML,BODY{height:100%;width:100%;margin:0;padding:0;overflow:hidden;}#mys-wrapper{height:100%;width:100%;overflow:hidden;position:absolute;top:0;left:0;align-items:center;display:flex;justify-content:center;line-height:normal;}#mys-overlay{height:100%;width:100%;overflow:hidden;position:absolute;top:0;left:0;box-sizing:border-box;pointer-events:none;z-index:1;border:1px solid #E5E5E5;;}.mys-wrapper A,.mys-wrapper A:visited,.mys-wrapper A:hov

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\ads[6].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):	92098
Entropy (8bit):	6.080844875489867
Encrypted:	false
SSDEEP:	768:AVxiCT4rhUZA/MpxRoDGcJsO+fVP06RvtSvn4rccBVgeMXR1xHAiem+C9vUaA:LCT4rhOpRoDGssOq5PRcArV4xHLZi
MD5:	8150A7EF2526C3B62E2B280856D4948D
SHA1:	C71AFD0927EB5F86B9CF6B531D69911C41F2EDF6
SHA-256:	C2EC261B87DDFD52BC76C257EF4F7D123D86D20A3574FED9F9A1A529D08DD127
SHA-512:	6AF185FAD293BCB967143ACC38B86652B11CEEFAC6762F95A078503C765750293B9DF3CCE87B3F14D0AAA0B2ECE076E30F8DD89313D8808A2092F0F426A0E5E0
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=1620167878&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&dt=1620167878401&bpp=5&bdt=6691&idt=-M&shv=r20210429&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D3308cfb7e7eaafa7-22cef212c3c700a1%3AT%3D1620135393%3ART%3D1620135393%3AS%3DALNI_MZvA0xUxZ4sGmu8lOwjMKzhvLszwQ&prev_fmts=0x0%2C1280x906%2C379x280%2C263x600&nras=5&correlator=2496065476927&frm=20&pv=1&ga_vid=1286235738.1620167791&ga_sid=1620167875&ga_hid=1189571962&ga_fc=0&u_tz=-420&u_his=8&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=2270&biw=1280&bih=906&scr_x=0&scr_y=0&eid=42530672%2C31060956&oid=3&pvsid=3915826362476766&pem=123&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=3&xpc=GtTZcefo2y&p=https%3A//localcoronavirus.com&dtd=536
Preview:	<!DOCTYPE html><html lang=fr><head><meta charset="UTF-8"><link rel="preload" href="https://www.gstatic.com/mysidia/a204a622610ec42c29322584ae03f5a9.js?tag=client_fast_engine" as="script"><script>var jscVersion = 'r20210429';</script><script>var google_casm=[];</script><script src="https://www.gstatic.com/mysidia/f27a2327937451811f326a3c5359709a.js?tag=pingback"></script><script>mys.pingback.init("CJyXi_6SsPACFRS4ewodkW4O5g", [4,1],"text/ryuk", {2:"server",1:"skyscraper-default",4:"mysidia_upscale,mysidia_analytics"},21);</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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	49153
Entropy (8bit):	5.520906949461031
Encrypted:	false
SSDEEP:	768:/yR3fYFBLbfs5sP5XqY3TyPnHpl1WY3SoavFVv6PU+CgYUD0lgEw0stZM:/y9gZfl5h3UHpaY3SoRCw0sk
MD5:	6DF1787C4BE82D1BB24F8BFFA10C7738
SHA1:	3634E839429E462E49C5F42B75FBFB4BA318AF6D
SHA-256:	2CB09C7B3E19BFC41743CA3624EF81C3258D56525647FEAC76AA757E0292627A
SHA-512:	CB3CE2BCEB61F390298C21E470423CCEB6DD93E648A7DD0467195B11FEF30BF7A086DFF47C4494E2533498D1448C1A22AAB1414C14FD73278F1C92E0F7BC3F54
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n=this||self,p=function(a,b){a=a.split(".");var c=n;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q={},r=function(){q.TAGGING=q.TAGGING||[];q.TAGGING[1]=!0};var t=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},v=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var x=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var y=window,z=document,A=function(a,b){z.addEventListener?z.addEventListener(a,b,!1):z.attachEvent&&z.attachEvent("on"+a,b)};var B=/:[0-9]+$/,C=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponent(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},F=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\bootstrap[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	197219

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\bootstrap[1].css	
Entropy (8bit):	4.968606270301307
Encrypted:	false
SSDEEP:	1536:Dyy/lspGffCWUQW8znWV64wpHeASzjN+QTzNo+xwwCrd+//zDL4iDF4j3:DxTCWUYz/wC4//zDL4iDF4r
MD5:	BC7CEA8CF9F47F4316A6D5575054EDEE
SHA1:	0A2D6B0472522B1FD04D91A3C21F5AAFCB4977F7
SHA-256:	C3E1D4D469F80D226AEFB03E3EF30C01181438F1BBA0175824DDD3FF7EE046E3
SHA-512:	B81DC287DB09636E977BE7C6D005795C5FA11085BD5C414F9AA89A1757B81BBEA20F790E2D4D8288B1642DC276FDB34E2DD0B1CFD711FFB7667C40BDADA93E7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19tracking.narrativa.com/v2/bootstrap-4.4.1-dist/css/bootstrap.css
Preview:	/*!. * Bootstrap v4.4.1 (https://getbootstrap.com/). * Copyright 2011-2019 The Bootstrap Authors. * Copyright 2011-2019 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.:root {. --blue: #007bff;. --indigo: #6610f2;. --purple: #6f42c1;. --pink: #e83e8c;. --red: #dc3545;. --orange: #fd7e14;. --yellow: #ffc107;. --green: #28a745;. --teal: #20c997;. --cyan: #17a2b8;. --white: #fff;. --gray: #6c757d;. --gray-dark: #000000;. --primary: #007bff;. --secondary: #6c757d;. --success: #28a745;. --info: #17a2b8;. --warning: #ffc107;. --danger: #dc3545;. --light: #f8f9fa;. --dark: #000000;. --breakpoint-xs: 0;. --breakpoint-sm: 576px;. --breakpoint-md: 768px;. --breakpoint-lg: 992px;. --breakpoint-xl: 1200px;. --font-family-sans-serif: -apple-system, BlinkMacSystemFont, "Segoe UI", Roboto, "Helvetica Neue", Arial, "Noto Sans", sans-serif, "Apple Color Emoji", "Segoe UI Emoji", "Segoe UI Symbol", "Noto Color Emoji";. --font-fa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	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\0MX4YUS9\elecciones-madrid-4m-en-directo-k7C--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 37x37, segment length 16, baseline, precision 8, 1024x512, frames 3
Category:	downloaded
Size (bytes):	84000
Entropy (8bit):	7.984409145884893
Encrypted:	false
SSDEEP:	1536:ul4XBHQPxuu2zK1OhXLHPQHKxEdWewAyHWlVGP5cIT8o7CPGGs336QCIZ8Qqo/Hf:ulukxz2+4JLHuOewAyHqaF8bP5s39Fq8
MD5:	CDB37453404918BC7C2D7C06961888FD
SHA1:	BA566E82B74789EAE999EB2A6F665B538F4C3FCA
SHA-256:	11BF0F344A99F0CC78D049DDD89C65090570BF989EB5E685A71DB4DDDC866C6A
SHA-512:	E2A0E0F3D0711BFA62FA5A6F98DDAA782CA5818D04BA28FDB7C5396BC3150A9E4F18BD18E58BEC24EB51CAF134DD88E412F570FADC1F47DC3F810EFE4E75633D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static4.abc.es/media/espana/2021/05/04/elecciones-madrid-4m-en-directo-k7C--1024x512@abc.jpg
Preview:	......JFIF.....%.%.....,Photoshop 3.0.8BIM.....%:.....%:.....C.....C.....".....\.....!..1A."Qa.2q#B...$3Rb....r..%4....CSt....&56DVcdsu...7Te....'8F.....6.....!1.."2A.#3Q..aq.$4BR.C.S.....?.....X.~~.X^..Q.D&|...)....N.7M.m{f>P....|z!6.....{....k...<9...7ot.XC.p..m.T0.sz.'...k..;.?a.TR{&X.c.`"..S....>c'.=..v...../.M@.H.[...nN..N..($>..:.h.....iE..[p.~.]...\w.z..N.NLn.....\Y.e....(.)g.j.....d...H..F.Q..~....y..m...g/..X.3t.4{-L.o...G..g..U&t.~....T....l.....4...i'.A.h?7T[.@>...,wSd....']..|"3..'.NxoG}..Z7...]8a.V..._.....f.R6..._..5....L../J.(.....,.X.=..Y...!X^..Y...!X^.....Y...!X^..Q...E....f....p.[...&.....)...S..1c..l.....M.K.Q.6.*X.....#..0.]8...]...N..l.7..s....9<u. .!.....x.s..\.v

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\errorPageStrings[1]	
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
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\0MX4YUS9\espana[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	168995
Entropy (8bit):	4.580986907290708
Encrypted:	false
SSDEEP:	768:Y61RgST7w7w4jf2eDnNbF5SHJeaIehcwsWD5CQIZDVeToG0I2n32+TS35UTzkbTw:eknMJh2g
MD5:	3F43AAE1AD6061F3025ABA76E93C74BC
SHA1:	862ECF61C5AE2194B10C31FC1E2068E829FAB239
SHA-256:	6BF2B2476B6AFC05EE205C67240D04EDE57009204556713E1A0BA3B68152B73A
SHA-512:	DC59E31A4C14D4B9C143472E40DE183F4044370BC2E594BF4856A1E22E6BD54948262AB80D1AB0B00D0440E985F82441D3780052F9E081D97A0CE8AB826AFAE
Malicious:	false
Reputation:	low
Preview:	[{"today_confirmeds":"120","today_deathss":"2","today_intensive_cares":"9","today_open_casess":"105","today_recovereds":"13","today_total_hospitalised_patients":"31","date":"2020-03-09","today_new_confirmeds":"28","today_new_deathss":"0","today_new_intensive_cares":"3","today_new_open_casess":"23","today_new_recovereds":"5","today_new_total_hospitalised_patientss":"15"},{"today_confirmeds":"2336","today_deathss":"34","today_intensive_cares":"110","today_open_casess":"2139","today_recovereds":"163","today_total_hospitalised_patients":"50","date":"2020-03-10","today_new_confirmeds":"746","today_new_deathss":"11","today_new_intensive_cares":"26","today_new_open_casess":"686","today_new_recovereds":"49","today_new_total_hospitalised_patientss":"19"},{"today_confirmeds":"221","today_deathss":"7","today_intensive_cares":"17","today_open_casess":"199","today_recovereds":"15","today_total_hospitalised_patients":"76","date":"2020-03-11","today_new_confirmeds":"89","today_new_deathss":"3","today

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\espana[2].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	168995
Entropy (8bit):	4.580986907290708
Encrypted:	false
SSDEEP:	768:Y61RgST7w7w4jf2eDnNbF5SHJeaIehcwsWD5CQIZDVeToG0I2n32+TS35UTzkbTw:eknMJh2g
MD5:	3F43AAE1AD6061F3025ABA76E93C74BC
SHA1:	862ECF61C5AE2194B10C31FC1E2068E829FAB239
SHA-256:	6BF2B2476B6AFC05EE205C67240D04EDE57009204556713E1A0BA3B68152B73A
SHA-512:	DC59E31A4C14D4B9C143472E40DE183F4044370BC2E594BF4856A1E22E6BD54948262AB80D1AB0B00D0440E985F82441D3780052F9E081D97A0CE8AB826AFAE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/includes/json/espana.json
Preview:	[{"today_confirmeds":"120","today_deathss":"2","today_intensive_cares":"9","today_open_casess":"105","today_recovereds":"13","today_total_hospitalised_patients":"31","date":"2020-03-09","today_new_confirmeds":"28","today_new_deathss":"0","today_new_intensive_cares":"3","today_new_open_casess":"23","today_new_recovereds":"5","today_new_total_hospitalised_patientss":"15"},{"today_confirmeds":"2336","today_deathss":"34","today_intensive_cares":"110","today_open_casess":"2139","today_recovereds":"163","today_total_hospitalised_patients":"50","date":"2020-03-10","today_new_confirmeds":"746","today_new_deathss":"11","today_new_intensive_cares":"26","today_new_open_casess":"686","today_new_recovereds":"49","today_new_total_hospitalised_patientss":"19"},{"today_confirmeds":"221","today_deathss":"7","today_intensive_cares":"17","today_open_casess":"199","today_recovereds":"15","today_total_hospitalised_patients":"76","date":"2020-03-11","today_new_confirmeds":"89","today_new_deathss":"3","today

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	210
Entropy (8bit):	5.469868473851629

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\f[1].txt	
Encrypted:	false
SSDEEP:	6:tDpuPNShL3Ml8wk3o/9N74V2jdaJaP0mjW:9pJd3wky9eedaJPmq
MD5:	3BFD0709828C21DA3DB8D1721DDF93F5
SHA1:	B028477957AF7318421EF49FD3ECA90D63C4C410
SHA-256:	1595425BC841EFBE62EC9D28A8535F0D1E70CE095C6FA6FA4953B3EC3B81010F
SHA-512:	B7AB9C34BD74093C285C93AE32BF878EC44623BA40498DD7A139424F2BE07D37290F58D1B87E7E816E42B3F9A765CB77787C10398818157AEA0C750EDCE5307
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=3308cfb7e7eaafa7-22cef212c3c700a1:T=1620135393:RT=1620135393:S=ALNI_MZvA0xUxZ4sGmu8lOwjMKzhvLszwQ","_expires_":1653831393,"_path_":"/","_domain_":"localcoronavirus.com"}]});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\f[2].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	15805
Entropy (8bit):	5.442118858633494
Encrypted:	false
SSDEEP:	384:KAkjyfwT1mb45rKe9Mk2tniGi+wn42hFah0A:2yfwT3KeYxwn42LahB
MD5:	94E9D6C8B6A1AFA3C870F0D7673F0956
SHA1:	F5C1AA68FE6E49DF85544B0652F4FB6AF3BC90C2
SHA-256:	653D929953AACFF5CEADE3EECAA393808A7AB086E8F87712FC4A5D4C0F9F178C
SHA-512:	36CCE09B281D729006A81A1B5FFF67BA613CCFFC84D360917145A1FA77DE7FBB1DD0C87FB198125FE6738FE71EFDA487992CD43B4413ECA8A2BF107C5EBDD1 32
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/pagead/js/r20210429/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\0MX4YUS9\f[3].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%3D3308cfb7e7eaafa7-22cef212c3c700a1%3AT%3D1620135393%3ART%3D1620135393%3AS%3DALNI_MZvA0xUxZ4sGmu8lOwjMKzhvLszwQ
Preview:	_gfp_s_({});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\fbevents[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	187548
Entropy (8bit):	5.392602416896564
Encrypted:	false
SSDEEP:	1536:sM+OWt6w6aic9MeipKKqQqcThe7Kdv0a9sIOC1jaMu5Qm2B+QNSMngUSZYSIlUiR:sOQMj1SVBYDGKqOQMj1SVBYDGKx
MD5:	D67E6D12EB6608E9D939B0E3EB70F7E5
SHA1:	AF4A18DD4EA23B6DF3B0092618A64A3733C2AE55
SHA-256:	8A407F25943E3E96B80C488FD36FF80000A45C9D85BAFA80E5C05890874E6695

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\fbevents[1].js	
SHA-512:	6B871EEFE532476E7FA735211C049F2CB33B684A765F5FE06F1107B0937940FCEB8FC8A71177141BDA7D6319643244B09C033F132FDF8E68D5CD4B7C39869D74
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/en_US/fbevents.js
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\fotonoticia_20210504121532_1024[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1024x1536, frames 3
Category:	downloaded
Size (bytes):	298411
Entropy (8bit):	7.979861151961286
Encrypted:	false
SSDEEP:	6144:DCJOCYzUVNkAXYb/II8ZyxlBaM/axdKZnROBY/sfc0Nj+BBjOZ:DMViMNkXjIlKWTcROG/McMj+TOZ
MD5:	E513A7641ED5A5658982F0EBA2804657
SHA1:	505ED048761136B0AAAE58DAE5B2461F7C77A22A
SHA-256:	2327EBA13E5540120D9C98F74581A8C3D5FA8CA282F1EA18D581FB99016CA07A
SHA-512:	3325C20E7AB03F74AC059CFFB7D41784438C7D6FBF168AA26BF031E615FE4B9E18C33DFE7D1022CB08B978454E4B751129330B43D1184131B60277AFD5E75BCI
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img.europapress.es/fotoweb/fotonoticia_20210504121532_1024.jpg
Preview:	......JFIF.....`.`.....Photoshop 3.0.8BIM.....h..Z...%G.....@economia bolsa ibex 35 cotiza maximos anuales busca 9000 puntos .....5.....FIN..7..20200527..<..0000 00+0000..P.!Marta Fern.ndez Jara - Europa Pr..i.zEconom.a/Bolsa.- El Ibex 35 cotiza en m.ximos anuales y busca los 9.000 puntos, con un alza del 0,9% en la media sesi.n..n..Europa Press..s..Europa Press..x..27/05/2020 Puerta de entrada al edificio de la Bolsa de Madrid, el d.a en que el Ibex 35 ampliaba sus ganancias al 2,19% en la media sesi.n de este mi.rcoles, lo que le permit.a hacerse con la cota de los 7.100 puntos en una jornada marcada de nuevo por las tensiones entre Estados Unidos y China, los planes de reapertura econ.mica de distintos pa.ses, entre ellos Espa.a, y las noticias relacionadas con posibles vacunas para el Covid-19. En Madrid (Espa.a), a 27 de mayo de 2020...ECONOMIA ..Marta Fern.ndez Jara - Europa Press.....I....."$".$.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\fotonoticia_20210504124210_1024[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1024x768, frames 3
Category:	downloaded
Size (bytes):	135924
Entropy (8bit):	7.978800297135593
Encrypted:	false
SSDEEP:	3072:M0vUDDz6pPQ7pfGaUyX5NzrMW3/VNKJ/JxoiozgRdahAt:M0vsQcGxyXbkeL8/JxoiomdeAt
MD5:	B11423B2E26746D93AD3039A238422E0
SHA1:	A0DE484AFA9FFD737FBF50FACED638E406B42F8A
SHA-256:	C823C6D030229127E5EB0992F09802C253297B3E497D255E8CC572780C476F3D
SHA-512:	24AD6068878B8C0D023FC34FAC5F20487EE5165A27C60EEB5D460443347457031F1D6A3D715F82AE1DB6615629EFC04C3753A5F0B5153FDB96AC15BE44143474
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img.europapress.es/fotoweb/fotonoticia_20210504124210_1024.jpg
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....C{....p.N>...o..I.3...>..8...<R*.0{..*]..h.?.....J..QN4m...Fx...*.pJU.qPJ....co<s...o....}om0...u.YcW.. ..+PE..._.....|.....DF....)..oc..>Y..n9.?*..5@.iljcPM...]..... R.s....x....."...\K.....XI.....%.B.....XqN..-.M.....k}...F+P....i2.@.L..Y.....[.+.6...8.....6W...Y.....J..[\.8....[..p...{....;....v..f...e6zz.(ib.....G....#..{m{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\fotonoticia_20210504125445_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, 1024x683, frames 3
Category:	downloaded
Size (bytes):	75689
Entropy (8bit):	7.963202385165171
Encrypted:	false
SSDEEP:	1536:wZGOOYShs3c5w6KLeB5nCtMT7sFAYVOxGuFiitVPO8OJ:GGwMKLI5niiwodPO8OJ
MD5:	1B15936B9CEB043670877B9115E82F68
SHA1:	F94F3A21C5676FFEAB9AE33DCD780DFE8E9FD962
SHA-256:	B18725692FA7B536729EC273601ABD9030A7CAC5F009DC825B0CE4D6B46AFF54

