ID: 423643
Cookbook: browseurl.jbs
Time: 09:20:52
Date: 25/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

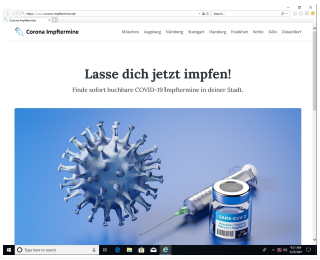
Analysis Report https://www.corona-impftermine.net/

Overview

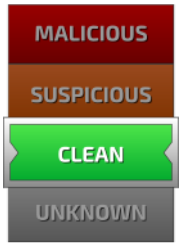
General Information

Sample URL:	http://https://www.corona-impftermine.net/
Analysis ID:	423643
Infos:	

Most interesting Screenshot:



Detection

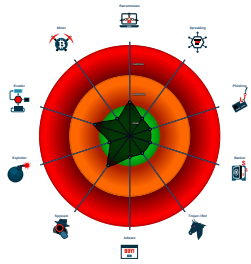


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Contains capabilities to detect virtua…
- Monitors certain registry keys / valu…
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 5792 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5100 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5792 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- OpenWith.exe (PID: 6164 cmdline: C:\Windows\system32\OpenWith.exe -Embedding MD5: D179D03728E95E040A889F760C1FC402)
- OpenWith.exe (PID: 7060 cmdline: C:\Windows\system32\OpenWith.exe -Embedding MD5: D179D03728E95E040A889F760C1FC402)
- **cleanup**

Malware Configuration

No configs have been found

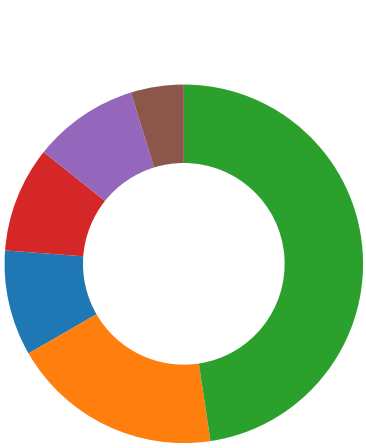
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



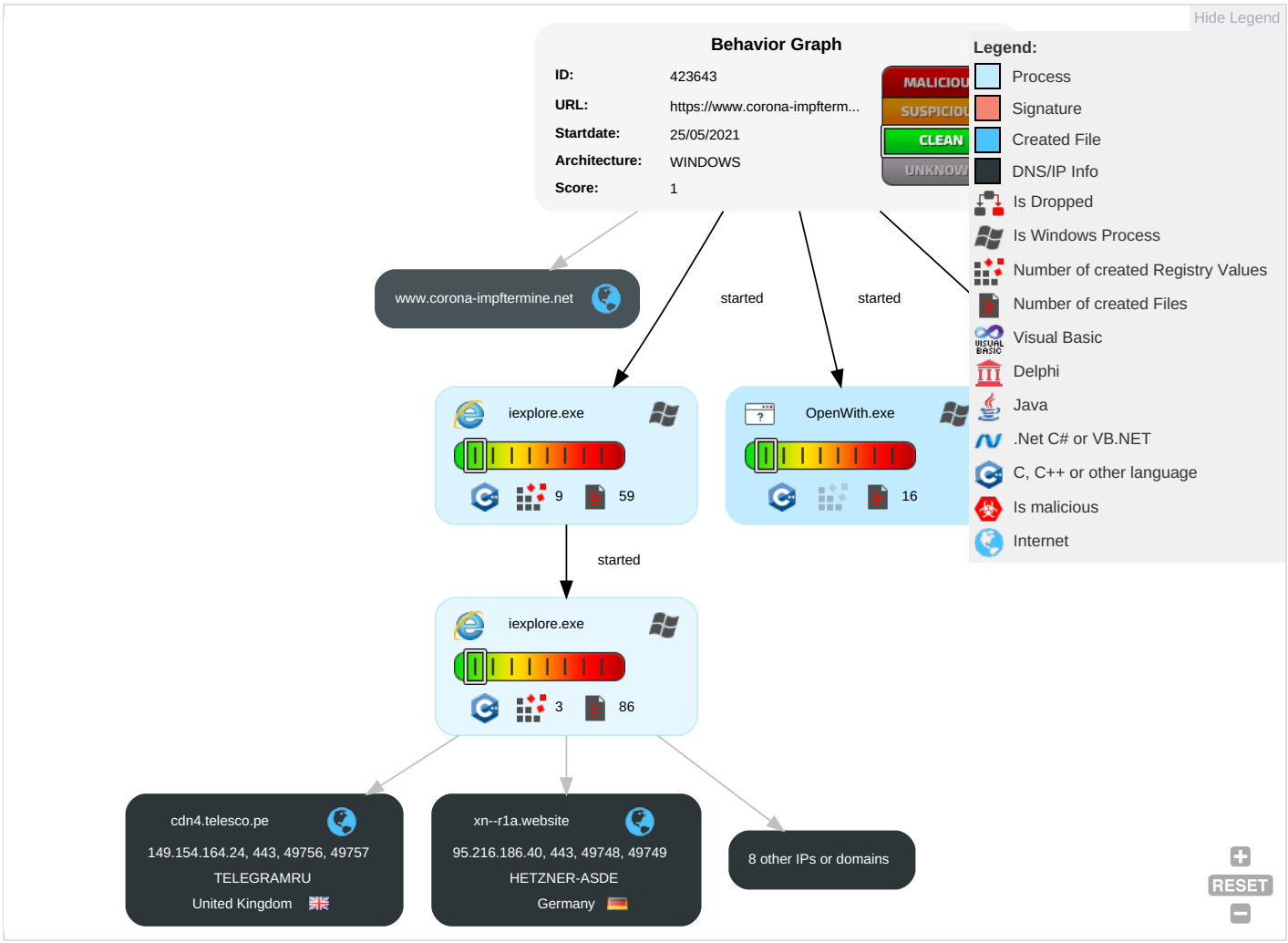
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Eff
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Re Tra Wi Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Re Wi Wi Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Ob De Clo Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