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\fotonoticia_20210504125445_1024[1].jpg	
SHA-512:	823A5920B99EC6EE7A59261FF805501F64D8A5F51F2969ED40E7F625B8558E3052357A7715E14D265989A79DA2AD390BD3F6FFEF7B3A8FF679036E89DFCCAEDA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img.europapress.es/fotoweb/fotonoticia_20210504125445_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..... .....?...{~Tg...!.K@.....%...>..jJQ@...E.~..%-0..o.'.....%....?*3.qIE..O..>....g..4...g..?.....>....8....'.....E..g..?..Q@..~T.....g..Q...E.....8....%-.....E...?.Q...%...>..~T.P..... (...'..'..JZ.\..(....)h.....%..g..Q..E.P.....H..?.KH.v.2.9.UQJ..^..Ui.L.j.o..<~UZ%.....gh...S..?.j..H.&..PO_.R.?.T..).@...3.o.Z.....7....J.".#*}.*@...M...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\global[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	20958
Entropy (8bit):	4.978366287319688
Encrypted:	false
SSDEEP:	192:tYWabFARMfLjICF52FckilMPI4VTYXcdKDwvhq1RjyXX+bVo5o4wIq1R+ypi/VYs:qJbvqcki+PbVTYXcAG4zyHwBDuypi/Ws
MD5:	FEAB1DC4F0DBFD3E4A6FCA334FC9F02A
SHA1:	559422BBC737F9DE66723E125B8F276C9E5FBC60
SHA-256:	32EEA542AA56D0A6FEBCE533CB08222D95EF58E75CEB89483CD028D10F2F5DA8
SHA-512:	05A1780B87A5A0EEDFE898CAF351C64036C025E1C6A6563A67FD50ED68F9C81AC9A96E4899D56AB4595B9C6A557BFA8EEB9E44A67E51E319FCE81AE75D7E0D 6B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/css/global.css
Preview:	html,body,div,span,applet,object,iframe,h1,h2,h3,h4,h5,h6,p,blockquote,pre,a,abbr,acronym,address,big,cite,code,del,dfn,em,img,ins,kbd,q,s,samp,small,strike,str ong,sub,sup,tt,var,b,u,i,center,dl,dt,dd,ol,ul,li,fieldset,form,label,legend,table,caption,tbody,tfoot,thead,tr,th,td,article,aside,canvas,details,embed,figure,figcaption,footer,he ader,hgroup,menu,nav,output,ruby,section,summary,time,mark,audio,video{margin:0;padding:0;border:0;font-size:100%;font:inherit;vertical-align:baseline}article,a side,details,figcaption,figure,footer,header,hgroup,menu,nav,section{display:block}body{line-height:1}ol,ul{list-style:none}blockquote,q{quotes:none}blockquote:before,blo ckquote:after,q:before,q:after{content:"";content:none}table{border-collapse:collapse;border-spacing:0}*,:before,:after{box-sizing:border-box;-moz-box-sizing:border-box;- webkit-box-sizing:border-box}html{-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%;font-size:100%}body{font-size:62.5%;font-family:biryani,sans-serif}h1,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\hotjar-2075733[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	3503
Entropy (8bit):	5.250665264817819
Encrypted:	false
SSDEEP:	48:81f+Bmr4DDiIr/CpDuMY6wRQAQl07k5G8r4U4R5UETledeHtwWNxsTnOf3DZ:9RPi6/snIQg24U4bU4qO0qTZ
MD5:	8418B3A731185E314FD4A47A0311501E
SHA1:	4EB2D0C19141B87844820AA07752E3D7EE873A33
SHA-256:	4FB9A7CF2C2E8538DDF3F1CB9052A4212239CC021ADD30BBCA03C3AD7FEF3343
SHA-512:	CF8A3A0824BA35C58C454E4B056DAAC0FF4B4D4D73F5D9DCCEAAE70A8D95CC27DD176EFA1596585E4F9FE44E2F33A12A8F52471B4F4C949F76BD68B9D0853 8E
Malicious:	false
Reputation:	low
Preview:	window.hjSiteSettings = window.hjSiteSettings || {"site_id":2075733,"r":0.6313131313131314,"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":fa lse,"suppress_location":false,"user_attributes_enabled":false,"legal_name":null,"privacy_policy_url":null,"deferred_page_contents":[],"record_targeting_rules":[],"feedbac k_widgets":[],"heatmaps":[],"polls":[],"integrations":{"optimizely":{"tag_recordings":false}},"features":["heatmap.continuous_capture","recordings.filter_new_user","surve y.impressions","feedback.widgetV2","feedback.full_screen_survey","settings.billing_v2","feedback.widget_telemetry"]};..!function(e){var t={};function n(o){if(t[o])return t[o].exports;var r=t[o]={i:o,l:!1,exports:{}};return e[o].call(r.exports,r,r.exports,n),r.l=!0,r.exports}n.m=e,n.c=t,n.d=function(e,t,o){n.o(e,t)||Object.defineProperty(e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\hotjar-2075733[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3504
Entropy (8bit):	5.253853668433864
Encrypted:	false
SSDEEP:	48:q1f+Bmr4DDiIr/CpDuMY6wRQAQl07k5G8r4U4R5UETledeHtwWNxsTnOf3DZ:7RPi6/snIQg24U4bU4qO0qTZ
MD5:	18813648961201589F11FBFE600760EA
SHA1:	FD0BE20C670679A820E793EFDCEDBFF0F0ADCA89
SHA-256:	4A4CF7771B4FF15FC7CD7D498521C42A7E3DE46C793B617BC98CA735C34C7F06
SHA-512:	B8D675955BA8A886698C9E1C0002754770F5A9B27A6159F99097C962F883AA451BF44BD6FED58ED700A71CE225DC079F10853A61F4E0D3A95221215AF89C0546

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\hotjar-2075733[2].js	
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":0.37555862929894185,"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(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\js[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	90459
Entropy (8bit):	5.505690028586786
Encrypted:	false
SSDEEP:	1536:Jb03wZdVQ0i+H71uo6Ni7Q3iEN2LsD8vhtqddENQuSt81z9jKPfcRQWzcLF+:Jb0gZs0943lgqnEZSt/+
MD5:	090F74C03C8526BC5926D18CE6E14F3B
SHA1:	97C7CDF1B7B7D649FFBB492F5B87AC751A0C7FD6
SHA-256:	B679ECC419C302D669CCC99B75B31C9325C49699CE46F8EE05F7568D5810A871
SHA-512:	59687FED22519EBCCBB84CAC9B95C640DB046E60AA3BDBD601BE33CCAAA17A936CF2A9E2EC020FCB60963C7C8750B00C6072FF6C6F913D0D55989FA6B9B0F75C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagmanager.com/gtag/js?id=UA-160283435-1
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"1",. . "macros":[{. "function":"__e". },{. "function":"__cid". }],. "tags":[{. "function":"__rep",. "once_per_event":true,. "vtp_containerId":["macro",1],. "tag_id":1. }],. "predicates":[{. "function":"_eq",. "arg0":["macro",0],. "arg1":"gtm.js". }],. "rules":[. [["if",0],["add",0]]],."runtime":[].....};../*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var aa,ba=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},ca=function(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:ba(a)}},da="function"==typeof Object.create?Object.create:function(a){var b=function(){};b.prototype=a;return new b},ea;.if("function"==typeof Object.setPrototypeOf)ea=Object.setPrototypeOf;else{var ia;a:{var ja={a:!0},ma={};

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\js[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	240183
Entropy (8bit):	5.543101485093977
Encrypted:	false
SSDEEP:	3072:EJZ0eK9LZk0y4K9j8EZStlG58xFKxnJZ0eK9LZk0T4K9j8EZStuG58xFKz+:KDK9XK655xFKFDK9+K65sxFKC
MD5:	8694892EA89DB83AB69348A64A4973D9
SHA1:	75494B9BCCD69FE7879CE2F77A6EE438BECA861F
SHA-256:	22D185E30B3301F35027E74F2364E66E14F017B51A006BEBD5CC34F77BC72FE3
SHA-512:	1B8A6EC64AAD559088EA00FE678003E8A1C58EB71ECD3F9563DB7D8F1D2DA1E136CBBF059AC6B3A78551D2CE265DDC05FB9260E4290B8D9B7C860FBE4114F40
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagmanager.com/gtag/js?id=G-4HNKTZ3GH8&l=dataLayer&cx=c
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"1",. . "macros":[{. "function":"__e". },{. "vtp_signal":1,. "function":"__c",. "vtp_value":1. },{. "function":"__c",. "vtp_value":"google.de". },{. "function":"__c",. "vtp_value":0. },{. "function":"__aev",. "vtp_varType":"URL",. "vtp_component":"IS_OUTBOUND",. "vtp_affiliatedDomains":["list"]. },{. "function":"__v",. "vtp_name":"gtm.triggers",. "vtp_dataLayerVersion":2,. "vtp_setDefaultValue":true,. "vtp_defaultValue":"". },{. "function":"__v",. "vtp_name":"gtm.elementId",. "vtp_dataLayerVersion":1. },{. "function":"__v",. "vtp_name":"gtm.elementClasses",. "vtp_dataLayerVersion":1. },{. "function":"__aev",. "vtp_varType":"URL",. "vtp_component":"URL_NO_FRAGMENT". },{. "function":"__aev",. "vtp_varType":"URL",.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\js[3].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	120103
Entropy (8bit):	5.54317559987937
Encrypted:	false
SSDEEP:	1536:BSJZ0eK9owZdVI0i+H7buo6Ni7QE12LsDjSdENQuSt81z9qKPfjGljAC2FSvOlHF:EJZ0eK9LZk0T4K9j8EZStuG58xFKz+
MD5:	A5E20B29C7EAB78BE337423C49FC2F37
SHA1:	0278DDB703E16703D3F225ABAA00DE7E1CF34CBD
SHA-256:	93710F11485F006CEF23AB842C27C96951C49942F6F0CD37384B785D3DEC00B8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\js[3].js	
SHA-512:	8113B5195067AB3D2866FA82A3A109C5FB9910EC7362D8C9ECA86CE7FF32BC15FBD52135A567C0A8AF9DC888C0F5F8B3ECCB1D35E445DAB7BB405F242F7064B
Malicious:	false
Reputation:	low
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"1",. . "macros":[{. "function":"__e". },{. "vtp_signal":1,. "function":"__c",. "vtp_value":1. },{. "function":"__c",. "vtp_value":"google.de". },{. "function":"__c",. "vtp_value":0. },{. "function":"__aev",. "vtp_varType":"URL",. "vtp_component":"IS_OUTBOUND",. "vtp_affiliatedDomains":["list"]. },{. "function":"__v",. "vtp_name":"gtm.triggers",. "vtp_dataLayerVersion":2,. "vtp_setDefaultValue":true,. "vtp_defaultValue":"". },{. "function":"__v",. "vtp_name":"gtm.elementId",. "vtp_dataLayerVersion":1. },{. "function":"__v",. "vtp_name":"gtm.elementClasses",. "vtp_dataLayerVersion":1. },{. "function":"__aev",. "vtp_varType":"URL",. "vtp_component":"URL_NO_FRAGMENT". },{. "function":"__aev",. "vtp_varType":"URL",.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\js[4].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	90461
Entropy (8bit):	5.505780505980878
Encrypted:	false
SSDEEP:	1536:Jb03wZdVQ0i+H7Huo6Ni7Q3iEN2LsD8vhtqddENQuSt81z9jKPfcRQWzcLF+:Jb0gZs0P43lgqnEZSt/+
MD5:	A111E7E050B63BAF155ABCE1535C8F51
SHA1:	587D20D5E7B8CF14955A470FE271043A341E8300
SHA-256:	EAF66A5FD6C0F2A2470E265F484F6644B5C6A9D290B458B83BAD185E6AE43AF2
SHA-512:	465CB96E2FAF4F8FB6A6448FF15B456BCA65C88FB83DF0981B9188B36FED6506861F02CCAB325C9B44A76DF0BDDBBD5CA4BB7AF66071D4676306CAD09CE60393
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagmanager.com/gtag/js?id=UA-60178641-2
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"1",. . "macros":[{. "function":"__e". },{. "function":"__cid". }],. "tags":[{. "function":"__rep",. "once_per_event":true,. "vtp_containerId":["macro",1],. "tag_id":1. }],. "predicates":[{. "function":"_eq",. "arg0":["macro",0],. "arg1":"gtm.js". }],. "rules":[. [["if",0],["add",0]]].},."runtime":[].....};../*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var aa,ba=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},ca=function(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:ba(a)}},da="function"==typeof Object.create?Object.create:function(a){var b=function(){};b.prototype=a;return new b},ea;.if("function"==typeof Object.setPrototypeOf)ea=Object.setPrototypeOf;else{var ia;a:{var ja={a:!0},ma={};

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\layers[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	66031
Entropy (8bit):	4.924868321474996
Encrypted:	false
SSDEEP:	384:ew45DokIn4Yb9k1pwjtoSRyrqqtXyezxfRNuqEYxVvUBAQhulzmkeHPRPF4ZD9wg:Oe8btR+jRe5b
MD5:	4A192124AB8A077D5AF731D63EF0BA88
SHA1:	11DA27D9A2FC225FC3FEF0B238F4A931451C5B9C
SHA-256:	90B749FE5655448C03FA19AEFA29DFAD2606C309DDAC206BFD9524711CAD94C2
SHA-512:	3965020D92EC43786AF5332375A6D1DBA7A6E7CB691BEC897C388147C08245193BABE4A930ABE5C97BE80CAC6504488642734D36B861D923F9796B09F14FADA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/css/layers.css
Preview:	.tp-caption.Twitter-Content a,.tp-caption.Twitter-Content a:visited{color:#0084b4!important}.tp-caption.Twitter-Content a:hover{color:#0084b4!important;text-decoration:underline!important}.tp-caption.medium_grey,.medium_grey{background-color:#888;border-style:none;border-width:0;color:#fff;font-family:Arial;font-size:20px;font-weight:700;line-height:20px;margin:0;padding:2px 4px;position:absolute;text-shadow:0 2px 5px rgba(0,0,0,.5);white-space:nowrap}.tp-caption.small_text,.small_text{border-style:none;border-width:0;color:#fff;font-family:Arial;font-size:14px;font-weight:700;line-height:20px;margin:0;position:absolute;text-shadow:0 2px 5px rgba(0,0,0,.5);white-space:nowrap}.tp-caption.medium_text,.medium_text{border-style:none;border-width:0;color:#fff;font-family:Arial;font-size:20px;font-weight:700;line-height:20px;margin:0;position:absolute;text-shadow:0 2px 5px rgba(0,0,0,.5);white-space:nowrap}.tp-caption.large_text,.large_text{border-style:none;border-width:0;color:#fff;font-fa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\o-0bIpQoyXQa2RxT7-5B6Ryxs2E_6n1iPHjc5a7dvQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 10584, version 1.1
Category:	downloaded
Size (bytes):	10584
Entropy (8bit):	7.935037651202795
Encrypted:	false
SSDEEP:	192:Mg52bOZio1sQ45gd7wyfETLnJZ5QP2xYV3j5y0KeyFxcHs0D7Uryt43yJmL:f5kOZEQ4ywxvnJZ5QPGYV1RKFxys0DQn
MD5:	51B173991712566DDB8827175A30AE34
SHA1:	C74ED180D02538DEA4B37394231B3393E16336D1
SHA-256:	376BA93837D6340723EAA6DF49EBB745508049D54506752C163CDFCF876EC6D4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\o-0bIpQoyXQa2RxT7-5B6Ryxs2E_6n1iPHjc5a7dvQ[1].woff	
SHA-512:	A4D59B6663FC5B7D407B56DD4026C138F93BD33B3251A0A8E85A595E4E1E3BA0AA901FD3F03CB56CE73F5D60B48E558E77CD3793645B30213D48A66E3D2ABC6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/catamaran/v8/o-0bIpQoyXQa2RxT7-5B6Ryxs2E_6n1iPHjc5a7dvQ.woff
Preview:	wOFF.....)X.....E.....GDEF...l...4...F....GPOS..... ... DvLuGSUB..... ... .OS/2.....O...`e...STAT...0...&...*y.h.cmap...X...^.....+.Agasp.....glyf..... k..9.9(({head..$,...6...6.#..hhea..$d.....$....hmtx..$.....!+loca..&X.....1}".maxp..(..... ....name..($.....h:.\/post..)<..... ...2prep..)P.....h...x.....@...y.....f]c..F..&.\c..Zc.q.8]....'~].!.....DFLT.....taml..tml2.....x.c`arg.....@...:H.....f8...$.....d...S..@J....(-.V.x.c`.B. f`...2.L...% &....bddHa`.,..c..x.....m.w.5f{...m.mM.m.C.|;...;.@(.E.....5....*.....l....ObB.4.=..0.q.%...."."A..N00.\ 22Sd..$.@9...N.#.q.u.|.ch..9...I`...CH...$.41G!f.1..)A.....o~..|.....<...z<..l..cO...U..].]_..kB.....t.F[l..)..... ...w.Z.l..v..U..{..@.U.Zd.%.z..[...yn.....K...k.[...:....i..^z.~.h.....d.&Z.b.a..a.6Z.l....n...i.(....\.....x..{.x..... .....eA./.4!..,B..z.-Y....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\o-0bIpQoyXQa2RxT7-5B6Ryxs2E_6n1iPPjd5a7dvQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 10920, version 1.1
Category:	downloaded
Size (bytes):	10920
Entropy (8bit):	7.934211889778374
Encrypted:	false
SSDEEP:	192:3Jg2nGmasPvuYNN4teH0eyc6nxODiNhJeONPVIEMCwRWskGX:ZgWzXJKo0eycQxr9J5MCwPX
MD5:	8E62CF3C89BED844EF728FC5598005C6
SHA1:	4C76A9FAA61FFEB966997FE9F9313CA5E437B0AA
SHA-256:	F3D34071C926C2AF63798CF5517EB2C4B49BBEDA676DEDCB1655DAF2EDE1AD21
SHA-512:	4DE7D05E38554DB32406AD61195B0A669D4CE9A47D01E1C25A80B40DCC4E510734B6AABFB112F9A378CC0ED51B7F02F4F9FD1E02F91B42C9EB0DC9C5894772D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/catamaran/v8/o-0bIpQoyXQa2RxT7-5B6Ryxs2E_6n1iPPjd5a7dvQ.woff
Preview:	wOFF.....*.....E.....GDEF...l...4...F....GPOS..... ... DvLuGSUB..... ... .OS/2.....O...`e...STAT...0...&...*y.iUcmap...X...^.....+.Agasp.....glyf.....!...9.KHz.head..%h...6...6.#..hhea..%.....$....hmtx..%.....m eloca..'.....3j$.maxp..)L..... ....name..)h...!....@.alpost..*..... ...2prep..*.....h...x.....@...y.....f]c..F..&.\c..Zc.q.8]....'~].!.....DFLT.....taml..tml2.....x.c`arg.....@...:H.....f8...$.....d...S..@J....(-.V.x.c`.B. f`...2.L...% &....bdb8....-@....x.....m.w.5f{...m.mM.m.C.|;...;.@(.E.....5....*.....l....ObB.4.=..0.q.%...."."A..N00.\ 22Sd..$.@9...N.#.q.u.|.ch..9...I`...CH...$.41G!f.1..)A.....o~..|.....<...z<..l..cO...U..].]_..kB.....t.F[l..)..... ...w.Z.l..v..U..{..@.U.Zd.%.z..[...yn.....K...k.[...:....i..^z.~.h.....d.&Z.b.a..a.6Z.l....n...i.(....\.....x..{.|.G.....d[ZI+...bZI+. .e.8..N....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\pfizer-logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	25788
Entropy (8bit):	7.969067361873914
Encrypted:	false
SSDEEP:	768:efMg5f4q+goDgHvsgWrGfl/om9gT5HQnSrNH:UMqA1gCJgWx/om9gFrNH
MD5:	498D26B6261740B6378E315CC35C4C5B
SHA1:	C56CC0FB60C886C65150F7201586F8415EBFB803
SHA-256:	ACDBB0CFE5275D71B31FF065FCDDC232DD9F26AC9C276F85733D4EAD8F0EEC5B
SHA-512:	458793234A4F57FE5661D780FB31177A6A127E911D3FB742EB1C57BE37FD24E6D3A331EA6EAE143AF4968973BC4DD95FA0A70577A6B1A1A15DFE1B5ABD26CEE6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/images/pfizer-logo.png
Preview:	.PNG.....IHDR.....\r.f....tEXtSoftware.Adobe ImageReadyq.e<....iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-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:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmpMM:OriginalDocumentID="uuid:65E6390686CF11DBA6E2D887CEACB407" xmpMM:DocumentID="xmp.did:81F2496E663D11EBACC59D179D8EB760" xmpMM:InstanceID="xmp.iid:81F2496D663D11EBACC59D179D8EB760" xmp:CreatorTool="Adobe Photoshop 22.1 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:D23EC4C6482D11EBA159B6E7412450D7" stRef:documentID="xmp.did:D23EC4C7482D11EBA159B6E7412450D7"/> <dc:title> <rdf:Alt> <rdf:li xml:lang="x-default">cen-09902-buscon14-p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\pixel[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1 x 1, 8-bit/color RGBA, non-interlaced
Category:	modified
Size (bytes):	1020
Entropy (8bit):	5.335916817166796
Encrypted:	false
SSDEEP:	24:M2s/65KXILo2s/65KXILo2s/65KXILo2s/65KXILo2s/65KXILo2s/65KXILr:W/6Ru/6Ru/6Ru/6Ru/6Ru/6Rf
MD5:	851192F1E20E124C2628B9329378A52C
SHA1:	BDCD1A79F49B52C9B531527EF79193C3E16AE5BA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\pixel[1].png	
SHA-256:	3E25E33591950CC7DCFCBAA53C6E8F6C012F3A63FEF868BE4DEEC0B0AF54873E
SHA-512:	FEDF2DFE65BA2002CFE413107E3D9D174EDC9693E76BA88920AFA959099B3D6052AA13FEEDFA78E3989788B5D1C373F077FA291327CD5AAA32E552C3754F08C 2
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`...PNG.....IHDR.....bKGD.. .....pHYs.....tIME.....-Q.7n....tEXtComment.Created with The GIMP.d%n....IDAT..c.iy.....+.....IEND.B`...PNG.....IHDR.....bKGD.....pHYs..... .....tIME.....-Q.7n....tEXtComment.Created with The GIMP.d%n....IDAT..c.iy.....+.....IEND.B`...PNG.....IHDR.....bKGD.....pHYs.....tIME.....- Q.7n....tEXtComment.Created with The GIMP.d%n....IDAT..c.iy.....+.....IEND.B`...PNG.....IHDR.....bKGD.....pHYs.....tIME.....-Q.7n....t EXtComment.Created with The GIMP.d%n....IDAT..c.iy....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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\0MX4YUS9\revolution.extension.navigation.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	22955
Entropy (8bit):	5.2395230939537685
Encrypted:	false
SSDEEP:	384:udu1VJRyVIzV2Ni4kUAtJsxwfB+icxIwpX2wgexB:ukDyVIzV2N8pvuxB
MD5:	986BCB52131428E8C489AE74ED6B3ACD
SHA1:	5B42148ACE79D164CC34F55DEBB3C9C47786B223
SHA-256:	1EC562DA78E7F254770ECE85B4433D02F035247F4C64EB51409696A56BFAD4F6
SHA-512:	A88267773C35334833F591468072F3B16B71B9400CCE4F934E96A8F2151A6535AAE63F735F2B0D2B26F57182F41E519EE1400CCFDA859DB0379B1276C42213F9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/extensions/revolution.extension.navigation.min.js
Preview:	/**********. * REVOLUTION 5.0 EXTENSION - NAVIGATION. * @version: 1.0.3 (25.09.2015). * @requires jquery.themepunch.revolution.js. * @author ThemePunch.**********/.!function(){var t=jQuery.fn.revolution,e=t.is_mobile();jQuery.extend(!0,t,{hideUnHideNav:function(t){var e= t.c.width(),i=t.navigation.arrows,a=t.navigation.bullets,n=t.navigation.thumbnails,r=t.navigation.tabs;h(i)&&y(t.c.find(".tparrows"),i.hide_under,e,i.hide_over),h(a)&&y(t .c.find(".tp-bullets"),a.hide_under,e,a.hide_over),h(n)&&y(t.c.parent().find(".tp-thumbs"),n.hide_under,e,n.hide_over),h(r)&&y(t.c.parent().find(".tp-tabs"),r.hide_under, e,r.hide_over),x(t)},resizeThumbsTabs:function(t){if(t.navigation&&t.navigation.tabs.enable||t.navigation&&t.navigation.thumbnails.enable){var e=(jQuery(window).width()-4 80)/500,i=new punchgs.TimelineLite,n=t.navigation.tabs,r=t.navigation.thumbnails;i.pause(),e=e>1?1:0>e?0:e,h(n)&&n.width>n.min_width&&a(e,i,t.c,n,t.sl

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\revolution.extension.parallax.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7952
Entropy (8bit):	5.293547913779524
Encrypted:	false
SSDEEP:	192:/C0Un9q1+1t1XYOGvIRp6yZUOZhpdyZUOkeLVpoZg/R:T1+1t1XYlv6pJbhpYGexpoq
MD5:	FBE22B59382A867C7724D896A5D8970B
SHA1:	098668D6CF4583F8F94B25BC9A14E266DCF77345

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\revolution.extension.parallax.min[1].js	
SHA-256:	756BC914C7F24DB5A3F8E3DA4CEF7C2035C92BBD2D1683D993906F66C9973A84
SHA-512:	3D03B5373882F7B97F151CB95DBAADF5DCB3B2B3407494263D94078B170FB454FC2D78A34D1F67717A6DFDB6F61EF84CC737398CC3BDC205C89E749FCE9AAC A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/extensions/revolution.extension.parallax.min.js
Preview:	/**********. * REVOLUTION 5.0 EXTENSION - PARALLAX. * @version: 1.0.5 (20.10.2015). * @requires jquery.themepunch.revolution.js. * @author ThemePunch.**********/.!function(){var e=jQuery.fn.revolution,r=e.is_mobile();jQuery.extend(!0,e,{checkForParallax:function(a,t){var o=t.parallax;return r&&"on"==o.disable_onmobile?!1:(("3D"==o.type||"3d"==o.type)&&(punchgs.TweenLite.set(t.c,{overflow:o.ddd_overflow}),punchgs.TweenLite.set(t.ul,{overflow:o.ddd_overflow}),"carousel"!=t.sliderType&&"on"==o.ddd_shadow&&(t.c.prepend(' '),punchgs.TweenLite.set(t.c.find(".dddwrappershadow"),{force3D:"auto",transformPerspective:1600,transformOrigin:"50% 50%",width:"100%",height:"100%",position:"absolute",top:0,left:0,zIndex:0})),t.li.each(function(){var e=jQuery(this);if("3D"==o.type||"3d"==o.type){e.find(".slotholder").wrapAll('<div class="dddwrapper" style="width:100%;height:100%;position:absolute;top

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\revolution.extension.slideanims.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	28147
Entropy (8bit):	5.409789576839525
Encrypted:	false
SSDEEP:	384:iF1EXOo+fkNgPwEN8v205g4f8QWwwBWCp1SjXUAgQN8yDFpkkmm:OrPwEN8ej49RjTkBm
MD5:	64D7B2C4F4E5A1E8787FB4DFB67A2085
SHA1:	E945B7335AA99F512069057D5C76835368510F96
SHA-256:	5AFCFB387C3B0E7B0D61511B722F0F5F64E7474C8D24F18E128819694395A929
SHA-512:	73437419D57D65BF38485A9B5F254BFBD6D0FAE5D27FF628F581593F249F7249C096AF445FA28418735BDE5406CF9A5491AAA015304AFA357A1B81AF2F0BD396
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/extensions/revolution.extension.slideanims.min.js
Preview:	/**********. * REVOLUTION 5.0 EXTENSION - SLIDE ANIMATIONS. * @version: 1.0.5 (20.10.2015). * @requires jquery.themepunch.revolution.js. * @author ThemePunch.**********/.!function(){var t=jQuery.fn.revolution;jQuery.extend(!0,t,{animateSlide:function(t,e,o,a,n,r,s,l,d){return i(t,e,o,a,n,r,s,l,d)}});var e=function(e,o,a,i){var n=e,r=n.find(".defaultimg"),s=n.data("zoomstart"),l=n.data("rotationstart");void 0!=r.data("currotate")&&(l=r.data("currotate")),void 0!=r.data("curscale")&&"box"==i?s=100*r.data("curscale"):void 0!=r.data("curscale")&&(s=r.data("curscale")),t.slotSize(r,o);var d=r.attr("src"),h=r.css("backgroundColor"),f=o.width,c=o.height,p=r.data("fxof"),u=0;"on"==o.autoHeight&&(c=o.c.height()),void 0==p&&(p=0);var g=0,w=r.data("bgfit"),v=r.data("bgrepeat"),m=r.data("bgposition");switch(void 0==w&&(w="cover"),void 0==v&&(v="no-repeat"),void 0==m&&(m="center center"),i){case"box":var x=0,y=0,T=0;if(x=o.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\rx_lidar[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	118639
Entropy (8bit):	5.333005082342983
Encrypted:	false
SSDEEP:	1536:vxtZwQQxoH2h4SKA/WQwSnqewOd1O0g6r94MgIPIq6O5tKuPeLQ/GcREJOeaE:qFE2h7uQqxMgYRPEAGEEknE
MD5:	AD77444381CE4D823282B3141F8B33FC
SHA1:	1193F1F29F6C9E54F272BA6471E0909035C3DD57
SHA-256:	BDAA38F52441BF7AF0793FBF059E5598FFD9D18FA264B14BD55F6B3655FCC958
SHA-512:	11567784AA51D7BA055BDDCC7ECBF8FC027209C26D76627E2BAFB05426BB1203E6A0228BEC6F62ACDC656B5DD7421194118B190FE51D54CC15D799241951A4 E
Malicious:	false
Reputation:	low
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n,ba=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},da="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a},ea=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("a");},p=ea(this),.t=function(a,b){if(b)a:{var c=p;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&da(c,a,{configurable:!0,writable:!0,value:b})}};.t("Symbol",function(a){if(a)return a;var b=function(f,h){this.sd=f;da(this,"description",{configurable:!0,writable:!0,value:h})};b.prototype.toString=function(){return this.sd};var c="

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\sdasdasd[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):	102508
Entropy (8bit):	7.968060992134895
Encrypted:	false
SSDEEP:	3072:jTMJeP+E2tFBVFElq6cRM2o0ClrG13sW/3h9RQzf2sR3usO:jlJeP+EYcqhyGxsYnQbFR3usO
MD5:	5F70284CD396437876B9001BA71FFEC1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\sdasdasd[1].jpg	
SHA1:	88881FAC450B53F0133545F4D090E91708ABD2ED
SHA-256:	55B2F0EA69D2C0DE956FC69F37EBBB5CC0FCCDE56FB8EAC9299E6D31BE0880BA
SHA-512:	3EA0CE9E7188D80D799FEA4C5D7BDF75A59AF7EFCD3C795977482F034F6C9DE9B7229D8877B50BB1285ABDC04E4CB6113E68DD312258A5FB39F41A7AC3ED8 1D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.lavozdegalicia.es/default/2021/04/14/00121618431541670624319/Foto/sdasdasd.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.....(...(((((((

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\teruel_buj-k0zG--1024x512@abc[1].jpg	
Reputation:	low
IE Cache URL:	http://https://static1.abc.es/media/espana/2021/05/04/teruel_buj-k0zG--1024x512@abc.JPG
Preview:	......JFIF.....4.4.....,Photoshop 3.0.8BIM.....4.....4.....C.....C....."..... .....Q.....!.1."AQ..aq2...#BR..3b..$CTr...4...%DSc..s..&'56Edt.....1.....!1.."A.2Q.#3aB.$q..C.....?.o]u4...H5..@*..B.. ..G;.C.....*.Q.3RDX.\m.5...HY.b..i.c.VN3RC....$...\85i .%....<.!*1e%i..{T.B...9g..*'..y3J8'.o..G..=y..*..!.}.4.J.#..=..)..... ...hi4...P. ..M!..Q.\R`.h....n..9....;;sH@.IU....:.z U....`.1*.8..b...Fk.i.0*....]H. ..$../mt.R".....m.B...%I*.....1.....x....lw..?.K.U.....8Uh[.D..k.*...S.....N..|..7...L..qd.k...c.K..N)$...j....5HN3l..&?3K$/.b..J[Z...(p.7.Ez....F&..%Ra..${.*..t. (aB.C.....&..!.M`.....f..1.{..B.}(.....#....\O.....HR...aJ.":.....&..5G/.....=...)..b0h.A....0.x.IIzZP;...|..L:~.....4Q..}.#.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\vacunacion-espana[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, 1000x667, frames 3
Category:	downloaded
Size (bytes):	82833
Entropy (8bit):	7.980913820098235
Encrypted:	false
SSDEEP:	1536:SWYkiQ5kWK3M66yghL0/K/2iee/6HWANnBAC0xFylFlnmiCDJgUbJsy0:SAIc66XF/2ieuW1NBAC0xcLZmi87bJu
MD5:	3F96E2906B4108AF9F34A06D995DD05E
SHA1:	5667FA5C1CF81F199C7DE12F8415926D4353F4DE
SHA-256:	DB3D1F59D7B943F972EE5B03F8FC887ED74CC481CF631D05005E084A8CD38401
SHA-512:	5619A750C56D56C086D47FEEFC2399CC01C025787246F6A10F4D2948830A2CB3D6AE55FD48B3008323C74DDC594D79D70C4022748DEE01E09A31935F45B0DA6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.republica.com/wp-content/uploads/2021/04/vacunacion-espana.jpg
Preview:	......JFIF.....,.....Photoshop 3.0.8BIM.....04.....ESPA.A CORONAVIRUS PANDEMIA.....4.....SYS..7..20210425.....Sanidad..<..000000+0000..P..Carlos Barba..U....Z. .Almer.a.._..Almer.a..e..Espa.a..g..GRAF1874..i..Vacunaci.n en Almer.a..n..EFE..s..EFE..x..GRAF1871. ALMER.A (ESPA.A), 25/04/2021.- Una enfermera pone la vacuna de Janssen a una mujer en el punto de vacunacion masiva en el Palacio de los Juegos del Mediterr.neo de Almer.a, donde se est. suministrando la vacuna de la es tadounidense Johnson&Johnson a las personas de 70 a.os y que se suma a las vacunas de Pfizer y Moderna y AstraZeneca con las que se contin.a vacunando a los dis tintos grupos de edad. EFE / Carlos Barba....z..CB..(.....spa....C.....".....)..."1+320+/.6<MB69I:./C\DIPRWWW4A_f^TeMUWS...C.....'..'S7/7SSSSSSSS SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS.....".....Q.....!.1AQ."aq..2R.....#34Bbr..$s.....5CSc..DT%....&6d.E..t..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\zYXgKVElMYYaJe8bpLHnCwDKhdHeEw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22620, version 1.1
Category:	downloaded
Size (bytes):	22620
Entropy (8bit):	7.9761014161385395
Encrypted:	false
SSDEEP:	384:2VQcYOB3hkUVFLXB9e+TBzbgby0n2u86NWx754v9PIU4t7uSzOS2xC9Jrmj+lGzI:2VQcYOBpVtXB9e+T2OMw6NWx754VgfbH
MD5:	A2C56F946488A9A267BA6BA21471A217
SHA1:	05124DD70199CD052531A4FDF3FEFC34B99D6AB4
SHA-256:	ED561C5D042D08481AF8CB1D52EF6B0365FF6B982F17983CC0E0778C1611AFC1
SHA-512:	E242BE2965AB97080EFC258D5FC6E440FA8ACAF0DFC1E2449AAA13E2997ECED0673918E0AC75738B30DDAC595D30DC9DB77CAC167893B5FD96C54064F4405 82
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/ibmplexsans/v8/zYXgKVElMYYaJe8bpLHnCwDKhdHeEw.woff
Preview:	wOFF.....X\.....GDEF.....9...@....GPOS.....56.n*.GSUB.....>.,GOS/2.....Y...`i. ecmap.....?.=.cvt .....>...>..m..fpgm.....s.Y.7gasp..... ...!glyf.....:d..~.....head..P8...6...6.*.ohhea..Pp.....$....hmtx..P.....';oloca..R.....v,..maxp..T.... .. ....name..T.....p.F8.post..Ux.....5.=..prep..Wp.....x.....@....O..u ..@.Ah....n.....P.&U,V.....K.....I...;...x.d...Q.E.:..b..Q.ll.?.ylc.m.....P....#....0....Yy..[l.}..]. ...(..j....Dn]yx..c.P...@.hw.....o.pQ{...S1.A.....0}.\...f.....L...Z.....i.)W..... a.#u.E{. ..0_.....)...k...r..[....6...c.j{n{m.....sQ..`.s..".....b5...F...mlg.;...r./.....u.q..|.3..$.x.H$..RI#....&.\...".)..2...*...:..k... ..c.33....}8}.....p.&.4af..|.`f..xu.T....O.U/.1.a.b..T.9^.+q...g...\. .....d..S.X'f..B\.E..Q.f.@Kv;.=:r....}v...F.....f.....*.U..:..Y.....u.7`A.%<.}K.X.....2*.....s]\aw.n..q.uw.j..%.(.....4..T:.mk.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\zrt_lookup[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10289
Entropy (8bit):	5.476565958835486
Encrypted:	false
SSDEEP:	192:28d3tZlVcwxkGOxn/CP00/Y7CPcy4j18a2fDaIT7E:2ktpY6PT0CPcF132fDaITA
MD5:	063C53466924D2BD0F9A0D57F098A66B
SHA1:	0F3F95456E019D0F958C1103E61B71A1097D1F49
SHA-256:	A5CB642EF22434A24612329870579FBB272CB9FA7475360035596EA56FB0431A
SHA-512:	1B24A9AA3A7B1E08D45E2DA9E34059DBA2E2AEF3A59F14DC1214BFAF72E4C138EEC81ACD38FF6480EE944055629BBC194D1923C5E497AF4F183FBDBE52CA7 53
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\zrt_lookup[1].htm	
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/html/r20210429/r20190131/zrt_lookup.html
Preview:	<!DOCTYPE html><html><head></head><body><script>.(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var aa="functio n"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};function ba(a){a=["obj ect"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var ca=ba(this);.function da(a,b){if(b)a:{var c=ca;a=a.split(".");for(var d=0;d<a.length-1;d++) {var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&aa(c,a,{configurable:!0,writable:!0,value:b})}}da("Array.prototype.find",function(a){return a?a:function(b,c){a:{var d=this;d instanceof String&&(d=String(d));for(var e=d.length,f=0;f<e;f++){var g=d[f];if(b.call(c,g,f,d)){b=g;break a}}b=void 0}return

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\1200x630BN[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=12, height=630, bps=0, PhotometricIntepretation=RGB, orientation=upper-left, width=1200], baseline, precision 8, 1200x630, frames 1
Category:	downloaded
Size (bytes):	457948
Entropy (8bit):	7.932228054155957
Encrypted:	false
SSDEEP:	12288:3+hT3fHNQAqaI9W/7rxRYD9nJCL8q/lnHqQRMXPnEi:Q7mjKwD94LX/lnHd0/Ei
MD5:	60F4A01053DB8D4BF08CE629D8046A7F
SHA1:	445C3B802A6BF8A9ECAD3AAF80AC5117D26807E5
SHA-256:	AD15A99A52ED9DA7DD708B15B5061F6A8F5362A51870AB2179277BE8276833B8
SHA-512:	2143E049AFA0C22A120CD02D185FC73983B54A1393F4B269DEB8ADEF2FA44ECD454FCB5FD711F6E737502FA7346AF1C0D949AC645618FD935E982E63AEAFFD 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.jornada.com.mx/imagemeta/1200x630BN.jpg
Preview:	....%.Exif..MM.*.....v.....(.....1..... .....2.....i..... .....B@..'...B@..'.Adobe Photoshop CS6 (Macintos h).2018:04:05 19:29:48.....0221.....v.....n.....v.(.....~.....$.....H.....H.....XICC_PROFILE.....HLino....mntrRGB XYZ .....1..acspMSFT....IEC sRGB.....-HP .....cprt...P...3desc.....lwtpt.....bkpt.....rXYZ.....gXYZ...,....bXYZ...@....dmnd...T... pdmdd.....vued...L....view.....$lumi.....meas.....$tech...0....rTRC...<....gTRC...<....bTRC...<....text....Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IE C61966-2.1.....sRGB IEC61966-2.1.....XYZ .....Q.....XYZ .....XYZ .....o...8.....XYZ .....b.....XYZ .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\2021011813310867262[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, 1010x568, frames 3
Category:	downloaded
Size (bytes):	41959
Entropy (8bit):	7.950230199389035
Encrypted:	false
SSDEEP:	768:LcG8p7dTilgu6JRrAW8ejyBBK/vjVXZXNwk3p5YYU8fetq2UJCy3rA+1QC9qp2:LclJu6fvjaBKrNwaEimt8JC4h1QC3
MD5:	D63283CAC06D6569E54DF7C6FE04313E
SHA1:	FE0D78F65E0919EEDD509930ECCC1557F08F30BB
SHA-256:	60CF5311F91EBEF76963414E9F4E501EA9B60029240E2CC9D146998E50D7E8D7
SHA-512:	3846B680BA24A1CB1D71A3192072AAD645BDD791622D692E984A6B5EFD6DB8FB0C02B9E5018D34052D5509493A7999F66C3A5C33A3C5D1C4D9FA424BDBDA73 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://navarra.elespanol.com/media/navarra/images/2021/01/18/2021011813310867262.jpg
Preview:	.....JFIF.....".."..8.....m...1....`..E\..c.c.....x.. .6..!....\Rn$.-=.s.i%.m....1.....O6....6....1...^m.,..[....Td.u....r.....+..m...`.....C.nB.....0....(...=D9<...m*...D..[..{y!...m.....`....m.....!.Q+rn...`.\...!S...4.v.....t..cc.....`.s .m...NVG.e..m...`..q.?j.%~...0N.8..U.g.Nj.....B.M..m.....C.7...::Z.]==]=.`..6....3..$.....c.L'(U...UnEu....t4t.m....c.....+..t.y..FWi.....G.. `.cd9..-.....On..9..#.sWd.#\lU.k.W. .]..m.....|.(.>t{s.{...M7.._bM....<.W/...{.w?V..|Nw>.....U...k,4w..`.....cc.0.0.....,_..MD.e...w...[...n.....6....98s...uF.k....o=.V.....]..m.....0.....x9.3....5.p..sJ.p.....`.6....:z..SY.. .Y+.W.S...Y..d.z?..|..cm.....`0....s..O.].-...7....{Og.C.....j..U...;.D*..Y....L.Jr.....lm..c.0.....0.?!.rN.V.;..U..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\2076313506083323656[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, 600x500, frames 3
Category:	downloaded
Size (bytes):	35758
Entropy (8bit):	7.902156040633782
Encrypted:	false
SSDEEP:	768:4gbPZW6i6YgBTwCFewMravfrOjFofFppa6/oXfSG6kWlQilh:Bba6YgvFAGvTOBofLpacovRAld
MD5:	8A7A5913679814B3B2C3C9BA376B19BF
SHA1:	AB2F5E129B8CC1946901AF47D417C787E742E77C
SHA-256:	A588E5276AF3C32060A5D442AB438B640B0F652763D785A8112B255908BD4078
SHA-512:	C12CEB89CDB8949C862E6613A8E0F8C05C6A7525159DF00BE429175ACEF295D0791F355E395CA29CB35B047ED4F55BEE9D5C154F0DF5579B6F8C7A5BE18D7E D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\2076313506083323656[1].jpg	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/13303269023874708913/2076313506083323656
Preview:	......JFIF.....C.....!......"$".$.....C.....X.."..... `.....!1.AQ."aq. 2..#8BRu...37Vbr.....$Ct....4Ssv.....6D.%'9Gce.....9.....!1AQ.a."q.....2..#B.R.$4r.....?..H..... .....{...1.i..w.+..&....Wn..k.]..Z)..f..$.....:.-.=.ACQz..g.V.q.~...;~..F..4.&WG..@.s.-w.C..V..ut.m..Cj...\..E%-}.$},.<.i{y.y.)oox... t[...*.g..u.*jKk*.m.%,,. (a..@.....-.....d.....Zl.3V.K.c.yy.O@..8.cU...BS...MW<.^.....G.y.#,...##.....N..c...xD~t.v.E:....9.;O...zF.r...)...o...O.3.....e.....,0...SFK.!.....=U..]..z3P:.,. .*...".7..z..2.y.....l..OEx....9..5..c.....X...,E7.S.'..>~....n..W..o?(.+*..I.'{c.(.=..4.2J.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\840_560[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, progressive, precision 8, 840x560, frames 3
Category:	downloaded
Size (bytes):	89263
Entropy (8bit):	7.9895783559235936
Encrypted:	false
SSDEEP:	1536:IBecNNW+I/DFVNQRnVE3ED0yArjnMhFXu4pDj+hEcohHdP4zyWjvKfNaKYWT:AecTW+IbFVNQZVKLyCM64YEcoIhsYe
MD5:	BEF6B1DE18CE8E403B78147B8176DCAE
SHA1:	72873BA4197CBBC399887CC056B866C837D6A4AE
SHA-256:	98944382D225D3FB2EC8E8D5C3247B2A74C04550BB5F66EE97EF7E7D60F2A922
SHA-512:	693F2617672C599F18EAAEACB08A534343888579D87883B99910760E9CD3562B0D91EA81E6208D154C8FCCF02E20FAC30C4B077FAC8E8ADB55263EFB693A2E0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://i.blogs.es/3d0f69/peugeot-concesionario-/840_560.jpeg
Preview:	......JFIF.....`.`.....C.....C.....0.H.."..... @@......C$.P...Af...c,.m..X6..#.&eam!.KV,*...~..M=4..m..6...L.!. .a$..I .o.4O.2.|..V..Pj ..GC.c)t...E...(.Hb.D..erl%M.Bh...B...%.D....&@0.D.I@H...$.$.p@.Z...=...4O.F#:..@`.. .I.&.2p.>..\...-r.N.-.. D`.!J.C...CaKZ.[..T.9....8.(`>...E0..LC#.....S).fI.B&'f.x.....r.r.T....D.FL .A.`q.JmG7.Q.)-F.#.L..A.4.Xcd.9A(.HY\$.T.(.HY.....~'...xF.6..4.K.;....d.L>.K. rC N.D.....&.M...h.. ..M.V.U..]*;.ff...$..R..(..<Ld.!4.....h.....7i._.0O..C.b.a.....P....a.... ....Q.r.<.`<T2..J.....J@.>.U{.g...#IP.k..$0.R\q..Y.y7....0m...a. ..0.)...Z\....V.s}i.D..d..l:.....R.. ...5-I.,.<....M.iM,.@.RLaN.G-.F...HJi.*&...E.@i)Zi!.....^E..J.-.nc...c$.d.@...I.tT...B.y..P..k?-)g={.u/..w..{.....F.ta.U...n.6.>#...@)m$sE{.,.0u.1).....(.$