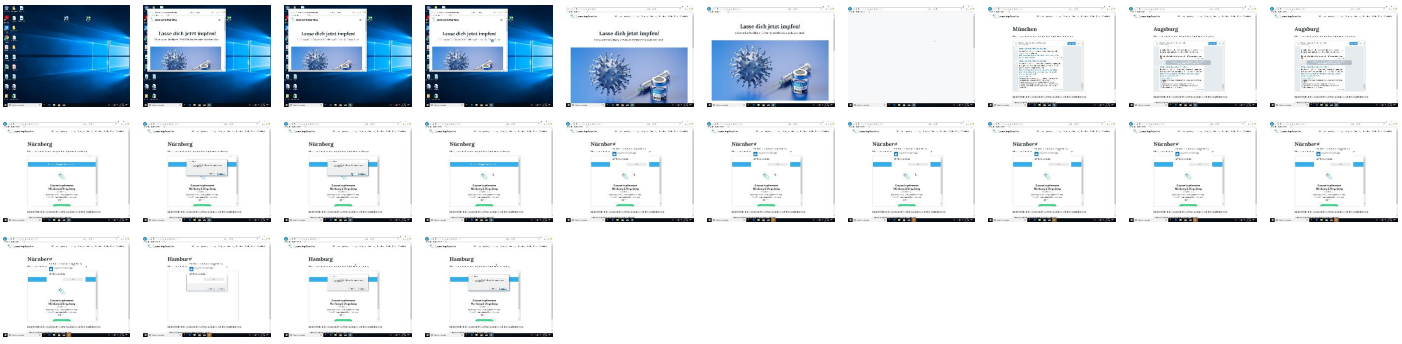
Behavior Graph

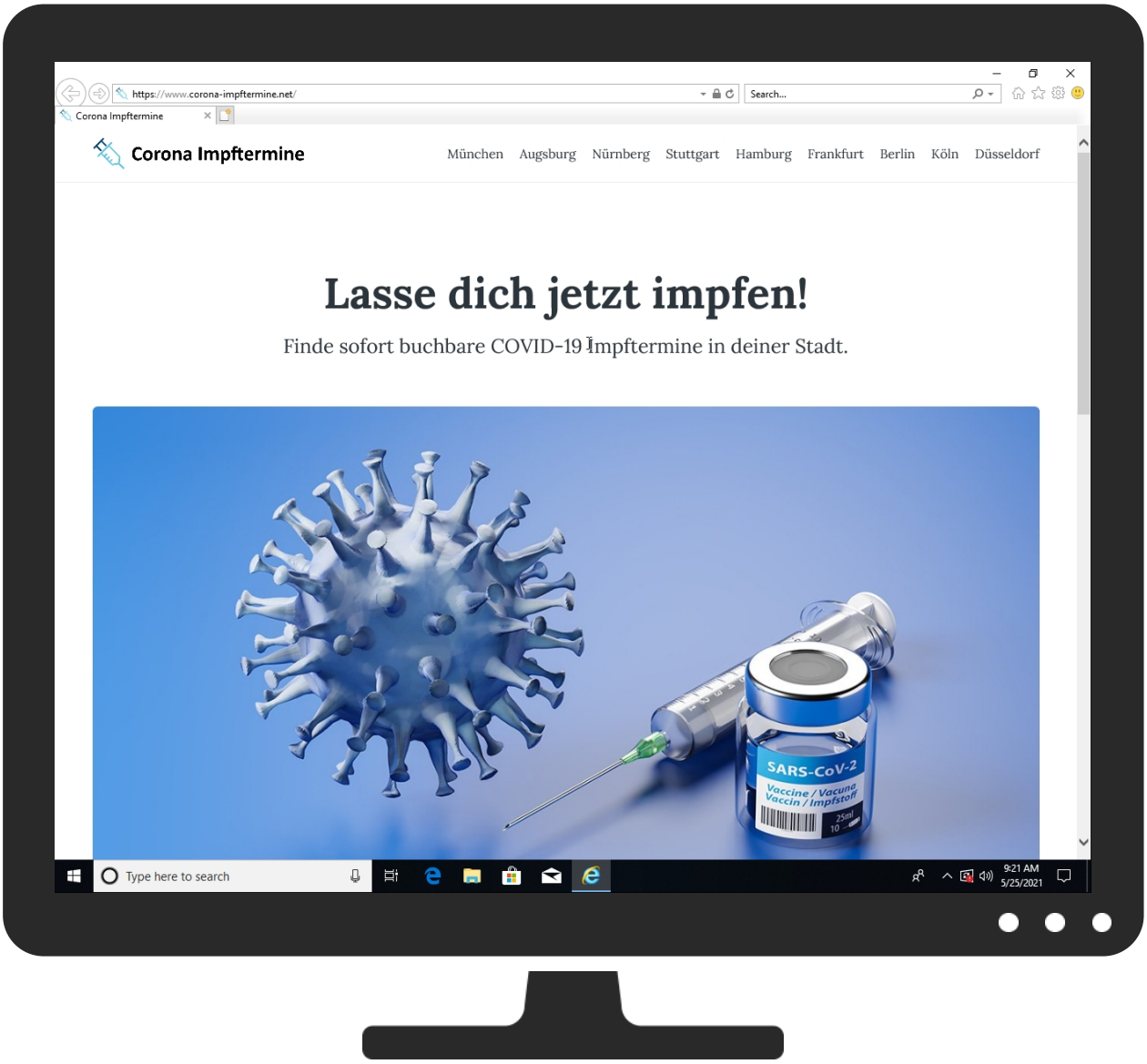


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://www.corona-impftermine.net/	0%	Virustotal		Browse
http://https://www.corona-impftermine.net/	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.corona-impftermine.net/hamburg/4Corona	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_nue	0%	Avira URL Cloud	safe	
http://https://osx.tlgr.org/updates/site/artboard.png)	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://xn--r1a.website/s/corona_impftermine_agb	0%	Avira URL Cloud	safe	
http://https://www.corona-impftermine.net/augsburg/z	0%	Avira URL Cloud	safe	
http://https://xn--r1a.website/s/corona_impftermine_dus	0%	Avira URL Cloud	safe	
http://https://www.corona-impftermine.net/munchen/4Corona	0%	Avira URL Cloud	safe	
http://https://www.corona-impftermine.net/hamburg/x	0%	Avira URL Cloud	safe	
http://https://www.corona-impftermine.net/hamburg/z	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://www.generateprivacypolicy.com/).	0%	Avira URL Cloud	safe	
http://https://www.corona-impftermine.net/Root	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/571	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/570	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/573	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/572	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/575	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/574	0%	Avira URL Cloud	safe	
http://https://xn--r1a.website/s/corona_impftermine_ffm	0%	Avira URL Cloud	safe	
http://https://www.corona-impftermine.net/munchen/x	0%	Avira URL Cloud	safe	
http://https://www.termsandconditionsgenerator.com/)	0%	Avira URL Cloud	safe	
http://https://app.stackbit.com	0%	Avira URL Cloud	safe	
http://https://xn--r1a.website/s/corona_impftermine_muc	0%	Avira URL Cloud	safe	
http://https://www.corona-impftermine.net/privacy-policy	0%	Avira URL Cloud	safe	
http://https://xn--r1a.website/s/corona_impftermine_hh	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/577	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/576	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/579	0%	Avira URL Cloud	safe	
http://https://www.corona-impftermine.net/augsburg/6Corona	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/578	0%	Avira URL Cloud	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://tttttt.me/cdn4/file/P7FovyAGrMzdIdkvULg3nvuBJd0NxOw5MKIMZjgd-15vXz4c8tE0SMtW6-lkZjh3t1CaK2iD	0%	Avira URL Cloud	safe	
http://https://www.corona-impftermine.net/images/corona.jpg	0%	Avira URL Cloud	safe	
http://https://www.corona-impftermine.net/imprint	0%	Avira URL Cloud	safe	
http://https://widget.stackbit.com	0%	Avira URL Cloud	safe	