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\840_560[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 144x144, segment length 16, progressive, precision 8, 840x560, frames 3
Category:	downloaded
Size (bytes):	99273
Entropy (8bit):	7.983696126011376
Encrypted:	false
SSDEEP:	3072:ab4RhkZXccjnXooXFiOieD4666rjz7W5wufBfFIGkfo:s4bKcm1XFQeD4666rPKVfx
MD5:	4148E928A98BE417C2E498E5897316C7
SHA1:	7066940674BF76C8BCE77E0A1F39033B0BFF1449
SHA-256:	A87979776C0D624233F8D1CDD4DF2F9857B1BCD9B7EBC520C12FE1D0AEF0C31E
SHA-512:	D809F9D0E31C1B7E551B35588E9FDD10F8B7B91ABF1B73505861B87CF5C8B96B0FC09AD0DD875C45F9E4E71CDFDB50CB07726B4197449A4E010AC76C369343 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://i.blogs.es/9fbb30/aforo-ios/840_560.jpg
Preview:	......JFIF.....C.....C.....0.H.."..... q)...N..S.q.....\.3.x..0]zRjKm.s'.H.....AI?J...':Or.)\.ILd..k%.S.q..\E:..N..S..B..s....%1...J,-.J.....J.Wl0.t.....t..K...\.8..N..S.q..\E9..)..1L`.RS..... .E."....0.E..."{N.V..&!.g....4.} .XO .....H!...2.C7.t x....N-.L.p.v.D-..t.0.U.....y.4R..XP.r..... ....l!.....S(Gi.C...%.....T....m.L#...*..i... .T.."....n.D[.Q..TJ-Pi...[=.0Hn.<nH(.F..W.....H.....<#>....I.....5...K...C.. ..^..`..`..`....K3.n/.i.....q#...X.4..$.....J..a.#.'zB.Ka.4.-P..t*"....B.-..t*"...]..... (.<..4.....d....A.<=. ....W.PX.ugjA8.....ik....~.F... .y....X.....^.....h....q.r.!.;...|@..J.. p$.....).Q]X.....J..c.r8=)#..2.@.=.(....}.....#....p....a5t...D.'[...E....p....y...}...Mg...hU..0.....6.b

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
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\2K7JPOQS\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.....(...((((((

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\a204a622610ec42c29322584ae03f5a9[1].js	
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};.function ca(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var l=ca(this);function da(a,b){if(b)a:{var c=l;a=a.split(".");for(var e=0;e<a.length-1;e++){var k=a[e];if(!(k in c))break a;c=c[k]}a=a[a.length-1];e=c[a];b=b(e);b!=e&&null!=b&&ba(c,a,{configurable:!0,writable:!0,value:b})}}.function n(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:aa(a)}}var ea="function"==typeof Objec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\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):	83343
Entropy (8bit):	6.0744526197642035
Encrypted:	false
SSDEEP:	1536:wcrhOpRoDGEhnYvaXxzBVuCDxeSCpCyED:wcrhJG4nYvQibS+yD
MD5:	90B1D58FCE6F4845AE6C3AE5E7A95200
SHA1:	1199EFAA81AA365417B7F4AA5542C0A35BDB96DC
SHA-256:	09FC211D659394594FFB8E1CD9106916B918ED2BB5130033174A6F141B69C851
SHA-512:	0FCEE34E5BD9F736AFF112CF8DD00600560E3EE9FCFF07C6EA0A263E40E58ADC0D0B2AAA4DEBE30106E1C3244B8EB542203BF0D1AD03A3FABD4E616545414AB6
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=1620167879&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&dt=1620167878401&bpp=7&bdt=6689&idt=7&shv=r20210429&cbv=%2Fr20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D3308cfb7e7eaafa7-22cef212c3c700a1%3AT%3D1620135393%3ART%3D1620135393%3AS%3DALNI_MZvA0xUxZ4sGmu8lOwjMKzhvLszwQ&prev_fmts=0x0%2C1280x906%2C379x280%2C263x600%2C263x600%2C263x600%2C263x600&nras=7&correlator=2496065476927&frm=20&pv=1&ga_vid=1286235738.1620167791&ga_sid=1620167875&ga_hid=1189571962&ga_fc=0&u_tz=-420&u_his=8&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=3785&biw=1280&bih=906&scr_x=0&scr_y=0&eid=42530672%2C31060956&oid=3&pvsid=3915826362476766&pem=123&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=7&uci=a!7&btvi=5&xpc=9T8pnLn8uZ&p=https%3A//localcoronavirus.com&dtd=793
Preview:	<!DOCTYPE html><html lang=fr><head><meta charset="UTF-8"><link rel="preload" href="https://www.gstatic.com/mysidia/a204a622610ec42c29322584ae03f5a9.js?tag=client_fast_engine" as="script"><script>var jscVersion = 'r20210429';</script><script>var google_casm=[];</script><script src="https://www.gstatic.com/mysidia/f27a2327937451811f326a3c5359709a.js?tag=pingback"></script><script>mys.pingback.init("COmfnv6SsPACFS7XEQgdfNQO5Q", [4,1],"scream/throne_image_och",{2:"server",1:"squareThroneWithoutBody",4:"mysidia_upscale,mysidia_analytics"},17);</script><style>HTML,BODY{height:100%;width:100%;margin:0;padding:0;overflow:hidden;}#mys-wrapper{height:100%;width:100%;overflow:hidden;position:absolute;top:0;left:0;align-items:center;display:flex;justify-content:center;line-height:normal;}#mys-overlay{height:100%;width:100%;overflow:hidden;position:absolute;top:0;left:0;box-sizing:border-box;pointer-events:none;z-index:1;border:1px solid #E5E5E5;;}.mys-wrapper A,.mys-wrapper A:visited,.mys-wrapper

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\api[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	850
Entropy (8bit):	5.529053739897451
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAv+KVCetTS1J6MsLqo40RWUnYN:VKEctKoeVS1YLrwUnG
MD5:	0B846E2C5285567AAAE5D0845E6E859B
SHA1:	A8D736348C32C48FCE73B2B2D01BE47957D6F9B1
SHA-256:	F26E4FF4EE18BF6300053A746E3557F8C07827B96C787F9927463CD6AE13E339
SHA-512:	74C92AAFF77F459D38517C1BE20C040B137FD40A9502A43A5706ABCD4A66DF4BA10B53440B003CA99A7E9FC52658AE952047F2680E2EF208091F783BF8657941
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/recaptcha/api.js
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('onload');w['___google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po.async=true;po.src='https://www.gstatic.com/recaptcha/releases/9qx0v7NiOAe_XnW_ULNZm9e3/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-3Y6TtXVyVz4uYxLkZdls2QB6LJNCm3B8Xng6ivLc8XwXOrNl1KhXyQFv5TJ+lsJr';var e=d.querySelector('script[nonce]'),n=e&&(e['nonce']||e.getAttribute('nonce'));if(n){po.setAttribute('nonce',n);}var s=d.getElementsByTagName('script')[0];s.parentNode.insertBefore(po, s);})();

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\appliedxlabs[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 434 x 94, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	5166
Entropy (8bit):	7.93670411135492

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\appliedxlabs[1].png	
Encrypted:	false
SSDEEP:	96:lmoxOVqvqZEpVxMb+usZAjuN43ezhs45Y1xBrtdiYJ9GF0:UoMVp4ry9sOjuu3Whs4Y7rtAIo6
MD5:	A88F34C9DB3A05836B3333237CED76A0
SHA1:	18719E3278BED9697F31D9ECF4100A5C3EF9B12A
SHA-256:	898411BB4B36A617F31FB304C99BEE6FC8E43CB2E4EAF68DDDB536A092AA13AC
SHA-512:	72C666A00BBECFE69C7F1D3AE48EF4C1F8F8121F76A1262EB4DA9214E5CC22D1E4D6A941AFB4705DB2E40F1B5F265CA73CE99F385CDF91BFAC3EF09171EA1(94
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19tracking.narrativa.com/img/appliedxlabs.png
Preview:	.PNG.....IHDR.....^.....Y.....bKGD.....pHYs.....B(.x....tIME.....1x.....IDATx..i`....5....L....(.\.Q.#.l"...A."n\.....!I.6.A...W/....@....v..P.z....[!.!...!.5.I.L.t'....KUu..e.t..:U. 0..0..0..0..0..0..0..0..0..0..0..0..0..0...a>+5..2rV.w.gj."..a.8oR..I8.#.).....jp.(..5Q;....{..m.+.fp.]A$D..O...P.l.o..P.9jka.'..U{.....|...s.....=.....j]9..v.xr.....N..=...W....< ..]..O...P.4(.;F.q....c....5xCl7!.....s.r....A5...b.s.A...:..4.\<.0..qE..W.C.a..#v*Yz..kD..!..%..==...*.....w...j0S....E.(...b.....~.|).q.....^.O...v.J..9.....D....$,.....a..Gu.....) RA..+f.4P..xSF..._.l3.z.T."A..G.Ea.mM.`R]..l6T1..{...JF..B.`.....E....j\"&~...w..F.q....!..J.}=,E.i....V.C.}.b1.6.pLI..<..[.V..}.....f..a.....w...t....v..Zh..d.XZ).3%..>.....3.uQ)C.>6L/ .A.Qd.....u.....v.:...m...K..@w..h..3...uJ.._.}.N.0.-....X\C...g..){.....)#.=.q.Y...S.C.. ..A';..>....0?.^'&.....6.....#u..a.nQ#/..s.)Y.x.....-1.c....j...!.B]8e.g+.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\astrazeneca-logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	10001
Entropy (8bit):	7.779400780780817
Encrypted:	false
SSDEEP:	192:E7F8knPEFkvvoeg3yj8lLkDaZkHyUTo6Py70jbgpKlDFyWjKjiFc:ENnP2WvBg3qSa+HFToiyQngQ7yWBc
MD5:	0EB50965A6EBF1A9DD33A20B07D53A49
SHA1:	B167501DA81B727AB866D26D7DA9E5CF2705A478
SHA-256:	24CF03363F105E60BF5B33BB9A6CBD809A20DB931D37510AB76EE25839E66C34
SHA-512:	7CCFCE4302958DBA617FCF628CA8D6F308CBB910DD43A601A2A825E8B1D112899FD73D812EEB99E6650EE74AD545826800DD1DD697DAF212296E76658D269C 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/images/astrazeneca-logo.png
Preview:	.PNG.....IHDR.....\r.f....pHYs.....g..R....iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adob e: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:Des cription rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#" xmlns:tiff="http://ns.adobe.com/tiff/1.0/" xmlns:ex if="http://ns.adobe.com/exif/1.0/" xmp:CreatorTool="Adobe Photoshop CC 2015.5 (Macintosh)" xmp:CreateDate="2016-10-27T10:24:14-07:00" xmp:ModifyDate="2021-02- 22T16:00:26+01:00" xmp:MetadataDate="2021-02-22T16:00:26+01:00" dc:format="image/png" photoshop:ColorMode="3" photoshop:ICCProfile="sRGB IEC61966-2.1" x mpMM:InstanceID="xmp.iid:00f58b47-cedc-f04d-8534

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\be158c80b2e94820893d17974baead9f[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, progressive, precision 8, 600x315, frames 3
Category:	downloaded
Size (bytes):	29100
Entropy (8bit):	7.974147390316368
Encrypted:	false
SSDEEP:	768:pAUagw/TKn/VmMqZT7RjG5+HOWjwcQvCUWeQS37dZ/lv:pAMw/TKndmMqtdM+uIRUxZ/J
MD5:	9F33A84821FA9212A182070F2707363D
SHA1:	670B75EC32413479A413853F9B50A7D68DF269D9
SHA-256:	7673CD64EBA5E5EC96F3AE59092013DD9D5D5D3E0DE4AF711A030F2F98E3663B
SHA-512:	B8BB8D865E72D9CBCAECB4F39145E3724DC459E00B72B2E364BB0E1A89152E0DEBA5A15311C143E97E7BDE1E486B45A82D7739F343AD13BF6B11BA6E40B99F E6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.ecestaticos.com/imagestatic/clipping/be1/58c/be158c80b2e94820893d17974baead9f.jpg
Preview:	.....JFIF.....,.....C.....#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C.....;("(;;;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\bootstrap[1].css	
Entropy (8bit):	5.093960028699236
Encrypted:	false
SSDEEP:	768:8sBGxw/wIHoS1LFN4vI6kHrviqbeoCk1NtFbdbHVO3+++vhuip3X22q0QmNaO:ww/nhOI6kHrviqIk3JVXB31V
MD5:	C5EC3E8CC0623722678112FAC229B8C8
SHA1:	AE1075BF5F15A8D794848FB974074227223A520D
SHA-256:	5F8DC136DA36D63CC6F9CAC536FDB5CB3B64B25C81269604B708E61A55FC8C6E
SHA-512:	CDB08C1EDC36C0C456D067FA6FBFBC5AC14D7FF85AE9BAA6D8A8E678D65AFD4B80BAC857C2553BEA63B691C0E018C220C179AD760E0C181A52E2CF9C7611C04
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/css/bootstrap.css
Preview:	/*!* Bootstrap v3.3.5 (http://getbootstrap.com).* Copyright 2011-2015 Twitter, Inc..* Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE) *//*!normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css*/html{font-family:sans-serif;-webkit-text-size-adjust:100%;-ms-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{margin:.67em 0;font-size:2em}mark{color:#000;background:#ff0}small{font-size:80%}sub,sup{position:relative;font-size:75%;line-height:0;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{height:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\box-5e3cec51ed8e99df6977c199d27812d7[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1514
Entropy (8bit):	5.492829226473901
Encrypted:	false
SSDEEP:	24:h+vFgj+AvQq9FkTqpNoVN96970UF2RS0GViso3RTsn4JRJ6MshCgrX4Nu:a1Ad8OpNgNAuUF2RtLR1Q4JRJChCgroU
MD5:	5E3CEC51ED8E99DF6977C199D27812D7
SHA1:	5547262C1169562043B7DC06A80FD832768726A1
SHA-256:	486762D56893F9B12FDFAD41C3A76F11FC745B5436E97E596A63C22EE13D2E33
SHA-512:	4ED903305DAA06CB822DC99636AF78E97A64A6339EE069C829F28DD1B77768FDA6783D3D46D91A97FDB30B4C3DFFB3C0704D17100ED38D28BF0F9255CDED56F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://vars.hotjar.com/box-5e3cec51ed8e99df6977c199d27812d7.html
Preview:	<!DOCTYPE html>..<html lang="en">.<head>.<meta charset="utf-8"/>.<script>(function(){function f(a){try{var b=JSON.parse(a.data);b.key&&g[b.key]&&g[b.key].parseCommand(b,a.origin)}catch(d){return null}}var p;try{p={cookie:{get:function(a){return(a=RegExp("(?:^|;)"+a+"=([^;]*)").exec(document.cookie))?a[1]:void 0},set:function(a,b,d,h){a=[a+"="+b,"path=/","expires="+d.toUTCString().concat(h||[]).join("; ");document.cookie=a},remove:function(a){document.cookie=a+"=; expires=Tue, 13 Mar 1979 00:00:00 UTC; path=/;"}}}catch(u){return}var g={_hjOptOut:new function(a,b,d,h,.f){this.parseCommand=function(c,g){function q(){var a=JSON.stringify({messageId:r,value:k||1});window.parent.postMessage(a,"*")}var l=p[a],m=c.action,n=c.key,r=c.messageId,e=c.siteId,e=h?n:n+":"+e,k=c.value,s=c.expiresMinutes||1440*(c.expiresDays||365),t=function(){var a=new Date;a.setTime(a.getTime()+6E4*s);return a}();if(!function(){var a={_hjSet:d,_hjGet:b,_hjRemove:d}[m]||[];return 0<=a.indexOf("*")||0<=a.indexOf(g)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\chart.js@2.8[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	156721
Entropy (8bit):	5.3437462807874025
Encrypted:	false
SSDEEP:	3072:9IqGk57miKaxSUE879VE7CjWX1gLQmZ23M:9IqG67miKaxSUE879VEXO3
MD5:	B235B564DE9C2C1D61D7EF07FCF2B93B
SHA1:	2EBF900E0386749373E9887026590FE7DAFC30AE
SHA-256:	52FF41341B9CBC23E2A4A436352F706292668BC0D33847D303F9C7D9AA0900BC
SHA-512:	99FEFC2AE914FDAF2B8EBEDA051BC26B657083FAB4B548C984BB5C2B9DCF1C46C5C0212A43976EAE5CEF55381080AA6FF9FC8D313E99413D40ABAB6936A7F59A
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&&"undefined"!=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,rgb2hsv: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)return[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\2K7JPOQS\cookie_push_onload[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\cookie_push_onload[1].htm	
Category:	dropped
Size (bytes):	1174
Entropy (8bit):	5.74166936214599
Encrypted:	false
SSDEEP:	24:hY6t2eJJBewfHDdUg8EcvjHODQMJXeK+C6uS/MLmeK+C6uSGymWAuDSXeMzCUtVv:9V4goLHODS1CTXT1CTVyPyCM6Nu
MD5:	2FE2B1F17888E326B010A8CDA72D48D3
SHA1:	59CBBEEDE4C472024C482BAE8529144119BBBD27
SHA-256:	9A9B7FB32E01FD70747F32EFDBD0472FD681C85EEBB0C42D10C7A514820A0062
SHA-512:	30BE2E73020EB97A67709E47DED40E999D352DA9B94EDD946D1315BDA65AD616AAA3CDFCFA675D061E4ED4AE1BAE3F0D245908D44411B2425C49B4345D2F66 07
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>.<head>. <title></title>. <script type="text/javascript">(function(){var f=null,g=null;function l(a){var b="";n(a,function(a){b+=String.fromCharCo de(a)});return b}function n(a,b){function c(b){for(;e<a.length;){var c=a.charAt(e++),d=g[c];if(null!=d)return d;if(!/^[\s\xa0]*$/.test(c))throw Error("Unknown base64 encoding at char: "+c);}return b}p();for(var e=0;;){var d=c(-1),m=c(0),h=c(64),k=c(64);if(64===k&&-1===d)break;b(d<<2|m>>4);64!=h&&(b(m<<4&240|h>>2),64!=k&&b(h<<6&192|k))}}.f unction p(){if(!f){f={};g={};for(var a=0;65>a;a++)f[a]="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=".charAt(a),g[f[a]]=a,62<=a&& (g["ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_.".charAt(a)]=a)}};function q(){for(var a=window.location.hash.substring(1).split(",",b=0;b<a.length;b++){var c=l(a[b]),e=window;e.google_image_requests||(e.google_image_requests=[]);var d=e.document.createElement("img");d.src=c;e.google_ima ge_requests.push(d)}}var r=!1;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\cookie_push_onload[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1174
Entropy (8bit):	5.74166936214599
Encrypted:	false
SSDEEP:	24:hY6t2eJJBewfHDdUg8EcvjHODQMJXeK+C6uS/MLmeK+C6uSGymWAuDSXeMzCUtVv:9V4goLHODS1CTXT1CTVyPyCM6Nu
MD5:	2FE2B1F17888E326B010A8CDA72D48D3
SHA1:	59CBBEEDE4C472024C482BAE8529144119BBBD27
SHA-256:	9A9B7FB32E01FD70747F32EFDBD0472FD681C85EEBB0C42D10C7A514820A0062
SHA-512:	30BE2E73020EB97A67709E47DED40E999D352DA9B94EDD946D1315BDA65AD616AAA3CDFCFA675D061E4ED4AE1BAE3F0D245908D44411B2425C49B4345D2F66 07
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/pagead/s/cookie_push_onload.html
Preview:	<!DOCTYPE html>.<html>.<head>. <title></title>. <script type="text/javascript">(function(){var f=null,g=null;function l(a){var b="";n(a,function(a){b+=String.fromCharCo de(a)});return b}function n(a,b){function c(b){for(;e<a.length;){var c=a.charAt(e++),d=g[c];if(null!=d)return d;if(!/^[\s\xa0]*$/.test(c))throw Error("Unknown base64 encoding at char: "+c);}return b}p();for(var e=0;;){var d=c(-1),m=c(0),h=c(64),k=c(64);if(64===k&&-1===d)break;b(d<<2|m>>4);64!=h&&(b(m<<4&240|h>>2),64!=k&&b(h<<6&192|k))}}.f unction p(){if(!f){f={};g={};for(var a=0;65>a;a++)f[a]="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=".charAt(a),g[f[a]]=a,62<=a&& (g["ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_.".charAt(a)]=a)}};function q(){for(var a=window.location.hash.substring(1).split(",",b=0;b<a.length;b++){var c=l(a[b]),e=window;e.google_image_requests||(e.google_image_requests=[]);var d=e.document.createElement("img");d.src=c;e.google_ima ge_requests.push(d)}}var r=!1;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	2906
Entropy (8bit):	5.290227902897662
Encrypted:	false
SSDEEP:	48:xOJa/OWaEOLxHOxTaYOCaLHOw6aJOS7rOJCOWbOLKOgPhOxTAOCuOw6lOMP:xOJa/OWaEOLxHOxTaYOCarOw6aJOS7rN
MD5:	945FB8178712AE2C2DFC24E50A8E49D8
SHA1:	26E232953561D40752A6FEF6C32B7EAEB9B3E4DC
SHA-256:	2E981F3FA57474A381C00BE7390B2E71AF67A5D35D05DEE637C047CAA4AC4E39
SHA-512:	FD2CCF423991D9E24626FB6C7F2A680CAC0CFB99E1542F387BC1773945C0BC0C8C52BEB594AD8285F16C0EAD86327237F75963EC249CCF8D614C8A812AF93D B
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Biryani';. font-style: normal;. font-weight: 200;. src: url(https://fonts.gstatic.com/s/biryani/v6/hv-TlzNxIFoO84YddYQyKTdYVA.woff) format ('woff');.}.@font-face {. font-family: 'Biryani';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/biryani/v6/hv-TlzNxIFoO84YddeAxKTdYVA.woff) format('woff');.}.@font-face {. font-family: 'Biryani';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/biryani/v6/hv-WlzNxIFoO84YdfUsTOg.woff) format('woff');.}.@font-face {. font-family: 'Biryani';. font-style: normal;. font-weight: 600;. src: url(https://fonts.gstatic.com/s/biryani/v6/hv-TlzNxIFoO84YddZQ3KTdYVA. woff) format('woff');.}.@font-face {. font-family: 'Biryani';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/biryani/v6/hv-TlzNxIFoO84Y ddfA2KTdYVA.woff) format('woff');.}.@font-face {. font-family: 'Biryani';. font-style: normal;. font-weight: 800;. src: url(ht

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\css[2].css	
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:	EFD365A575C5DB8B1E225BB82B964DC3FC3D8FB1B8A4102160226662011363O5E06AFD8FC7FA95CCD4DE5EC3953A32677C7381323FA5C6E8E3BB74F974119E9
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\2K7JPOQS\designit_logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1700 x 540, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	62677
Entropy (8bit):	7.0270475811331945
Encrypted:	false
SSDEEP:	768:9tQFsxaEWNFp/7sr8reideibexpPMLsmjtly0+9hjWDN0K9u1PDOCOGaJPG13/YD:9Ms47/7ckFVbq8lijjWeFO237QjONs
MD5:	26CCFDA9F374939FB247AFED86055DA5
SHA1:	BC0D32B36AE398792667BC9925E1AA86D62AEA4A
SHA-256:	910B0C98D9983510E251DBAA40C805A37DB054755F18EB45C1C29B68C5FF4196
SHA-512:	731FEE2AD12CB018A066E254A5967ADEBFE37A62575CEEFD28D5EAF19445AD43A4DAEF2CB958D5C7F7728776C594ABFCA8A1111457C8B19DF237D4E3126E429D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19tracking.narrativa.com/img/designit_logo.png
Preview:	.PNG.....IHDR.....3....pHYs.....9.iTXtXML:com.adobe.xmp.....<?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:dc="http://purl.org/dc/elements/1.1/". xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/". xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/">. <xmp:CreatorTool>Adobe Photoshop CC 2017 (Macintosh)</xmp:CreatorTool>. <xmp:CreateDate>2017-08-17T12:32:15-04:00</xmp:CreateDate>. <xmp:ModifyDate>2017-08-17T12:36:08-04:00</xmp:ModifyDate>. <xmp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\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:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
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(); 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\2K7JPOQS\downsize_200k_v1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\downsize_200k_v1[1].jpg	
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 100x100, frames 3
Category:	downloaded
Size (bytes):	1911
Entropy (8bit):	7.621947858534851
Encrypted:	false
SSDEEP:	48:rwcwFCxCMVs7nz6uQEHt9AjuvedyeFb/SYHSfy/yfrCkq:joMu7nzVN9AKmdyqOYH7/Y+
MD5:	BA71F81377F6E06BD4864CAF64A16AD9
SHA1:	E7429A18496DABB8B73CA9AD30C4B7E49F787F59
SHA-256:	8BFF9EC3A2C218DB516F668F50F0B70958136D28892DC840BC0544A20EF7D61B
SHA-512:	7BEB75F7784ECC3625835B897D5B99B78EDFEB916094A0871A75EAB3BA5952325481E01DC5C9DF29014CDE3129397E0FAAF5F6285E0B3BC3ECAFE056807D844 5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/6525030626783894 69/downsize_200k_v1?w=100&h=100
Preview:	......JFIF..... .'"" ...$(4,$&1'..-=-157:::#+?D?8C49:7.....7%.%77777777777777777777777777777777777777777777777777.....d.d..... .....;.....!..1Aa..2."#7Qqst....Br.46bu.....?..h.....@.P(.....@.P(.....@.P(.....@.P(.....@.P(.....@.....f.J...I...(=.(...W.u.m.no..... .'..uZ.....R.....w.w..vr.....wH..(.c9Q....q<j.....;'.mR.oG.. ....,.Rznr.79.,=.s.^t...yC(.).P.....pI....@.....+B.[JRH.#...2.....(q..~F...g.g..B.J\t..9.(.Nq..P^<..7.....J5.....G. 6N=W.....d....p...T.+@Q...@..>?.B...|.M.Z..F.?.*..xm...Z.v..e..O....Y.|.....*.x....mWVV.-{..q...QA.. x.A.....!.#...H.%).....I_.b...W9O.....Hl....e....dy..p....~...:....p.....@..... .'P.G...P.m..)..VR.{.A.|Q.B.~-_....;.v~.F..y2...N3Ek8R..:u$..g.z...[..x.....G.....!....4...=.V..$1.....].7.../.8y.[Dm..Dk.t....Zz./..'c.'c..o.^..%{=....8C..n.J...A..!.....}...QJ.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\efe_20210414_073806655[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):	82989
Entropy (8bit):	7.9551564749534736
Encrypted:	false
SSDEEP:	1536:dlhjLSSc20axXwyGPMr61sZ8Tnm1nvmoikhnFkTLcZ3c4+dGuF0MuPajcVNC7e8I:RySWaxggrt8Tm1nvRikPkkFc41IcPaKR
MD5:	530F864B6E849A4EA7D9FEF44B9E0E0D
SHA1:	0C16919D529585E6A780A8D6401EA58EA067A042
SHA-256:	6EF903ADBF42F28569C1FB213FB844365FED9B9B4632D10CF4CAD94CF1C7E5E7
SHA-512:	EAEE6EC903386D2C74F4279990DE2F1F3EA98A2F930EA6DF09B8D18232C38616ED0126A1E367E3DAA12DF4330D35A3C60243BF156E3F8655FD83041E6F88AF3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.lavozdegalicia.es/default/2021/04/14/00121618386603074724936/Foto/efe_20210414_073806655.jpg
Preview:	......JFIF.....H.H.....C.....%...#... , #&')*)..-0-(0%()(...C.....(...((((((

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\f[1].txt	
Category:	downloaded
Size (bytes):	135276
Entropy (8bit):	5.559974423342489
Encrypted:	false
SSDEEP:	3072:H5kfO59PvOi0TNe8MEvirRPuQ7lDURW6a:dnshMEvANj7lIRW6a
MD5:	4D85A52F96B7F21C56292C2C9C9C6A23
SHA1:	37985D1865D0D638F047A7E3D3AA698F3A07751F
SHA-256:	BD02A9FE74094375001F382DE8066DD322A2E7C9A67821418104C9518BFE802B
SHA-512:	D009B2F666B8C9B3CCA614575CC6A176D038696C3EFFC84C29F84E5F11DF1123FBF5BB1E2F2F6BFF7838C8682973BF99D187B79B2FE59AC2245BD9FA8B16836
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js
Preview:	(function(sttc){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .var n,aa;function ba(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var ca="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a}; .function da(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var ea=da(this),fa="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),p={},ha={};function r(a,b){var c=ha[b];if(null==c)return a[b];c=a[c];return void 0!==c?c:a[b]} .function u(a,b,c){if(b)a:{var d=a.split(".");a=1===d.length;var e=d[0],f;!a&&e in p?f=p:f=ea;for(e=0;e<d.length-1;e++){var g=d[e];if(!(g in f))break a;f=f[g]}d=d[d.length-1];c=fa&&"es6"===c?f[d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\f[2].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	253758
Entropy (8bit):	5.501823771178204
Encrypted:	false
SSDEEP:	3072:/lR1M7SRCcd4IvIRJJ8bVAwATA/E690cWD1JRkdBl651e3Z5fA:nZqIvIRJeV/ATA/E6ikdBl6re3Z54
MD5:	D0C00B8E9BC800A7464CA47E8F77B5A5
SHA1:	4DB4B9E775191D01EF30A40A0C43D7F3C618B1E0
SHA-256:	9B458D60B6E55B50F6AFE3912990E5577BD2C9B7065473EA05001359E5311D30
SHA-512:	252EDEE656A137917214C789328D3C86766A8F1AB515EBBFA00524B8B75E46C23C855E42AFB7A2B267B2A885DD4BD726F6A24BE3FCDA50A02E14CD0FCD58918
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/pagead/js/r20210429/r20190131/show_ads_impl_with_ama.js?client=ca-pub-4607443575710795&plah=localcoronavirus.com&amaexp=1
Preview:	(function(sttc){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .var r,aa;function ba(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var ca="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a}; .function da(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var ea=da(this),ha="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),v={},ia={};function w(a,b){var c=ia[b];if(null==c)return a[b];c=a[c];return void 0!==c?c:a[b]} .function x(a,b,c){if(b)a:{var d=a.split(".");a=1===d.length;var e=d[0],f;!a&&e in v?f=v:f=ea;for(e=0;e<d.length-1;e++){var g=d[e];if(!(g in f))break a;f=f[g]}d=d[d.length-1];c=ha&&"es6"===c?f[d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\f[3].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	21878
Entropy (8bit):	5.4097110490020635
Encrypted:	false
SSDEEP:	384:IXAmFuHJemiS2MwYArfa2iRop0PGHJxSyl0PLfQemrKvqY:sTxB2UrfeSSyl0Pz8eqY
MD5:	F720FA603B3E2514D36557034C3C6F0E
SHA1:	8F695234514B5F81167953C43C6E1006FF1865F1
SHA-256:	023AB520F198F85225F9E86CD2D4D7BC71EA1116D27F9A9B92E2A4F4993967F4
SHA-512:	F3D9B4D323C9F4372DE3AE62E7E695AD544E1E2E80F9B94752D47128B281D638974348C5D7A2E3DFAAC67C59A0C6E1EEC52AC10B2D75F82139878013E962128
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/pagead/js/r20210429/r20110914/elements/html/interstitial_ad_frame.js
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .var n;function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a}; .function ca(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var r=ca(this);function da(a,b){if(b)a:{var c=r;a=a.split(".");for(var e=0;e<a.length-1;e++){var f=a[e];if(!(f in c))break a;c=c[f]}a=a[a.length-1];e=c[a];b=b(e);b!=e&&null!=b&&ba(c,a,{configurable:!0,writable:!0,value:b})}} .function t(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:aa(a)}}var ea="function"==typeof Objec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\f[4].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\f[4].txt	
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/r20210429/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)};fun ction 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\2K7JPOQS\facebook_local_coronavirus[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 240 x 240, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	8444
Entropy (8bit):	7.856669552818226
Encrypted:	false
SSDEEP:	192:4dgy7F8kn2U4jQ9IAkTduQlWdAw18dk337N4s3iJNVL8AjJIdi:uvNnTwkQlWdAmgk6sYVL8aJIQ
MD5:	81731CA250FE21DF7BCE2A0E756FB120
SHA1:	02884C6A8EEA7E2C2A663F30447E218E8199548A
SHA-256:	DF4D4189514EABA48D59BB3EF5FF113E71EBAB40BBD226B463858DE7C02C3DBC
SHA-512:	229F23C62BDBDE24C9D26EE0AF45E994E4D63C5FD65E26D86879C7E66B6A78CB9E3127ADCB4540050EE46EBD2469FCC5AE16F8AC6A34B2E2A88C8204583BCF2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/assets/images/facebook_local_coronavirus.png
Preview:	.PNG.....IHDR.....>U....&iCCPAdobe RGB (1998)..(.c``2ptqre.``..+).rwR...R`?.....> v^~^*...v...D_....@..J.(*.....(%.8...../)..3...E..... vQH.3.}...K.....I..... ..H}: ....6....KR+@.28..T.e.g.(.ZZZ*8..'.*.W.....+x.%.....%.....B.....j..d.2.....9....bg.b..\ZT.e22...#.#.....B...a.....T...!...>..9...O..:6\....pHYs.....+.....iTXtXML:com.adobe.xmp..... <?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http://p url.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xa p/1.0/sType/ResourceEvent#" xmp:CreatorTool="Adobe Photoshop CC 2018 (Windows)" xmp:CreateDate="2020-08-24T14:35:41+02:00" xmp:Modi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\favicon[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 64 x 65, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5775
Entropy (8bit):	7.751685370473314
Encrypted:	false
SSDEEP:	96:NhuQ5Vo7FhknmWpYOxYbOLMHfmH0mgzdtsfNFeC933ktunIOys60yiiLEgY4yJVJ:NEQ07FhknOuM/muPs1Fqmd9nyiiZqr
MD5:	EC13B2751C7EF22C9989C123F791982D
SHA1:	413F21C91A623984D4661E90C07316EDD319284E
SHA-256:	098C85205D28FAB0B778E0446FA66C804312B7554A99E965EBF99D4991949FA2
SHA-512:	F79F79DE495A11BC288AA5520DE655B81B3E3F933FBBA4C5D17769704E5A7D4037DA174B2862AB3B076FA76FB193111EBAA087E7A1F862D07AAAF0DAF0234E07
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://localcoronavirus.com/favicon.png
Preview:	.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.I7..V.....=...en.G.@,=.YAx...U.;..b.p...azTd.7p....E.Z...<.....O..S?.....pHYs...#...#.x.?v....iTXtXML :com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmp:CreatorTool="Adobe Photoshop CC (Windows)" xmp:CreateDate="2020-03-11T13:21:54+01:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\free-v4-shims.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	26701
Entropy (8bit):	4.829823522211244
Encrypted:	false
SSDEEP:	192:dP6hT1bIl4w0QUmQ10PwKLaAu5CwWavpHo4O6wgLPbJVR8XD7mycP:0hal4w0QK+PwK05eavpmgPPeXD7mycP
MD5:	8A99CE81EC2F89FBCA03F2C8CF1A3679
SHA1:	58F9EF32D12A5DA52CBAB7BD518BCC998FC59EF9
SHA-256:	362DAEAF1F7E05FEE9A609E549F148AACBE518C166FBD96EAD69057E295742AF
SHA-512:	930F28449365FAED13718BB8F332625DB110ABB08C3778DC632FDF00A0187A61A086B5EB4765FFC1923B64E2584C02592A213914B024DE6890FF3DBFC3A12FE5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.3/css/free-v4-shims.min.css?token=b745858f50
Preview:	/*!. * Font Awesome Free 5.15.3 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa.fa-glass:before{content:"\f000"}.fa.fa-meetup{font-family:"Font Awesome 5 Brands";font-weight:400}.fa.fa-star-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-star-o:before{content:"\f005"}.fa.fa-close:before,.fa.fa-remove:before{content:"\f00d"}.fa.fa-gear:before{content:"\f013"}.fa.fa-trash-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-trash-o:before{content:"\f2ed"}.fa.fa-file-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-file-o:before{content:"\f15b"}.fa.fa-clock-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-clock-o:before{content:"\f017"}.fa.fa-arrow-circle-o-down{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arrow-circle-o-down:before{content:"\f358"}.fa.fa-arrow-circle-o-up{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\free.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	60351
Entropy (8bit):	4.728641238865369
Encrypted:	false
SSDEEP:	768:0Uh31IPiyXNq4YxBowbgJlkwF//zMQyYJYX9Bft6VSz8:0U0PxXE4YXJgndFTfy9lt5Q
MD5:	390B4210E10C744C3C597500BCF0B31A
SHA1:	2600C7C2F25D7DBCBC668231601E426010DC6489
SHA-256:	C2819CA1F7AD1AF7BA53C4EDFDFD395C547BCB16D29892A234D7860C689ED929
SHA-512:	E8A7E466BE8CC092E12994B51A6A8A39E2FBB66DD48221BCF499BB89365B4004D73C1909F8FE0BBBBF13907D5901D76FFE127D92FDD7493853646F83F5985CB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.3/css/free.min.css?token=b745858f50
Preview:	/*!. * Font Awesome Free 5.15.3 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa,.fab,.fad,.fal,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-variant:normal;text-rendering:auto;line-height:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font-size:1em}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font-size:9em}.fa-10x{font-size:10em}.fa-fw{text-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;position:absolute;text-align:center;width:2em;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pul

Static File Info

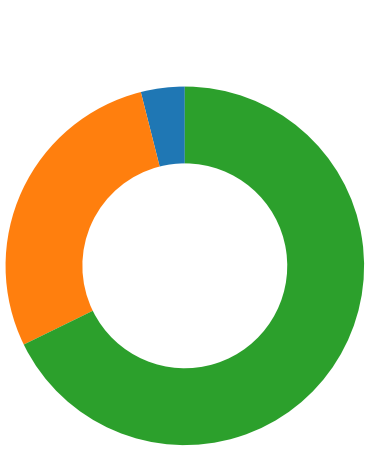
No static file info

Network Behavior

Network Port Distribution

Total Packets: 152

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:36:29.232979059 CEST	49696	80	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.233808994 CEST	49697	80	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.275624990 CEST	80	49696	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.275981903 CEST	80	49697	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.276107073 CEST	49697	80	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.276274920 CEST	49696	80	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.276551008 CEST	49696	80	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.317377090 CEST	80	49696	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.335083961 CEST	80	49696	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.335256100 CEST	49696	80	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.342730045 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.383510113 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.383611917 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.389894009 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.432949066 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.437325001 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.437350988 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.437467098 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.473561049 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.480721951 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.480818033 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.514292955 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.514746904 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.514766932 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.514853954 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.514874935 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.515602112 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.521482944 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.521506071 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.528482914 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.528547049 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.599373102 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.887634039 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.887753963 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.889816046 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.889837980 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.889859915 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.889873981 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.889926910 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.889962912 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.890244961 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.890269041 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.890295982 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.890332937 CEST	49698	443	192.168.2.7	104.21.18.245

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:36:29.891227007 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.891246080 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.891283035 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.891335011 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.927181959 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.927201986 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.927292109 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.927297115 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.927309036 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.927342892 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.927375078 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.928272963 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.928293943 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.928332090 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.928344965 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.929261923 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.929318905 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.929351091 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.929420948 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.930351019 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.930367947 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.930417061 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.930453062 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.953533888 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.954129934 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.954657078 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.955167055 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.955705881 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.956212997 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.956571102 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.957164049 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.957515955 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.957906008 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:29.994225025 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.994716883 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.995320082 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.995829105 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.996264935 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.996819019 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.997261047 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.997746944 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.997994900 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:29.998441935 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:30.005064964 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:30.005170107 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:30.005188942 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:30.005237103 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:30.005310059 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:30.005321980 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:30.005354881 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:30.005400896 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:30.005700111 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:30.005723953 CEST	443	49698	104.21.18.245	192.168.2.7
May 4, 2021 15:36:30.005758047 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:30.005780935 CEST	49698	443	192.168.2.7	104.21.18.245
May 4, 2021 15:36:30.006771088 CEST	443	49698	104.21.18.245	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:36:20.591171026 CEST	53	50848	8.8.8.8	192.168.2.7
May 4, 2021 15:36:20.848273993 CEST	61242	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:20.897069931 CEST	53	61242	8.8.8.8	192.168.2.7
May 4, 2021 15:36:22.740029097 CEST	58562	53	192.168.2.7	8.8.8.8