http://https://web.tel.onl/	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_hh	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_agb/20	0%	Avira URL Cloud	safe	
http://https://onlinetermine.zollsoft.de/patientenTermine.php?uniqueident=607feb7a343fb	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_agb	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_agb/22	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_agb/21	0%	Avira URL Cloud	safe	
http://https://xn--r1a.website/s/corona_impftermine_nue	0%	Avira URL Cloud	safe	
http://https://www.maxritter.net/	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/580	0%	Avira URL Cloud	safe	
http://https://www.corona-impftermine.net/h	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/582	0%	Avira URL Cloud	safe	
http://https://www.corona-impftermine.net/munchen/.corona-impftermine.net/munchen/	0%	Avira URL Cloud	safe	
http://https://xn--r1a.website/s/corona_impftermine_cgn	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/581	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/584	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/583	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/586	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/585	0%	Avira URL Cloud	safe	
http://https://xn--r1a.website/s/corona_impftermine_ber	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/588	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/587	0%	Avira URL Cloud	safe	
http://https://tttttt.me/corona_impftermine_muc/589	0%	Avira URL Cloud	safe	
http://https://osx.tlgr.org/updates/site/artboard_2x.png);	0%	Avira URL Cloud	safe	
http://https://www.corona-impftermine.net/terms-and-conditions	0%	Avira URL Cloud	safe	
http://https://tttttt.me/cdn4/file/WMPWzsM8W37tnne6-j1xjcoxulxwfB2wwds_UyVJOQ8yH9ng3jtjihpzXs1AWj23fkkYir6-	0%	Avira URL Cloud	safe	
http://x1.i.lencr.org/	0%	Avira URL Cloud	safe	
http://https://www.corona-impftermine.net/content	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tlgr.org	95.216.186.40	true	false		unknown
ttttt.me	95.216.186.40	true	false		unknown
www.corona-impftermine.net	206.189.50.60	true	false		unknown
cloudflareinsights.com	104.16.95.65	true	false		unknown
static.cloudflareinsights.com	104.16.95.65	true	false		unknown
cdn4.telesco.pe	149.154.164.24	true	false		high
xn--r1a.website	95.216.186.40	true	false		unknown
d33wubrfki0l68.cloudfront.net	13.225.84.15	true	false		high
widget.stackbit.com	3.65.48.84	true	false		unknown
x1.i.lencr.org	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.corona-impftermine.net/augsburg/	false		unknown
http://https://www.corona-impftermine.net/hamburg/	false		unknown
http://https://www.corona-impftermine.net/nurnberg/	false		unknown