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:36:22.799901009 CEST	53	58562	8.8.8.8	192.168.2.7
May 4, 2021 15:36:28.061335087 CEST	56590	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:28.125365973 CEST	53	56590	8.8.8.8	192.168.2.7
May 4, 2021 15:36:29.146943092 CEST	60501	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:29.211848021 CEST	53	60501	8.8.8.8	192.168.2.7
May 4, 2021 15:36:29.434561968 CEST	53775	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:29.484169006 CEST	53	53775	8.8.8.8	192.168.2.7
May 4, 2021 15:36:29.952707052 CEST	51837	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:29.963641882 CEST	55411	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:29.979970932 CEST	63668	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:30.012099981 CEST	53	55411	8.8.8.8	192.168.2.7
May 4, 2021 15:36:30.021004915 CEST	53	51837	8.8.8.8	192.168.2.7
May 4, 2021 15:36:30.030605078 CEST	53	63668	8.8.8.8	192.168.2.7
May 4, 2021 15:36:30.060276985 CEST	54640	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:30.071759939 CEST	58739	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:30.095165968 CEST	60338	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:30.102920055 CEST	58717	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:30.107083082 CEST	59762	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:30.117443085 CEST	53	54640	8.8.8.8	192.168.2.7
May 4, 2021 15:36:30.128757954 CEST	53	58739	8.8.8.8	192.168.2.7
May 4, 2021 15:36:30.161470890 CEST	54329	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:30.166285038 CEST	53	60338	8.8.8.8	192.168.2.7
May 4, 2021 15:36:30.168421030 CEST	53	59762	8.8.8.8	192.168.2.7
May 4, 2021 15:36:30.187474966 CEST	53	58717	8.8.8.8	192.168.2.7
May 4, 2021 15:36:30.221988916 CEST	53	54329	8.8.8.8	192.168.2.7
May 4, 2021 15:36:30.408689022 CEST	58052	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:30.409910917 CEST	54008	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:30.440869093 CEST	59451	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:30.479522943 CEST	53	58052	8.8.8.8	192.168.2.7
May 4, 2021 15:36:30.495585918 CEST	53	54008	8.8.8.8	192.168.2.7
May 4, 2021 15:36:30.503468037 CEST	53	59451	8.8.8.8	192.168.2.7
May 4, 2021 15:36:30.693485022 CEST	52914	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:30.753315926 CEST	53	52914	8.8.8.8	192.168.2.7
May 4, 2021 15:36:31.031666994 CEST	64569	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:31.097410917 CEST	53	64569	8.8.8.8	192.168.2.7
May 4, 2021 15:36:31.142452955 CEST	52816	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:31.199464083 CEST	53	52816	8.8.8.8	192.168.2.7
May 4, 2021 15:36:31.530837059 CEST	50781	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:31.593497992 CEST	53	50781	8.8.8.8	192.168.2.7
May 4, 2021 15:36:31.634912968 CEST	54230	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:31.693798065 CEST	53	54230	8.8.8.8	192.168.2.7
May 4, 2021 15:36:31.749764919 CEST	54911	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:31.752443075 CEST	49958	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:31.800357103 CEST	53	54911	8.8.8.8	192.168.2.7
May 4, 2021 15:36:31.806687117 CEST	50860	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:31.844305992 CEST	53	49958	8.8.8.8	192.168.2.7
May 4, 2021 15:36:31.857511044 CEST	53	50860	8.8.8.8	192.168.2.7
May 4, 2021 15:36:31.892232895 CEST	50452	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:31.985969067 CEST	53	50452	8.8.8.8	192.168.2.7
May 4, 2021 15:36:32.092113972 CEST	59730	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:32.148977041 CEST	53	59730	8.8.8.8	192.168.2.7
May 4, 2021 15:36:32.289483070 CEST	59310	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:32.349493980 CEST	53	59310	8.8.8.8	192.168.2.7
May 4, 2021 15:36:32.949412107 CEST	51919	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:32.952897072 CEST	64296	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:32.970494986 CEST	56680	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:32.993797064 CEST	58820	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:33.000960112 CEST	53	51919	8.8.8.8	192.168.2.7
May 4, 2021 15:36:33.009809971 CEST	53	64296	8.8.8.8	192.168.2.7
May 4, 2021 15:36:33.030216932 CEST	60983	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:33.030790091 CEST	53	56680	8.8.8.8	192.168.2.7
May 4, 2021 15:36:33.040148020 CEST	49247	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:33.058743954 CEST	53	58820	8.8.8.8	192.168.2.7
May 4, 2021 15:36:33.097064972 CEST	53	49247	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:36:33.098334074 CEST	53	60983	8.8.8.8	192.168.2.7
May 4, 2021 15:36:33.167984962 CEST	52286	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:33.233313084 CEST	53	52286	8.8.8.8	192.168.2.7
May 4, 2021 15:36:33.699039936 CEST	56064	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:33.763566971 CEST	53	56064	8.8.8.8	192.168.2.7
May 4, 2021 15:36:34.543126106 CEST	63744	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:34.592459917 CEST	53	63744	8.8.8.8	192.168.2.7
May 4, 2021 15:36:34.600229025 CEST	61457	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:34.650747061 CEST	53	61457	8.8.8.8	192.168.2.7
May 4, 2021 15:36:35.437401056 CEST	58367	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:35.495656967 CEST	53	58367	8.8.8.8	192.168.2.7
May 4, 2021 15:36:35.921401978 CEST	60599	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:35.983171940 CEST	53	60599	8.8.8.8	192.168.2.7
May 4, 2021 15:36:36.018068075 CEST	59571	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:36.068947077 CEST	53	59571	8.8.8.8	192.168.2.7
May 4, 2021 15:36:40.130274057 CEST	52689	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:40.141700983 CEST	50290	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:40.151976109 CEST	60427	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:40.163346052 CEST	56209	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:40.184029102 CEST	59582	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:40.189614058 CEST	53	52689	8.8.8.8	192.168.2.7
May 4, 2021 15:36:40.190546036 CEST	53	50290	8.8.8.8	192.168.2.7
May 4, 2021 15:36:40.203394890 CEST	53	60427	8.8.8.8	192.168.2.7
May 4, 2021 15:36:40.208612919 CEST	60949	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:40.211981058 CEST	53	56209	8.8.8.8	192.168.2.7
May 4, 2021 15:36:40.249142885 CEST	53	59582	8.8.8.8	192.168.2.7
May 4, 2021 15:36:40.289413929 CEST	53	60949	8.8.8.8	192.168.2.7
May 4, 2021 15:36:47.636292934 CEST	58542	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:47.699398041 CEST	53	58542	8.8.8.8	192.168.2.7
May 4, 2021 15:36:48.398708105 CEST	59179	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:48.449167013 CEST	53	59179	8.8.8.8	192.168.2.7
May 4, 2021 15:36:51.748485088 CEST	60927	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:51.809402943 CEST	53	60927	8.8.8.8	192.168.2.7
May 4, 2021 15:36:56.185167074 CEST	57854	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:56.236721992 CEST	53	57854	8.8.8.8	192.168.2.7
May 4, 2021 15:36:57.697931051 CEST	62026	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:57.746881008 CEST	53	62026	8.8.8.8	192.168.2.7
May 4, 2021 15:36:58.118993044 CEST	59453	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:58.170485973 CEST	53	59453	8.8.8.8	192.168.2.7
May 4, 2021 15:36:58.980638027 CEST	62468	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:59.030874014 CEST	53	62468	8.8.8.8	192.168.2.7
May 4, 2021 15:36:59.598690033 CEST	59453	53	192.168.2.7	8.8.8.8
May 4, 2021 15:36:59.650233984 CEST	53	59453	8.8.8.8	192.168.2.7
May 4, 2021 15:37:00.162053108 CEST	62468	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:00.211585045 CEST	53	62468	8.8.8.8	192.168.2.7
May 4, 2021 15:37:00.685010910 CEST	59453	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:00.736512899 CEST	53	59453	8.8.8.8	192.168.2.7
May 4, 2021 15:37:03.127825975 CEST	62468	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:03.176554918 CEST	53	62468	8.8.8.8	192.168.2.7
May 4, 2021 15:37:03.201944113 CEST	59453	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:03.253520966 CEST	53	59453	8.8.8.8	192.168.2.7
May 4, 2021 15:37:05.133462906 CEST	62468	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:05.190435886 CEST	53	62468	8.8.8.8	192.168.2.7
May 4, 2021 15:37:05.439791918 CEST	52563	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:05.499736071 CEST	53	52563	8.8.8.8	192.168.2.7
May 4, 2021 15:37:05.546082020 CEST	54721	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:05.618727922 CEST	53	54721	8.8.8.8	192.168.2.7
May 4, 2021 15:37:05.863600969 CEST	62826	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:05.922939062 CEST	53	62826	8.8.8.8	192.168.2.7
May 4, 2021 15:37:06.182018042 CEST	62046	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:06.248045921 CEST	53	62046	8.8.8.8	192.168.2.7
May 4, 2021 15:37:07.240053892 CEST	59453	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:07.292251110 CEST	53	59453	8.8.8.8	192.168.2.7
May 4, 2021 15:37:09.148230076 CEST	62468	53	192.168.2.7	8.8.8.8

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:37:09.196918011 CEST	53	62468	8.8.8.8	192.168.2.7
May 4, 2021 15:37:11.302525997 CEST	51223	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:11.351931095 CEST	53	51223	8.8.8.8	192.168.2.7
May 4, 2021 15:37:15.728324890 CEST	63908	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:15.786007881 CEST	53	63908	8.8.8.8	192.168.2.7
May 4, 2021 15:37:15.860795975 CEST	49226	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:15.913561106 CEST	53	49226	8.8.8.8	192.168.2.7
May 4, 2021 15:37:17.017426968 CEST	60212	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:17.074604034 CEST	53	60212	8.8.8.8	192.168.2.7
May 4, 2021 15:37:22.179203033 CEST	58867	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:22.231386900 CEST	53	58867	8.8.8.8	192.168.2.7
May 4, 2021 15:37:25.283648014 CEST	50864	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:25.332353115 CEST	53	50864	8.8.8.8	192.168.2.7
May 4, 2021 15:37:26.068780899 CEST	61504	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:26.118632078 CEST	53	61504	8.8.8.8	192.168.2.7
May 4, 2021 15:37:26.981228113 CEST	60231	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:27.034450054 CEST	53	60231	8.8.8.8	192.168.2.7
May 4, 2021 15:37:27.051229000 CEST	50095	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:27.100018978 CEST	53	50095	8.8.8.8	192.168.2.7
May 4, 2021 15:37:28.508384943 CEST	59654	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:28.558089972 CEST	53	59654	8.8.8.8	192.168.2.7
May 4, 2021 15:37:29.706675053 CEST	58233	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:29.758207083 CEST	53	58233	8.8.8.8	192.168.2.7
May 4, 2021 15:37:30.597831011 CEST	56822	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:30.648498058 CEST	53	56822	8.8.8.8	192.168.2.7
May 4, 2021 15:37:31.734080076 CEST	62572	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:31.785712957 CEST	53	62572	8.8.8.8	192.168.2.7
May 4, 2021 15:37:32.844600916 CEST	57179	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:32.897447109 CEST	53	57179	8.8.8.8	192.168.2.7
May 4, 2021 15:37:38.835381985 CEST	56124	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:38.888406038 CEST	53	56124	8.8.8.8	192.168.2.7
May 4, 2021 15:37:39.912138939 CEST	62287	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:39.960886955 CEST	53	62287	8.8.8.8	192.168.2.7
May 4, 2021 15:37:48.921555042 CEST	54644	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:48.988209009 CEST	53	54644	8.8.8.8	192.168.2.7
May 4, 2021 15:37:49.249552011 CEST	59159	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:49.259143114 CEST	57924	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:49.313894033 CEST	53	59159	8.8.8.8	192.168.2.7
May 4, 2021 15:37:49.321712017 CEST	53	57924	8.8.8.8	192.168.2.7
May 4, 2021 15:37:49.602268934 CEST	51712	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:49.665277958 CEST	53	51712	8.8.8.8	192.168.2.7
May 4, 2021 15:37:52.996649981 CEST	58865	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:53.059221029 CEST	53	58865	8.8.8.8	192.168.2.7
May 4, 2021 15:37:53.165889978 CEST	64337	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:53.224966049 CEST	53	64337	8.8.8.8	192.168.2.7
May 4, 2021 15:37:53.324820995 CEST	50407	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:53.398495913 CEST	53	50407	8.8.8.8	192.168.2.7
May 4, 2021 15:37:53.578241110 CEST	61075	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:53.633419037 CEST	54952	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:53.647227049 CEST	53	61075	8.8.8.8	192.168.2.7
May 4, 2021 15:37:53.653141022 CEST	59186	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:53.662055016 CEST	52280	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:53.672657967 CEST	51794	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:53.681974888 CEST	50815	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:53.693798065 CEST	58498	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:53.713972092 CEST	53	54952	8.8.8.8	192.168.2.7
May 4, 2021 15:37:53.717144966 CEST	53	59186	8.8.8.8	192.168.2.7
May 4, 2021 15:37:53.725308895 CEST	56862	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:53.732680082 CEST	53	51794	8.8.8.8	192.168.2.7
May 4, 2021 15:37:53.748311996 CEST	53	52280	8.8.8.8	192.168.2.7
May 4, 2021 15:37:53.768430948 CEST	61807	53	192.168.2.7	8.8.8.8
May 4, 2021 15:37:53.777674913 CEST	53	58498	8.8.8.8	192.168.2.7
May 4, 2021 15:37:53.783550978 CEST	53	50815	8.8.8.8	192.168.2.7
May 4, 2021 15:37:53.788677931 CEST	53	56862	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:37:53.833760023 CEST	53	61807	8.8.8.8	192.168.2.7
May 4, 2021 15:38:02.893307924 CEST	52009	53	192.168.2.7	8.8.8.8
May 4, 2021 15:38:02.941955090 CEST	53	52009	8.8.8.8	192.168.2.7
May 4, 2021 15:38:04.396384954 CEST	58648	53	192.168.2.7	8.8.8.8
May 4, 2021 15:38:04.476283073 CEST	53	58648	8.8.8.8	192.168.2.7
May 4, 2021 15:38:05.240077972 CEST	59337	53	192.168.2.7	8.8.8.8
May 4, 2021 15:38:05.291500092 CEST	53	59337	8.8.8.8	192.168.2.7
May 4, 2021 15:38:16.917027950 CEST	59269	53	192.168.2.7	8.8.8.8
May 4, 2021 15:38:16.979984045 CEST	53	59269	8.8.8.8	192.168.2.7
May 4, 2021 15:38:23.684372902 CEST	49802	53	192.168.2.7	8.8.8.8
May 4, 2021 15:38:23.736048937 CEST	53	49802	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 15:36:29.146943092 CEST	192.168.2.7	8.8.8.8	0x49b6	Standard query (0)	localcoronavirus.com	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.071759939 CEST	192.168.2.7	8.8.8.8	0x2a84	Standard query (0)	www.republica.com	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.095165968 CEST	192.168.2.7	8.8.8.8	0x6ae7	Standard query (0)	www.lavozdegalicia.es	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.102920055 CEST	192.168.2.7	8.8.8.8	0xb1a8	Standard query (0)	static.eldiario.es	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.107083082 CEST	192.168.2.7	8.8.8.8	0x8a3f	Standard query (0)	i.blogs.es	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.161470890 CEST	192.168.2.7	8.8.8.8	0xa15d	Standard query (0)	img.europapress.es	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.408689022 CEST	192.168.2.7	8.8.8.8	0x165e	Standard query (0)	static1.abc.es	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.409910917 CEST	192.168.2.7	8.8.8.8	0xc531	Standard query (0)	estaticos-cdn.elperiodico.com	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.440869093 CEST	192.168.2.7	8.8.8.8	0x62bc	Standard query (0)	media.revistagq.com	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.693485022 CEST	192.168.2.7	8.8.8.8	0x9fb7	Standard query (0)	www.meneame.net	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.031666994 CEST	192.168.2.7	8.8.8.8	0xc654	Standard query (0)	imagenes.20minutos.es	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.142452955 CEST	192.168.2.7	8.8.8.8	0x679c	Standard query (0)	s.libertaddigital.com	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.530837059 CEST	192.168.2.7	8.8.8.8	0x5356	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.634912968 CEST	192.168.2.7	8.8.8.8	0xbe4e	Standard query (0)	platform.twitter.com	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.749764919 CEST	192.168.2.7	8.8.8.8	0x75b0	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.752443075 CEST	192.168.2.7	8.8.8.8	0xc81c	Standard query (0)	static.hotjar.com	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.892232895 CEST	192.168.2.7	8.8.8.8	0xb76a	Standard query (0)	proteccion10.net	A (IP address)	IN (0x0001)
May 4, 2021 15:36:32.092113972 CEST	192.168.2.7	8.8.8.8	0x7751	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
May 4, 2021 15:36:32.289483070 CEST	192.168.2.7	8.8.8.8	0x2fef	Standard query (0)	script.hotjar.com	A (IP address)	IN (0x0001)
May 4, 2021 15:36:32.952897072 CEST	192.168.2.7	8.8.8.8	0xd831	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
May 4, 2021 15:36:32.970494986 CEST	192.168.2.7	8.8.8.8	0x3350	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
May 4, 2021 15:36:33.030216932 CEST	192.168.2.7	8.8.8.8	0x3ccf	Standard query (0)	adservice.google.de	A (IP address)	IN (0x0001)
May 4, 2021 15:36:33.167984962 CEST	192.168.2.7	8.8.8.8	0x78bf	Standard query (0)	www.googletagservices.com	A (IP address)	IN (0x0001)
May 4, 2021 15:36:33.699039936 CEST	192.168.2.7	8.8.8.8	0x932c	Standard query (0)	vars.hotjar.com	A (IP address)	IN (0x0001)
May 4, 2021 15:36:36.018068075 CEST	192.168.2.7	8.8.8.8	0xd1c3	Standard query (0)	in.hotjar.com	A (IP address)	IN (0x0001)
May 4, 2021 15:36:40.130274057 CEST	192.168.2.7	8.8.8.8	0xe17d	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
May 4, 2021 15:36:40.141700983 CEST	192.168.2.7	8.8.8.8	0x70e2	Standard query (0)	odr.mookie1.com	A (IP address)	IN (0x0001)
May 4, 2021 15:36:40.151976109 CEST	192.168.2.7	8.8.8.8	0x9cd	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 15:36:40.163346052 CEST	192.168.2.7	8.8.8.8	0x957e	Standard query (0)	image6.publ matic.com	A (IP address)	IN (0x0001)
May 4, 2021 15:36:40.184029102 CEST	192.168.2.7	8.8.8.8	0x983c	Standard query (0)	cm.g.doubl eclick.net	A (IP address)	IN (0x0001)
May 4, 2021 15:36:40.208612919 CEST	192.168.2.7	8.8.8.8	0x78f3	Standard query (0)	token.rubi conproject.com	A (IP address)	IN (0x0001)
May 4, 2021 15:36:47.636292934 CEST	192.168.2.7	8.8.8.8	0x120e	Standard query (0)	localcoron avirus.com	A (IP address)	IN (0x0001)
May 4, 2021 15:37:05.546082020 CEST	192.168.2.7	8.8.8.8	0x8f24	Standard query (0)	facebook.com	A (IP address)	IN (0x0001)
May 4, 2021 15:37:05.863600969 CEST	192.168.2.7	8.8.8.8	0xc107	Standard query (0)	m.facebook.com	A (IP address)	IN (0x0001)
May 4, 2021 15:37:06.182018042 CEST	192.168.2.7	8.8.8.8	0xca82	Standard query (0)	www.facebo ok.com	A (IP address)	IN (0x0001)
May 4, 2021 15:37:48.921555042 CEST	192.168.2.7	8.8.8.8	0x90a4	Standard query (0)	covid19tra cking.narr ativa.com	A (IP address)	IN (0x0001)
May 4, 2021 15:37:49.249552011 CEST	192.168.2.7	8.8.8.8	0xf633	Standard query (0)	kit.fontaw esome.com	A (IP address)	IN (0x0001)
May 4, 2021 15:37:49.259143114 CEST	192.168.2.7	8.8.8.8	0x2f46	Standard query (0)	4i2g925ohj .execute-api.eu-west-3.amazonaws.com	A (IP address)	IN (0x0001)
May 4, 2021 15:37:49.602268934 CEST	192.168.2.7	8.8.8.8	0x89ba	Standard query (0)	ka-f.fonta wesome.com	A (IP address)	IN (0x0001)
May 4, 2021 15:37:52.996649981 CEST	192.168.2.7	8.8.8.8	0x96d7	Standard query (0)	s01.europa press.net	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.165889978 CEST	192.168.2.7	8.8.8.8	0xabe	Standard query (0)	static3.abc.es	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.324820995 CEST	192.168.2.7	8.8.8.8	0x2b37	Standard query (0)	www.ecesta ticos.com	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.578241110 CEST	192.168.2.7	8.8.8.8	0xcc4d	Standard query (0)	eldiarioca ntabria.publico.es	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.633419037 CEST	192.168.2.7	8.8.8.8	0xe3ae	Standard query (0)	static.hos teltur.com	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.653141022 CEST	192.168.2.7	8.8.8.8	0x76bf	Standard query (0)	www.jornad a.com.mx	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.662055016 CEST	192.168.2.7	8.8.8.8	0xef11	Standard query (0)	img2.rtve.es	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.672657967 CEST	192.168.2.7	8.8.8.8	0x2d1e	Standard query (0)	navarra.el espanol.com	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.681974888 CEST	192.168.2.7	8.8.8.8	0xc28a	Standard query (0)	static4.abc.es	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.693798065 CEST	192.168.2.7	8.8.8.8	0x77e1	Standard query (0)	cronicaglo bal.elespa nol.com	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.725308895 CEST	192.168.2.7	8.8.8.8	0x813f	Standard query (0)	img.huffin gtonpost.com	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.768430948 CEST	192.168.2.7	8.8.8.8	0x56f5	Standard query (0)	phantom-el mundo.unid adeditorial.es	A (IP address)	IN (0x0001)
May 4, 2021 15:38:02.893307924 CEST	192.168.2.7	8.8.8.8	0x76c2	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
May 4, 2021 15:38:04.396384954 CEST	192.168.2.7	8.8.8.8	0x405c	Standard query (0)	c1.adform.net	A (IP address)	IN (0x0001)
May 4, 2021 15:38:05.240077972 CEST	192.168.2.7	8.8.8.8	0x2a67	Standard query (0)	eu-u.openx.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 15:36:29.211848021 CEST	8.8.8.8	192.168.2.7	0x49b6	No error (0)	localcoron avirus.com		104.21.18.245	A (IP address)	IN (0x0001)
May 4, 2021 15:36:29.211848021 CEST	8.8.8.8	192.168.2.7	0x49b6	No error (0)	localcoron avirus.com		172.67.183.244	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.128757954 CEST	8.8.8.8	192.168.2.7	0x2a84	No error (0)	www.republ ica.com	republica.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:30.128757954 CEST	8.8.8.8	192.168.2.7	0x2a84	No error (0)	republica.com		146.255.19.152	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.166285038 CEST	8.8.8.8	192.168.2.7	0x6ae7	No error (0)	www.lavozd egalicia.es	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 15:36:30.166285038 CEST	8.8.8.8	192.168.2.7	0x6ae7	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		52.210.129.255	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.166285038 CEST	8.8.8.8	192.168.2.7	0x6ae7	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		54.194.71.119	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.166285038 CEST	8.8.8.8	192.168.2.7	0x6ae7	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		52.211.67.210	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.166285038 CEST	8.8.8.8	192.168.2.7	0x6ae7	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		54.194.190.147	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.166285038 CEST	8.8.8.8	192.168.2.7	0x6ae7	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		34.249.141.22	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.166285038 CEST	8.8.8.8	192.168.2.7	0x6ae7	No error (0)	akavozpr-galicia-1149308574.eu-west-1.elb.amazonaws.com		52.211.217.51	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.168421030 CEST	8.8.8.8	192.168.2.7	0x8a3f	No error (0)	i.blogs.es	d1j70itqjm2icu.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:30.168421030 CEST	8.8.8.8	192.168.2.7	0x8a3f	No error (0)	d1j70itqjm2icu.cloudfront.net		13.225.74.97	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.168421030 CEST	8.8.8.8	192.168.2.7	0x8a3f	No error (0)	d1j70itqjm2icu.cloudfront.net		13.225.74.64	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.168421030 CEST	8.8.8.8	192.168.2.7	0x8a3f	No error (0)	d1j70itqjm2icu.cloudfront.net		13.225.74.3	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.168421030 CEST	8.8.8.8	192.168.2.7	0x8a3f	No error (0)	d1j70itqjm2icu.cloudfront.net		13.225.74.128	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.187474966 CEST	8.8.8.8	192.168.2.7	0xb1a8	No error (0)	static.eldiario.es	static.eldiario.es.cdn.bitban.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:30.187474966 CEST	8.8.8.8	192.168.2.7	0xb1a8	No error (0)	static.eldiario.es.cdn.bitban.net	caching.c19.edge2befaster.io		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:30.187474966 CEST	8.8.8.8	192.168.2.7	0xb1a8	No error (0)	caching.c19.edge2befaster.io	aec01.esg.eldiario.edgetcdn.io		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:30.187474966 CEST	8.8.8.8	192.168.2.7	0xb1a8	No error (0)	aec01.esg.eldiario.edgetcdn.io		84.17.62.22	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.187474966 CEST	8.8.8.8	192.168.2.7	0xb1a8	No error (0)	aec01.esg.eldiario.edgetcdn.io		84.17.62.23	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.221988916 CEST	8.8.8.8	192.168.2.7	0xa15d	No error (0)	img.europapress.es	d2dzdx91mh5kpx.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:30.221988916 CEST	8.8.8.8	192.168.2.7	0xa15d	No error (0)	d2dzdx91mh5kpx.cloudfront.net		13.224.193.96	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.221988916 CEST	8.8.8.8	192.168.2.7	0xa15d	No error (0)	d2dzdx91mh5kpx.cloudfront.net		13.224.193.112	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.221988916 CEST	8.8.8.8	192.168.2.7	0xa15d	No error (0)	d2dzdx91mh5kpx.cloudfront.net		13.224.193.60	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.221988916 CEST	8.8.8.8	192.168.2.7	0xa15d	No error (0)	d2dzdx91mh5kpx.cloudfront.net		13.224.193.101	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.479522943 CEST	8.8.8.8	192.168.2.7	0x165e	No error (0)	static1.abc.es	static.abc.es		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 15:36:30.479522943 CEST	8.8.8.8	192.168.2.7	0x165e	No error (0)	static.abc.es	static-abc.akamaized.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:30.495585918 CEST	8.8.8.8	192.168.2.7	0xc531	No error (0)	estaticos-cdn.elperiodico.com	prensaiberica.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:30.495585918 CEST	8.8.8.8	192.168.2.7	0xc531	No error (0)	prensaiberica.map.fastly.net		199.232.194.133	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.495585918 CEST	8.8.8.8	192.168.2.7	0xc531	No error (0)	prensaiberica.map.fastly.net		199.232.198.133	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.503468037 CEST	8.8.8.8	192.168.2.7	0x62bc	No error (0)	media.revistagq.com	cni-digital.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:30.503468037 CEST	8.8.8.8	192.168.2.7	0x62bc	No error (0)	cni-digital.map.fastly.net		151.101.2.133	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.503468037 CEST	8.8.8.8	192.168.2.7	0x62bc	No error (0)	cni-digital.map.fastly.net		151.101.66.133	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.503468037 CEST	8.8.8.8	192.168.2.7	0x62bc	No error (0)	cni-digital.map.fastly.net		151.101.130.133	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.503468037 CEST	8.8.8.8	192.168.2.7	0x62bc	No error (0)	cni-digital.map.fastly.net		151.101.194.133	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.753315926 CEST	8.8.8.8	192.168.2.7	0x9fb7	No error (0)	www.meneame.net		108.128.145.3	A (IP address)	IN (0x0001)
May 4, 2021 15:36:30.753315926 CEST	8.8.8.8	192.168.2.7	0x9fb7	No error (0)	www.meneame.net		52.212.89.238	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.097410917 CEST	8.8.8.8	192.168.2.7	0xc654	No error (0)	imagenes.20minutos.es	di7juyclzlgyp.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:31.097410917 CEST	8.8.8.8	192.168.2.7	0xc654	No error (0)	di7juyclzlgyp.cloudfront.net		13.225.74.87	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.097410917 CEST	8.8.8.8	192.168.2.7	0xc654	No error (0)	di7juyclzlgyp.cloudfront.net		13.225.74.99	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.097410917 CEST	8.8.8.8	192.168.2.7	0xc654	No error (0)	di7juyclzlgyp.cloudfront.net		13.225.74.23	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.097410917 CEST	8.8.8.8	192.168.2.7	0xc654	No error (0)	di7juyclzlgyp.cloudfront.net		13.225.74.48	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.199464083 CEST	8.8.8.8	192.168.2.7	0x679c	No error (0)	s.libertaddigital.com		213.149.255.231	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.593497992 CEST	8.8.8.8	192.168.2.7	0x5356	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:31.593497992 CEST	8.8.8.8	192.168.2.7	0x5356	No error (0)	scontent.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.693798065 CEST	8.8.8.8	192.168.2.7	0xbe4e	No error (0)	platform.twitter.com	cs472.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:31.693798065 CEST	8.8.8.8	192.168.2.7	0xbe4e	No error (0)	cs472.wac.edgecastcdn.net	cs1-apr-8315.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:31.693798065 CEST	8.8.8.8	192.168.2.7	0xbe4e	No error (0)	cs1-apr-8315.wac.edgecastcdn.net	wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:31.693798065 CEST	8.8.8.8	192.168.2.7	0xbe4e	No error (0)	cs1-lb-eu.8315.ecdns.net	cs41.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:31.693798065 CEST	8.8.8.8	192.168.2.7	0xbe4e	No error (0)	cs41.wac.edgecastcdn.net		93.184.220.66	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.800357103 CEST	8.8.8.8	192.168.2.7	0x75b0	No error (0)	cdn.jsdelivr.net	dualstack.f3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:31.844305992 CEST	8.8.8.8	192.168.2.7	0xc81c	No error (0)	static.hotjar.com	static-cdn.hotjar.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 15:36:31.844305992 CEST	8.8.8.8	192.168.2.7	0xc81c	No error (0)	static-cdn .hotjar.com		13.225.74.30	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.844305992 CEST	8.8.8.8	192.168.2.7	0xc81c	No error (0)	static-cdn .hotjar.com		13.225.74.66	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.844305992 CEST	8.8.8.8	192.168.2.7	0xc81c	No error (0)	static-cdn .hotjar.com		13.225.74.74	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.844305992 CEST	8.8.8.8	192.168.2.7	0xc81c	No error (0)	static-cdn .hotjar.com		13.225.74.20	A (IP address)	IN (0x0001)
May 4, 2021 15:36:31.985969067 CEST	8.8.8.8	192.168.2.7	0xb76a	No error (0)	proteccion10.net		193.32.242.105	A (IP address)	IN (0x0001)
May 4, 2021 15:36:32.148977041 CEST	8.8.8.8	192.168.2.7	0x7751	No error (0)	googleads. g.doubleclick.net		142.250.185.194	A (IP address)	IN (0x0001)
May 4, 2021 15:36:32.349493980 CEST	8.8.8.8	192.168.2.7	0x2fef	No error (0)	script.hotjar.com		13.224.193.122	A (IP address)	IN (0x0001)
May 4, 2021 15:36:32.349493980 CEST	8.8.8.8	192.168.2.7	0x2fef	No error (0)	script.hotjar.com		13.224.193.31	A (IP address)	IN (0x0001)
May 4, 2021 15:36:32.349493980 CEST	8.8.8.8	192.168.2.7	0x2fef	No error (0)	script.hotjar.com		13.224.193.121	A (IP address)	IN (0x0001)
May 4, 2021 15:36:32.349493980 CEST	8.8.8.8	192.168.2.7	0x2fef	No error (0)	script.hotjar.com		13.224.193.38	A (IP address)	IN (0x0001)
May 4, 2021 15:36:33.009809971 CEST	8.8.8.8	192.168.2.7	0xd831	No error (0)	stats.g.do ubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:33.009809971 CEST	8.8.8.8	192.168.2.7	0xd831	No error (0)	stats.l.do ubleclick.net		74.125.133.155	A (IP address)	IN (0x0001)
May 4, 2021 15:36:33.009809971 CEST	8.8.8.8	192.168.2.7	0xd831	No error (0)	stats.l.do ubleclick.net		74.125.133.157	A (IP address)	IN (0x0001)
May 4, 2021 15:36:33.009809971 CEST	8.8.8.8	192.168.2.7	0xd831	No error (0)	stats.l.do ubleclick.net		74.125.133.154	A (IP address)	IN (0x0001)
May 4, 2021 15:36:33.009809971 CEST	8.8.8.8	192.168.2.7	0xd831	No error (0)	stats.l.do ubleclick.net		74.125.133.156	A (IP address)	IN (0x0001)
May 4, 2021 15:36:33.030790091 CEST	8.8.8.8	192.168.2.7	0x3350	No error (0)	www.google.de		142.250.185.227	A (IP address)	IN (0x0001)
May 4, 2021 15:36:33.058743954 CEST	8.8.8.8	192.168.2.7	0x426f	No error (0)	partnerad. l.doubleclick.net		142.250.185.194	A (IP address)	IN (0x0001)
May 4, 2021 15:36:33.098334074 CEST	8.8.8.8	192.168.2.7	0x3ccf	No error (0)	adservice. google.de	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:33.098334074 CEST	8.8.8.8	192.168.2.7	0x3ccf	No error (0)	pagead46.l .doubleclick.net		142.250.186.162	A (IP address)	IN (0x0001)
May 4, 2021 15:36:33.233313084 CEST	8.8.8.8	192.168.2.7	0x78bf	No error (0)	www.google tagservices.com		142.250.186.34	A (IP address)	IN (0x0001)
May 4, 2021 15:36:33.763566971 CEST	8.8.8.8	192.168.2.7	0x932c	No error (0)	vars.hotjar.com		13.224.193.73	A (IP address)	IN (0x0001)
May 4, 2021 15:36:33.763566971 CEST	8.8.8.8	192.168.2.7	0x932c	No error (0)	vars.hotjar.com		13.224.193.91	A (IP address)	IN (0x0001)
May 4, 2021 15:36:33.763566971 CEST	8.8.8.8	192.168.2.7	0x932c	No error (0)	vars.hotjar.com		13.224.193.12	A (IP address)	IN (0x0001)
May 4, 2021 15:36:33.763566971 CEST	8.8.8.8	192.168.2.7	0x932c	No error (0)	vars.hotjar.com		13.224.193.116	A (IP address)	IN (0x0001)
May 4, 2021 15:36:36.068947077 CEST	8.8.8.8	192.168.2.7	0xd1c3	No error (0)	in.hotjar.com	in-live.live.eks.hotjar.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:36.068947077 CEST	8.8.8.8	192.168.2.7	0xd1c3	No error (0)	in-live.li ve.eks.hot jar.com		63.33.16.37	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 15:36:36.068947077 CEST	8.8.8.8	192.168.2.7	0xd1c3	No error (0)	in-live.live.eks.hotjar.com		52.51.23.49	A (IP address)	IN (0x0001)
May 4, 2021 15:36:36.068947077 CEST	8.8.8.8	192.168.2.7	0xd1c3	No error (0)	in-live.live.eks.hotjar.com		34.252.74.75	A (IP address)	IN (0x0001)
May 4, 2021 15:36:36.068947077 CEST	8.8.8.8	192.168.2.7	0xd1c3	No error (0)	in-live.live.eks.hotjar.com		52.208.57.208	A (IP address)	IN (0x0001)
May 4, 2021 15:36:36.068947077 CEST	8.8.8.8	192.168.2.7	0xd1c3	No error (0)	in-live.live.eks.hotjar.com		52.49.237.17	A (IP address)	IN (0x0001)
May 4, 2021 15:36:36.068947077 CEST	8.8.8.8	192.168.2.7	0xd1c3	No error (0)	in-live.live.eks.hotjar.com		54.171.249.106	A (IP address)	IN (0x0001)
May 4, 2021 15:36:36.068947077 CEST	8.8.8.8	192.168.2.7	0xd1c3	No error (0)	in-live.live.eks.hotjar.com		52.18.148.102	A (IP address)	IN (0x0001)
May 4, 2021 15:36:36.068947077 CEST	8.8.8.8	192.168.2.7	0xd1c3	No error (0)	in-live.live.eks.hotjar.com		52.19.70.84	A (IP address)	IN (0x0001)
May 4, 2021 15:36:40.189614058 CEST	8.8.8.8	192.168.2.7	0xe17d	No error (0)	id.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
May 4, 2021 15:36:40.190546036 CEST	8.8.8.8	192.168.2.7	0x70e2	No error (0)	odr.mookie1.com	tagr-gcp-odr-euw4.mookie1.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:40.190546036 CEST	8.8.8.8	192.168.2.7	0x70e2	No error (0)	tagr-gcp-odr-euw4.mookie1.com		34.98.67.61	A (IP address)	IN (0x0001)
May 4, 2021 15:36:40.203394890 CEST	8.8.8.8	192.168.2.7	0x9cd	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
May 4, 2021 15:36:40.203394890 CEST	8.8.8.8	192.168.2.7	0x9cd	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
May 4, 2021 15:36:40.211981058 CEST	8.8.8.8	192.168.2.7	0x957e	No error (0)	image6.pubmatic.com	pugm22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:40.211981058 CEST	8.8.8.8	192.168.2.7	0x957e	No error (0)	pugm22000nfc.pubmatic.com	pugm22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:40.211981058 CEST	8.8.8.8	192.168.2.7	0x957e	No error (0)	pugm22000nf.pubmatic.com		185.64.189.115	A (IP address)	IN (0x0001)
May 4, 2021 15:36:40.249142885 CEST	8.8.8.8	192.168.2.7	0x983c	No error (0)	cm.g.doubleclick.net		142.250.185.226	A (IP address)	IN (0x0001)
May 4, 2021 15:36:40.289413929 CEST	8.8.8.8	192.168.2.7	0x78f3	No error (0)	token.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:36:47.699398041 CEST	8.8.8.8	192.168.2.7	0x120e	No error (0)	localcoronavirus.com		172.67.183.244	A (IP address)	IN (0x0001)
May 4, 2021 15:36:47.699398041 CEST	8.8.8.8	192.168.2.7	0x120e	No error (0)	localcoronavirus.com		104.21.18.245	A (IP address)	IN (0x0001)
May 4, 2021 15:37:05.618727922 CEST	8.8.8.8	192.168.2.7	0x8f24	No error (0)	facebook.com		31.13.92.36	A (IP address)	IN (0x0001)
May 4, 2021 15:37:05.922939062 CEST	8.8.8.8	192.168.2.7	0xc107	No error (0)	m.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:05.922939062 CEST	8.8.8.8	192.168.2.7	0xc107	No error (0)	star-mini.c10r.facebook.com		31.13.92.36	A (IP address)	IN (0x0001)
May 4, 2021 15:37:06.248045921 CEST	8.8.8.8	192.168.2.7	0xca82	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:06.248045921 CEST	8.8.8.8	192.168.2.7	0xca82	No error (0)	star-mini.c10r.facebook.com		31.13.92.36	A (IP address)	IN (0x0001)
May 4, 2021 15:37:48.988209009 CEST	8.8.8.8	192.168.2.7	0x90a4	No error (0)	covid19tracking.narrativa.com	d2jcax5o6gwtn6.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:48.988209009 CEST	8.8.8.8	192.168.2.7	0x90a4	No error (0)	d2jcax5o6gwtn6.cloudfront.net		143.204.98.33	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 15:37:48.988209009 CEST	8.8.8.8	192.168.2.7	0x90a4	No error (0)	d2jcax5o6gwtn6.cloudfront.net		143.204.98.44	A (IP address)	IN (0x0001)
May 4, 2021 15:37:48.988209009 CEST	8.8.8.8	192.168.2.7	0x90a4	No error (0)	d2jcax5o6gwtn6.cloudfront.net		143.204.98.2	A (IP address)	IN (0x0001)
May 4, 2021 15:37:48.988209009 CEST	8.8.8.8	192.168.2.7	0x90a4	No error (0)	d2jcax5o6gwtn6.cloudfront.net		143.204.98.97	A (IP address)	IN (0x0001)
May 4, 2021 15:37:49.313894033 CEST	8.8.8.8	192.168.2.7	0xf633	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:49.321712017 CEST	8.8.8.8	192.168.2.7	0x2f46	No error (0)	4i2g925ohj.execute-api.eu-west-3.amazonaws.com		13.225.74.124	A (IP address)	IN (0x0001)
May 4, 2021 15:37:49.321712017 CEST	8.8.8.8	192.168.2.7	0x2f46	No error (0)	4i2g925ohj.execute-api.eu-west-3.amazonaws.com		13.225.74.55	A (IP address)	IN (0x0001)
May 4, 2021 15:37:49.321712017 CEST	8.8.8.8	192.168.2.7	0x2f46	No error (0)	4i2g925ohj.execute-api.eu-west-3.amazonaws.com		13.225.74.123	A (IP address)	IN (0x0001)
May 4, 2021 15:37:49.321712017 CEST	8.8.8.8	192.168.2.7	0x2f46	No error (0)	4i2g925ohj.execute-api.eu-west-3.amazonaws.com		13.225.74.113	A (IP address)	IN (0x0001)
May 4, 2021 15:37:49.665277958 CEST	8.8.8.8	192.168.2.7	0x89ba	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.059221029 CEST	8.8.8.8	192.168.2.7	0x96d7	No error (0)	s01.europapress.net	d1gubrkaoxki64.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.059221029 CEST	8.8.8.8	192.168.2.7	0x96d7	No error (0)	d1gubrkaoxki64.cloudfront.net		13.225.74.27	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.059221029 CEST	8.8.8.8	192.168.2.7	0x96d7	No error (0)	d1gubrkaoxki64.cloudfront.net		13.225.74.73	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.059221029 CEST	8.8.8.8	192.168.2.7	0x96d7	No error (0)	d1gubrkaoxki64.cloudfront.net		13.225.74.32	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.059221029 CEST	8.8.8.8	192.168.2.7	0x96d7	No error (0)	d1gubrkaoxki64.cloudfront.net		13.225.74.76	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.224966049 CEST	8.8.8.8	192.168.2.7	0xabe	No error (0)	static3.abc.es	static.abc.es		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.224966049 CEST	8.8.8.8	192.168.2.7	0xabe	No error (0)	static.abc.es	static-abc.akamaized.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.398495913 CEST	8.8.8.8	192.168.2.7	0x2b37	No error (0)	www.ecesticos.com	cdn2_incap2.titania.es		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.398495913 CEST	8.8.8.8	192.168.2.7	0x2b37	No error (0)	cdn2_incap2.titania.es	caching.elconfidencial.edge2befaster.io		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.398495913 CEST	8.8.8.8	192.168.2.7	0x2b37	No error (0)	caching.elconfidencial.edge2befaster.io	caching.meta-cluster-04.edge2befaster.io		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.398495913 CEST	8.8.8.8	192.168.2.7	0x2b37	No error (0)	caching.meta-cluster-04.edge2befaster.io	cec01.eug.edgetcdn.io		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.398495913 CEST	8.8.8.8	192.168.2.7	0x2b37	No error (0)	cec01.eug.edgetcdn.io		51.255.81.138	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.398495913 CEST	8.8.8.8	192.168.2.7	0x2b37	No error (0)	cec01.eug.edgetcdn.io		51.68.35.185	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.647227049 CEST	8.8.8.8	192.168.2.7	0xcc4d	No error (0)	eldiariocantabria.publico.es	eldiariocantabria.publico.es.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.713972092 CEST	8.8.8.8	192.168.2.7	0xe3ae	No error (0)	static.hosteltur.com	z30hostelturelb01.srv.joopbox.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 15:37:53.713972092 CEST	8.8.8.8	192.168.2.7	0xe3ae	No error (0)	z30hostelturelb01.srv.joopbox.com	ec2-34-243-184-100.eu-west-1.compute.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.713972092 CEST	8.8.8.8	192.168.2.7	0xe3ae	No error (0)	ec2-34-243-184-100.eu-west-1.compute.amazonaws.com		34.243.184.100	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.717144966 CEST	8.8.8.8	192.168.2.7	0x76bf	No error (0)	www.jornada.com.mx	www.jornada.com.mx.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.732680082 CEST	8.8.8.8	192.168.2.7	0x2d1e	No error (0)	navarra.elespanol.com	navarra.elespanol.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.748311996 CEST	8.8.8.8	192.168.2.7	0xef11	No error (0)	img2.rtve.es	caching.c251.edge2befaster.io		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.748311996 CEST	8.8.8.8	192.168.2.7	0xef11	No error (0)	caching.c251.edge2befaster.io	aec01.esg.rtve.edgetcdn.io		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.748311996 CEST	8.8.8.8	192.168.2.7	0xef11	No error (0)	aec01.esg.rtve.edgetcdn.io		185.57.173.170	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.748311996 CEST	8.8.8.8	192.168.2.7	0xef11	No error (0)	aec01.esg.rtve.edgetcdn.io		51.210.220.43	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.748311996 CEST	8.8.8.8	192.168.2.7	0xef11	No error (0)	aec01.esg.rtve.edgetcdn.io		51.195.63.235	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.748311996 CEST	8.8.8.8	192.168.2.7	0xef11	No error (0)	aec01.esg.rtve.edgetcdn.io		51.210.220.45	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.748311996 CEST	8.8.8.8	192.168.2.7	0xef11	No error (0)	aec01.esg.rtve.edgetcdn.io		51.89.235.116	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.748311996 CEST	8.8.8.8	192.168.2.7	0xef11	No error (0)	aec01.esg.rtve.edgetcdn.io		185.103.37.61	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.748311996 CEST	8.8.8.8	192.168.2.7	0xef11	No error (0)	aec01.esg.rtve.edgetcdn.io		185.103.37.59	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.748311996 CEST	8.8.8.8	192.168.2.7	0xef11	No error (0)	aec01.esg.rtve.edgetcdn.io		51.195.63.237	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.748311996 CEST	8.8.8.8	192.168.2.7	0xef11	No error (0)	aec01.esg.rtve.edgetcdn.io		51.89.172.162	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.748311996 CEST	8.8.8.8	192.168.2.7	0xef11	No error (0)	aec01.esg.rtve.edgetcdn.io		185.99.186.203	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.748311996 CEST	8.8.8.8	192.168.2.7	0xef11	No error (0)	aec01.esg.rtve.edgetcdn.io		185.103.37.62	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.777674913 CEST	8.8.8.8	192.168.2.7	0x77e1	No error (0)	cronicaglobal.elespanol.com	caching.elespanol.edge2befaster.io		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.777674913 CEST	8.8.8.8	192.168.2.7	0x77e1	No error (0)	caching.elespanol.edge2befaster.io	caching.meta-cluster-03.edge2befaster.io		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.777674913 CEST	8.8.8.8	192.168.2.7	0x77e1	No error (0)	caching.meta-cluster-03.edge2befaster.io	cec01.eug.edgetcdn.io		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.777674913 CEST	8.8.8.8	192.168.2.7	0x77e1	No error (0)	cec01.eug.edgetcdn.io		51.255.81.138	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.777674913 CEST	8.8.8.8	192.168.2.7	0x77e1	No error (0)	cec01.eug.edgetcdn.io		51.68.35.185	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.783550978 CEST	8.8.8.8	192.168.2.7	0xc28a	No error (0)	static4.abc.es	static.abc.es		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.783550978 CEST	8.8.8.8	192.168.2.7	0xc28a	No error (0)	static.abc.es	static-abc.akamaized.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.788677931 CEST	8.8.8.8	192.168.2.7	0x813f	No error (0)	img.huffingtonpost.com	cs491300.wpc.mucdn.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 15:37:53.788677931 CEST	8.8.8.8	192.168.2.7	0x813f	No error (0)	cs491300.wpc.mucdn.net		192.229.220.196	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.833760023 CEST	8.8.8.8	192.168.2.7	0x56f5	No error (0)	phantom-elmundo.unidadeditorial.es	dbpabf0off7y1.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:37:53.833760023 CEST	8.8.8.8	192.168.2.7	0x56f5	No error (0)	dbpabf0off7y1.cloudfront.net		13.224.193.117	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.833760023 CEST	8.8.8.8	192.168.2.7	0x56f5	No error (0)	dbpabf0off7y1.cloudfront.net		13.224.193.123	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.833760023 CEST	8.8.8.8	192.168.2.7	0x56f5	No error (0)	dbpabf0off7y1.cloudfront.net		13.224.193.26	A (IP address)	IN (0x0001)
May 4, 2021 15:37:53.833760023 CEST	8.8.8.8	192.168.2.7	0x56f5	No error (0)	dbpabf0off7y1.cloudfront.net		13.224.193.11	A (IP address)	IN (0x0001)
May 4, 2021 15:38:02.941955090 CEST	8.8.8.8	192.168.2.7	0x76c2	No error (0)	match.adsrvr.org	match-1943069928.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:38:02.941955090 CEST	8.8.8.8	192.168.2.7	0x76c2	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		54.76.6.247	A (IP address)	IN (0x0001)
May 4, 2021 15:38:02.941955090 CEST	8.8.8.8	192.168.2.7	0x76c2	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.211.206.55	A (IP address)	IN (0x0001)
May 4, 2021 15:38:02.941955090 CEST	8.8.8.8	192.168.2.7	0x76c2	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		63.33.11.43	A (IP address)	IN (0x0001)
May 4, 2021 15:38:02.941955090 CEST	8.8.8.8	192.168.2.7	0x76c2	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.208.69.189	A (IP address)	IN (0x0001)
May 4, 2021 15:38:02.941955090 CEST	8.8.8.8	192.168.2.7	0x76c2	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		34.250.26.236	A (IP address)	IN (0x0001)
May 4, 2021 15:38:02.941955090 CEST	8.8.8.8	192.168.2.7	0x76c2	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.210.202.173	A (IP address)	IN (0x0001)
May 4, 2021 15:38:02.941955090 CEST	8.8.8.8	192.168.2.7	0x76c2	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.215.57.184	A (IP address)	IN (0x0001)
May 4, 2021 15:38:02.941955090 CEST	8.8.8.8	192.168.2.7	0x76c2	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.30.186.230	A (IP address)	IN (0x0001)
May 4, 2021 15:38:04.476283073 CEST	8.8.8.8	192.168.2.7	0x405c	No error (0)	c1.adform.net	track.adformnet.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:38:05.291500092 CEST	8.8.8.8	192.168.2.7	0x2a67	No error (0)	eu-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
May 4, 2021 15:38:05.291500092 CEST	8.8.8.8	192.168.2.7	0x2a67	No error (0)	eu-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- localcoronavirus.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49696	104.21.18.245	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 15:36:29.276551008 CEST	485	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 4, 2021 15:36:29.335083961 CEST	488	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 04 May 2021 13:36:29 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Tue, 04 May 2021 14:36:29 GMT Location: https://localcoronavirus.com/ cf-request-id: 09d931407f00002c0da4863000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=aIWllRvW61PajfW3r9afja%2FApQy7pq5XoI9Jkv9JQX6Cz8RPxs6pF3cVR%2Fouzj8pyJ70IIugm48Fp3Pa7VdUr6GUCmIc%2BvZk7zmhsCtAiwoMIJu7rQ%3D%3D"}]} NEL: {"max_age":604800,"report_to":"cf-nel"} Vary: Accept-Encoding Server: cloudflare CF-RAY: 64a21e473abe2c0d-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:36:29.437350988 CEST	104.21.18.245	443	192.168.2.7	49698	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	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
May 4, 2021 15:36:30.309024096 CEST	13.225.74.97	443	192.168.2.7	49713	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	Mon Mar 07 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
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 15:36:30.331365108 CEST	13.225.74.97	443	192.168.2.7	49712	CN=*.blogs.es CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Feb 05 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Mar 07 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 15:36:30.350061893 CEST	146.255.19.152	443	192.168.2.7	49708	CN=republica.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 04 11:00:51 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed May 05 12:00:51 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 4, 2021 15:36:30.350652933 CEST	52.210.129.255	443	192.168.2.7	49711	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:36:30.453303099 CEST	146.255.19.152	443	192.168.2.7	49709	CN=republica.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 04 11:00:51 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed May 05 12:00:51 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 4, 2021 15:36:30.454461098 CEST	52.210.129.255	443	192.168.2.7	49710	CN=*.lavozdegalicia.es, OU=PremiumSSL Legacy Wildcard, O=LA VOZ DE GALICIA S.A., STREET="RONDA DE OUTEIRO, 1 - 3 BAJO", L=A CORUNA, ST=La Corua, OID.2.5.4.17=15006, C=ES CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Thu Oct 17 02:00:00 CEST 2019 Fri Nov 02 01:00:00 CET 2018	Tue Jan 18 01:00:00 CET 2022 Wed Jan 01 00:59:59 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
May 4, 2021 15:36:30.477521896 CEST	13.224.193.96	443	192.168.2.7	49716	CN=img.europapress.es CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue Jun 16 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Fri Jul 16 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:36:30.477920055 CEST	13.224.193.96	443	192.168.2.7	49717	CN=img.europapress.es CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue Jun 16 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Fri Jul 16 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 15:36:30.499216080 CEST	13.224.193.96	443	192.168.2.7	49718	CN=img.europapress.es CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue Jun 16 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Fri Jul 16 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:36:30.501130104 CEST	84.17.62.22	443	192.168.2.7	49715	CN=15m2016.eldiario.es CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 25 23:25:48 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Thu Jun 24 00:25:48 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 4, 2021 15:36:30.503489971 CEST	84.17.62.22	443	192.168.2.7	49714	CN=15m2016.eldiario.es CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 25 23:25:48 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Thu Jun 24 00:25:48 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 4, 2021 15:36:30.621027946 CEST	199.232.194.133	443	192.168.2.7	49721	CN=*.albaeditorial.es CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Apr 26 22:21:49 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sat May 28 22:21:48 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
May 4, 2021 15:36:30.621704102 CEST	199.232.194.133	443	192.168.2.7	49722	CN=*.albaeditorial.es CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Apr 26 22:21:49 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sat May 28 22:21:48 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
May 4, 2021 15:36:30.624413967 CEST	151.101.2.133	443	192.168.2.7	49723	CN=cni-digital1.map.fastly.net, O="Fastly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Mar 29 18:12:10 CEST 2021 Wed Aug 19 02:00:00 CEST 2015	Sat Mar 26 14:09:35 CET 2022 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:36:30.625174999 CEST	151.101.2.133	443	192.168.2.7	49724	CN=cni-digital1.map.fastly.net, O="Fastly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Mar 29 18:12:10 CEST 2021	Sat Mar 26 14:09:35 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
							Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
May 4, 2021 15:36:31.052651882 CEST	108.128.145.3	443	192.168.2.7	49726	CN=meneame.net CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sat Jan 02 01:00:00 CET 2021	Tue Feb 01 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 Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
							Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
							Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 15:36:31.054713011 CEST	108.128.145.3	443	192.168.2.7	49725	CN=meneame.net CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sat Jan 02 01:00:00 CET 2021	Tue Feb 01 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 Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
							Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
							Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 15:36:31.187627077 CEST	13.225.74.87	443	192.168.2.7	49728	CN=*.20minutos.es CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Apr 05 02:00:00 CEST 2021 Mon Nov 06 13:23:52 CET 2017	Mon Apr 25 01:59:59 CEST 2022 Sat Nov 06 13:23:52 CET 2027	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:52 CET 2017	Sat Nov 06 13:23:52 CET 2027		
May 4, 2021 15:36:31.188009024 CEST	13.225.74.87	443	192.168.2.7	49727	CN=*.20minutos.es CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Apr 05 02:00:00 CEST 2021 Mon Nov 06 13:23:52 CET 2017	Mon Apr 25 01:59:59 CEST 2022 Sat Nov 06 13:23:52 CET 2027	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Thawte RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:52 CET 2017	Sat Nov 06 13:23:52 CET 2027		
May 4, 2021 15:36:31.681458950 CEST	31.13.92.14	443	192.168.2.7	49731	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Apr 06 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Sun Jul 04 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 4, 2021 15:36:31.683847904 CEST	31.13.92.14	443	192.168.2.7	49732	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Apr 06 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Sun Jul 04 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 4, 2021 15:36:31.814009905 CEST	93.184.220.66	443	192.168.2.7	49734	CN=*.twimg.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 05 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Wed Nov 10 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Copyright Joe Security LLC 2021