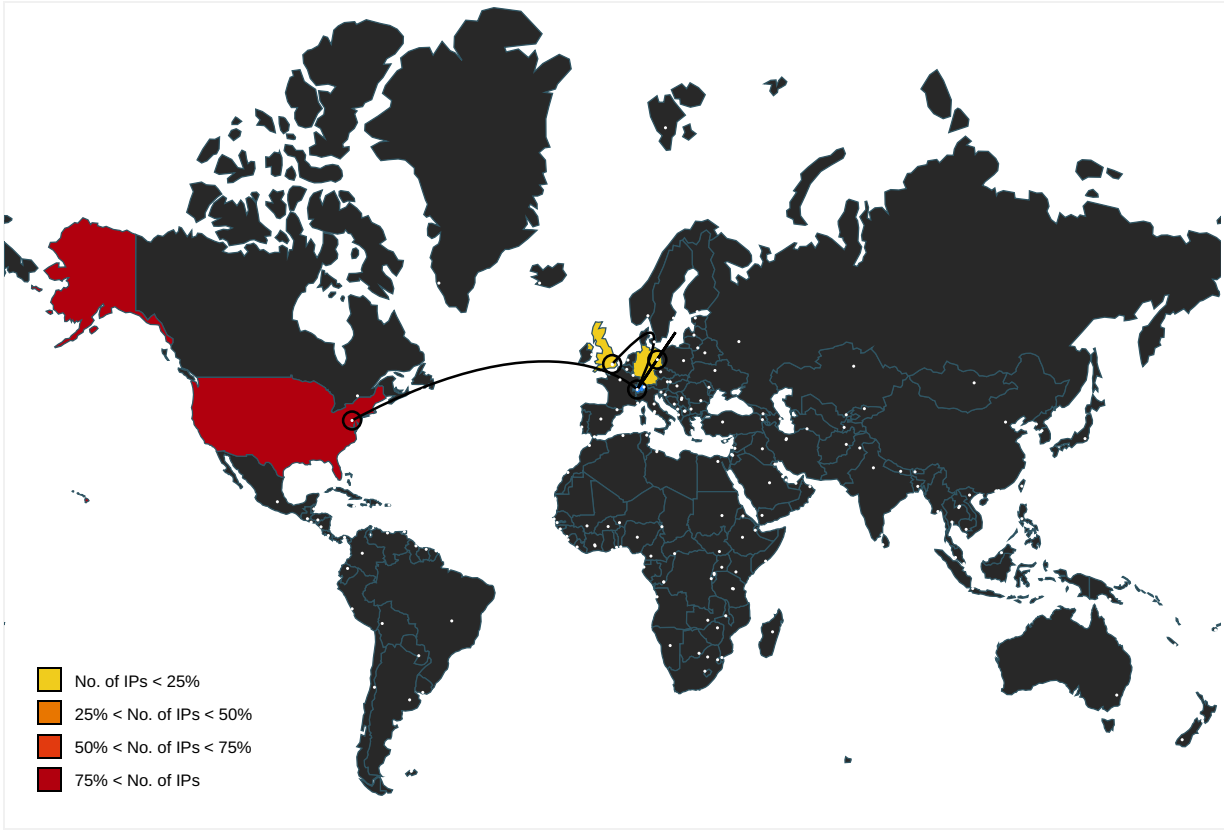
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t.me/corona_impftermine_muc	augsburg[1].htm.3.dr, munchen[1].htm.3.dr	false		high
http://https://telegram.org/apps	augsburg[1].htm.3.dr	false		high
http://https://www.doctolib.de/gemeinschaftspraxis/aichach/aerzte-aichach?pid=practice-115296	corona_impftermine_agb[1].htm.3.dr	false		high
http://https://www.corona-impftermine.net/hamburg/4Corona	{4A1F861A-BD75-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://paulirish.com/2011/requestanimationframe-for-smart-animating/	widget-frame[1].js.3.dr	false		high
http://https://www.corona-impftermine.net/#content	{4A1F861A-BD75-11EB-90E5-ECF4BB2D2496}.dat.1.dr, ~DFF1CF27BECECB5F3A.TMP.1.dr	false		unknown
http://jqueryui.com	jquery-ui.min[1].js.3.dr	false		high
http://https://ttttt.me/corona_impftermine_nue	{4A1F861A-BD75-11EB-90E5-ECF4BB2D2496}.dat.1.dr, corona_impftermine_nue[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://d33wubrfki0l68.cloudfront.net/bundles/b979d43d3560770a058a4e5c8365a89b7a34bd97.js	augsburg[1].htm.3.dr, hamburg[1].htm.3.dr, nurnberg[1].htm.3.dr, munchen[1].htm.3.dr, W7YU039Z.htm.3.dr	false		high
http://https://osx.tlgr.org/updates/site/artboard.png)	telegram[1].css.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://xn--r1a.website/s/corona_impftermine_agb	{4A1F861A-BD75-11EB-90E5-ECF4BB2D2496}.dat.1.dr, augsburg[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.corona-impftermine.net/augsburg/z	~DFF1CF27BECECB5F3A.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn4.telesco.pe/file/W64IsBmmsFuC9_GQAxZjWJM2xi_VDAdUZWx5uPYuDtdljMogWKJ6Ml4ZIRjw9UiHxwGyP00	corona_impftermine_agb[1].htm.3.dr	false		high
http://https://xn--r1a.website/s/corona_impftermine_dus	augsburg[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.corona-impftermine.net/munchen/4Corona	{4A1F861A-BD75-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.corona-impftermine.net/hamburg/x	~DFF1CF27BECECB5F3A.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.stmgp.bayern.de/presse/holetschek-priorisierung-fuer-corona-impfungen-in-arztpraxen-aufg	augsburg[1].htm.3.dr, W7YU039Z.htm.3.dr	false		high
http://https://www.corona-impftermine.net/hamburg/z	~DFF1CF27BECECB5F3A.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.doctolib.de/gemeinschaftspraxis/muenchen/fuchs-hierl?pid=practice-25230	corona_impftermine_muc[1].htm.3.dr	false		high
http://getbootstrap.com)	bootstrap.min[1].css.3.dr	false	• Avira URL Cloud: safe	low
http://https://t.me/corona_impftermine_ffm	augsburg[1].htm.3.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.3.dr	false		high
http://https://www.generateprivacypolicy.com/).	augsburg[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.corona-impftermine.net/Root	{4A1F861A-BD75-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://t.me/corona_impftermine_agb	augsburg[1].htm.3.dr	false		high