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:36:31.814501047 CEST	93.184.220.66	443	192.168.2.7	49733	CN=*.twimg.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 05 01:00:00 CET 2020	Wed Nov 10 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 4, 2021 15:36:31.969197989 CEST	13.225.74.30	443	192.168.2.7	49738	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	Mon Jan 24 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
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 15:36:31.970489025 CEST	13.225.74.30	443	192.168.2.7	49737	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	Mon Jan 24 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
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 15:36:32.328697920 CEST	142.250.185.194	443	192.168.2.7	49748	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:36:35 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:36:34 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 4, 2021 15:36:32.330595970 CEST	142.250.185.194	443	192.168.2.7	49747	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:36:35 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:36:34 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 4, 2021 15:36:32.391237020 CEST	193.32.242.105	443	192.168.2.7	49746	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 4, 2021 15:36:32.391607046 CEST	193.32.242.105	443	192.168.2.7	49745	CN=proteccion10.net CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Mar 24 02:05:17 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 22 03:05:17 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:36:32.468189001 CEST	13.224.193.122	443	192.168.2.7	49749	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 15:36:32.473661900 CEST	13.224.193.122	443	192.168.2.7	49750	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:36:33.119812965 CEST	74.125.133.155	443	192.168.2.7	49753	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Apr 13 12:11:12 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:11:11 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
May 4, 2021 15:36:33.121623039 CEST	74.125.133.155	443	192.168.2.7	49754	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Apr 13 12:11:12 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:11:11 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
May 4, 2021 15:36:33.141391993 CEST	142.250.185.227	443	192.168.2.7	49756	CN=www.google.de CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:41:49 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:41:48 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 4, 2021 15:36:33.147326946 CEST	142.250.185.227	443	192.168.2.7	49755	CN=www.google.de CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:41:49 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:41:48 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:36:33.166636944 CEST	142.250.185.194	443	192.168.2.7	49757	CN=*.googleadservices.com CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:40:58 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:40:57 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 4, 2021 15:36:33.167541981 CEST	142.250.185.194	443	192.168.2.7	49758	CN=*.googleadservices.com CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:40:58 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:40:57 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 4, 2021 15:36:33.210526943 CEST	142.250.186.162	443	192.168.2.7	49762	CN=*.google.de CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:46:01 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:46:00 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:36:33.213691950 CEST	142.250.186.162	443	192.168.2.7	49761	CN=*.google.de CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:46:01 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:46:00 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 4, 2021 15:36:33.342432022 CEST	142.250.186.34	443	192.168.2.7	49764	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:36:35 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:36:34 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 4, 2021 15:36:33.347033978 CEST	142.250.186.34	443	192.168.2.7	49763	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:36:35 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:36:34 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:36:33.853586912 CEST	13.224.193.73	443	192.168.2.7	49765	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 15:36:33.855081081 CEST	13.224.193.73	443	192.168.2.7	49766	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:36:36.207231998 CEST	63.33.16.37	443	192.168.2.7	49776	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	Sat Aug 29 02:00:00 CEST 2020	Tue Sep 28 14:00:00 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 15:36:40.275296926 CEST	34.98.67.61	443	192.168.2.7	49777	CN=*.mookie1.com, O=Xaxis LLC, L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Feb 22 01:00:00 CET 2021	Sat Mar 26 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
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 4, 2021 15:36:40.275747061 CEST	34.98.67.61	443	192.168.2.7	49778	CN=*.mookie1.com, O=Xaxis LLC, L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Feb 22 01:00:00 CET 2021	Sat Mar 26 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
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:36:40.296380997 CEST	35.244.174.68	443	192.168.2.7	49779	CN=*.rlcdn.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Feb 25 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Tue Mar 29 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 4, 2021 15:36:40.304754972 CEST	35.244.174.68	443	192.168.2.7	49780	CN=*.rlcdn.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Feb 25 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Tue Mar 29 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:36:40.305223942 CEST	35.244.159.8	443	192.168.2.7	49781	CN=*.openx.net, O=OpenX Technologies inc., L=Pasadena, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jun 18 02:00:00 CEST 2020 Mon Nov 06 13:23:45 CET 2017 Fri Nov 10 01:00:00 CET 2006	Tue Aug 17 14:00:00 CEST 2021 Sat Nov 06 13:23:45 CET 2027 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 4, 2021 15:36:40.309041977 CEST	185.64.189.115	443	192.168.2.7	49784	CN=*.pubmatic.com, O="PubMatic, Inc.", L=Redwood City, ST=California, C=US CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Dec 07 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri May 12 20:46:00 CEST 2000	Wed Dec 15 00:59:59 CET 2021 Mon May 12 01:59:59 CEST 2025 Tue May 13 01:59:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Sep 24 02:00:00 CEST 2020	Mon May 12 01:59:59 CEST 2025		
					CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri May 12 20:46:00 CEST 2000	Tue May 13 01:59:00 CEST 2025		
May 4, 2021 15:36:40.309175968 CEST	185.64.189.115	443	192.168.2.7	49783	CN=*.pubmatic.com, O="PubMatic, Inc.", L=Redwood City, ST=California, C=US CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Dec 07 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri May 12 20:46:00 CEST 2000	Wed Dec 15 00:59:59 CET 2021 Mon May 12 01:59:59 CEST 2025 Tue May 13 01:59:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Sep 24 02:00:00 CEST 2020	Mon May 12 01:59:59 CEST 2025		
					CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri May 12 20:46:00 CEST 2000	Tue May 13 01:59:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:36:40.312566042 CEST	35.244.159.8	443	192.168.2.7	49782	CN=*.openx.net, O=OpenX Technologies inc., L=Pasadena, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jun 18 02:00:00 CEST 2020 Mon Nov 06 13:23:45 CET 2017 Fri Nov 10 01:00:00 CET 2006	Tue Aug 17 14:00:00 CEST 2021 Sat Nov 06 13:23:45 CET 2027 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 4, 2021 15:36:40.459625959 CEST	142.250.185.226	443	192.168.2.7	49785	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:36:35 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:36:34 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 4, 2021 15:36:40.460074902 CEST	142.250.185.226	443	192.168.2.7	49786	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:36:35 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:36:34 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		

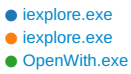
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:37:05.705409050 CEST	31.13.92.36	443	192.168.2.7	49798	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Apr 06 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Sun Jul 04 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 4, 2021 15:37:05.706103086 CEST	31.13.92.36	443	192.168.2.7	49797	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Apr 06 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Sun Jul 04 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 4, 2021 15:37:06.047959089 CEST	31.13.92.36	443	192.168.2.7	49799	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Apr 06 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Sun Jul 04 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 4, 2021 15:37:06.048122883 CEST	31.13.92.36	443	192.168.2.7	49800	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Apr 06 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Sun Jul 04 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 4, 2021 15:37:06.334851027 CEST	31.13.92.36	443	192.168.2.7	49802	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 4, 2021 15:37:06.335141897 CEST	31.13.92.36	443	192.168.2.7	49801	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Apr 06 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Sun Jul 04 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 2960 Parent PID: 792

General

Start time:	15:36:26
Start date:	04/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6be330000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Copyright Joe Security LLC 2021

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: 5880 Parent PID: 2960

General

Start time:	15:36:27
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2960 CREDAT:17410 /prefetch:2
Imagebase:	0x290000
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: 4880 Parent PID: 792

General

Start time:	15:37:46
Start date:	04/05/2021
Path:	C:\Windows\System32\OpenWith.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\OpenWith.exe -Embedding
Imagebase:	0x7ff61ae90000
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