http://https://tttttt.me/corona_impftermine_muc/571	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/corona_impftermine_muc/570	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/corona_impftermine_muc/573	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/corona_impftermine_muc/572	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/corona_impftermine_muc/575	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/corona_impftermine_muc/574	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://xn--r1a.website/s/corona_impftermine_ffm	augsburg[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://my.opera.com/emoller/blog/2011/12/20/requestanimationframe-for-smart-er-animating	widget-frame[1].js.3.dr	false		high
http://https://t.me/corona_impftermine_dus	augsburg[1].htm.3.dr	false		high
http://getbootstrap.com/customize/?id=92d2ac1b31978642b6b6)	bootstrap.min[1].css.3.dr	false		high
http://https://cdn4.telesco.pe/file/If4Zr2ttuL_7uT0wdXVMydXgy_Nja4zvrsxqDp6LlQb7RMEdm67uWKgfvm7NECHzJlYx40X	corona_impftermine_agb[1].htm.3.dr	false		high
http://https://www.corona-impftermine.net/munchen/x	~DFF1CF27BECECB5F3A.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.termsandconditionsgenerator.com/)	augsburg[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://app.stackbit.com	init[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.wissenschaft.de	augsburg[1].htm.3.dr	false		high
http://https://xn--r1a.website/s/corona_impftermine_muc	{4A1F861A-BD75-11EB-90E5-ECF4BB2D2496}.dat.1.dr, augsburg[1].htm.3.dr, munchen[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.corona-impftermine.net/privacy-policy	augsburg[1].htm.3.dr, hamburg[1].htm.3.dr, nurnberg[1].htm.3.dr, munchen[1].htm.3.dr, W7YU039Z.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://xn--r1a.website/s/corona_impftermine_hh	augsburg[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/corona_impftermine_muc/577	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/corona_impftermine_muc/576	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/corona_impftermine_muc/579	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.corona-impftermine.net/augsburg/6Corona	{4A1F861A-BD75-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/corona_impftermine_muc/578	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.google.%/ads/ga-audiences	analytics[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/priorisierung-in-arztpraxen	augsburg[1].htm.3.dr	false		high
http://https://tttttt.me/cdn4/file/P7FovyAGrMzdIdkvULg3nvuBJd0NxOw5MKIMZjgd-15vXz4c8tE0SMtW6-lkZjh3t1CaK2iD	corona_impftermine_nue[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].css.3.dr	false		high
http://https://www.corona-impftermine.net/images/corona.jpg	W7YU039Z.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.corona-impftermine.net/imprint	augsburg[1].htm.3.dr, hamburg[1].htm.3.dr, nurnberg[1].htm.3.dr, munchen[1].htm.3.dr, W7YU039Z.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/dollarshaveclub/reframe.js#readme	b979d43d3560770a058a4e5c8365a89b7a34bd97[1].js.3.dr	false		high
http://https://widget.stackbit.com	init[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.doctolib.de/medizinisches-versorgungszentrum-mvz/muenchen/medizinisches-versorgungszentr	corona_impftermine_muc[1].htm.3.dr	false		high
http://https://web.tel.onl/	augsburg[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.kvberlin.de/fuer-patienten/corona/corona-impfungen	augsburg[1].htm.3.dr	false		high
http://https://cdn4.telesco.pe/file/ICVK3nG1WQZ2PlqPX2EgfYssz-2u_Ih8AK1GV_WiJLXKs8fTJCLPFTELhERyPjmktublhsE	corona_impftermine_muc[1].htm.3.dr	false		high
http://https://tttttt.me/corona_impftermine_hh	{4A1F861A-BD75-11EB-90E5-ECF4BB2D2496}.dat.1.dr, corona_impftermine_hh[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://gist.github.com/92d2ac1b31978642b6b6	bootstrap.min[1].css.3.dr	false		high
http://https://tttttt.me/corona_impftermine_agb/20	corona_impftermine_agb[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://onlinetermine.zollsoft.de/patientenTermine.php?uniqueident=607feb7a343fb	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/corona_impftermine_agb	corona_impftermine_agb[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/corona_impftermine_agb/22	corona_impftermine_agb[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/corona_impftermine_agb/21	corona_impftermine_agb[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://xn--r1a.website/s/corona_impftermine_nue	{4A1F861A-BD75-11EB-90E5-ECF4BB2D2496}.dat.1.dr, augsburg[1].htm.3.dr, nurnberg[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://d33wubrfki0l68.cloudfront.net/011e84784814d6cc0b2d8fe255786117680fc476/557b6/images/majestic	augsburg[1].htm.3.dr, hamburg[1].htm.3.dr, nurnberg[1].htm.3.dr, munchen[1].htm.3.dr, W7YU039Z.htm.3.dr	false		high
http://https://www.maxritter.net/	augsburg[1].htm.3.dr, hamburg[1].htm.3.dr, nurnberg[1].htm.3.dr, munchen[1].htm.3.dr, W7YU039Z.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.buymeacoffee.com/maxritter	W7YU039Z.htm.3.dr	false		high
http://https://tttttt.me/corona_impftermine_muc/580	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.corona-impftermine.net/h	{4A1F861A-BD75-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/corona_impftermine_muc/582	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.corona-impftermine.net/munchen/.corona-impftermine.net/munchen/	~DFF1CF27BECECB5F3A.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://xn--r1a.website/s/corona_impftermine_cgn	augsburg[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/corona_impftermine_muc/581	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/corona_impftermine_muc/584	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/corona_impftermine_muc/583	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.corona-impftermine.net/	{4A1F861A-BD75-11EB-90E5-ECF4BB2D2496}.dat.1.dr, augsburg[1].htm.3.dr, ~DFF1CF27BECECB5F3A.TMP.1.dr	false		unknown
http://https://tttttt.me/corona_impftermine_muc/586	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/corona_impftermine_muc/585	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.corona-impftermine.net/augsburg/	{4A1F861A-BD75-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false		unknown
http://https://xn--r1a.website/s/corona_impftermine_ber	augsburg[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://t.me/corona_impftermine_hh	augsburg[1].htm.3.dr, hamburg[1].htm.3.dr	false		high
http://https://t.me/corona_impftermine_str	augsburg[1].htm.3.dr	false		high
http://https://cdn4.telesco.pe/file/LfekFXXO2DQSrc3ldOK4ODQ_elHefA0r6trM-qwkMHrTlH1dZMnG3fGqkm_0LtpGUipVaY7	corona_impftermine_muc[1].htm.3.dr	false		high
http://https://tttttt.me/corona_impftermine_muc/588	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.corona-impftermine.net/hamburg/	{4A1F861A-BD75-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false		unknown
http://https://tttttt.me/corona_impftermine_muc/587	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/corona_impftermine_muc/589	corona_impftermine_muc[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://osx.tlgr.org/updates/site/artboard_2x.png);	telegram[1].css.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.corona-impftermine.net/terms-and-conditions	augsburg[1].htm.3.dr, hamburg[1].htm.3.dr, nurnberg[1].htm.3.dr, munchen[1].htm.3.dr, W7YU039Z.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.doctolib.de/praxis/muenchen/hausarztpraxis-dr-grassl?pid=practice-116543	corona_impftermine_muc[1].htm.3.dr	false		high
http://https://tttttt.me/cdn4/file/WMPWzsM8W37tnne6-j1xjcoxulxwfB2wwds_UyVJOQ8yH9ng3jtjihpzXs1AWj23fkkYir6-	corona_impftermine_hh[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://x1.i.lencr.org/	2D85F72862B55C4EADD9E66E06947F3D.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.corona-impftermine.net/content	~DFF1CF27BECECB5F3A.TMP.1.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.225.84.15	d33wubrfki0l68.cloudfront.net	United States		16509	AMAZON-02US	false
95.216.186.40	tlgr.org	Germany		24940	HETZNER-ASDE	false
149.154.164.24	cdn4.telesco.pe	United Kingdom		62041	TELEGRAMRU	false
206.189.50.60	www.corona-impftermine.net	United States		14061	DIGITALOCEAN-ASNUS	false
3.65.48.84	widget.stackbit.com	United States		16509	AMAZON-02US	false
104.16.95.65	cloudflareinsights.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	423643
Start date:	25.05.2021
Start time:	09:20:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.corona-impftermine.net/
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:	23
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:	clean1.win@5/56@11/6
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://www.corona-impftermine.net/#content • Browsing link: https://www.corona-impftermine.net/ • Browsing link: https://www.corona-impftermine.net/munchen/ • Browsing link: https://www.corona-impftermine.net/augsburg/ • Browsing link: https://www.corona-impftermine.net/nurnberg/ • Browsing link: https://www.corona-impftermine.net/stuttgart/ • Browsing link: https://www.corona-impftermine.net/hamburg/

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.43.193.48, 92.122.145.220, 88.221.62.148, 172.217.20.10, 142.250.185.99, 104.83.124.33, 8.253.207.120, 8.238.30.126, 8.241.79.126, 8.238.29.254, 8.241.89.126, 13.64.90.137, 152.199.19.161, 20.82.210.154, 216.58.214.238, 20.54.7.98, 20.54.104.15, 20.54.26.129, 92.122.213.247, 92.122.213.194, 92.122.144.200 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, e8652.dscx.akamaiedge.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, crl.root-x1.letsencrypt.org.edgekey.net, www.google-analytics.com, fonts.googleapis.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, www-google-analytics.l.google.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, consumerrp-displaycatalog-aks2aks-europe.md.mp.microsoft.com.akadns.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, cs9.wpc.v0cdn.net, neu-consumerrp-displaycatalog-aks2aks-europe.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:22:41	API Interceptor	2x 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\LocalLow\Microsoft\CryptnetUrlCache\Content\2D85F72862B55C4EADD9E66E06947F3D	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	2782
Entropy (8bit):	7.705940075877404
Encrypted:	false
SSDEEP:	48:ooVguI3Kcx8WIzNeCUkJMmSuMXOoVguI3Kcx8WIzNeCUkJMmSuMX1:Jzcx8WBCUoMmSuMHzcx8WBCUoMmSuM1
MD5:	E419AD112571CBB67C14E4CED1322129
SHA1:	E5321CAA9F2DE9BF66B72B3306DA51BE6A7250F7
SHA-256:	1D6C1CC637095B227D226ECEB60C61B7969A53612FA74743C667967E5E1421EF
SHA-512:	AAF3711DD859AA98153509ADD3A7614BF4B62D82D85B3BEFCA42DC1C661D4C19E2EB4CF46479997959B1EB447CA287A6303F3B8643E7EFFF691192DAA54F194 0
Malicious:	false
Reputation:	low
Preview:	0..k0..S.....@.YDc.c...0...*.H.....0O1.0...U....US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10...150604110438Z..350604110438Z0O1.0...U... .US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10.."0...*.H.....0.....$s..7.+W(.....8..n<.W.x.u...jn..O(..h.lD...c...k....1.!~.3<.H..y.....!.K...qiJffl.~<p. .)".....K...~....G.|.H#S.8.O.o...lW..t../.8.{.p!.u.0<.....c...O..K~.....w...{J.L.%.p..)..S$.....J.?..aQ.....cq...o[...\4ylv.;.by.../&.....6....7..6u...r.....l....*.A..v.....5/(.l....dwn G7..Y^h..r...A)>Y>.&.$...Z.L@.F....:Qn.;.}r...xY.>Qx...../..>{J.Ks.....P.|C.t..t.....0.[q6....00\H..;..}`...).....A.....|.;F.H*..v.v..j.=...8.d..+..(.....B.".']..y...p..N..:.'Qn..d.3CO.....B0 @0...U.....0...U.....0....0...U.....y.Y.{....s.....X..n0...*.H.....U.X....P.....i ').au\.n...i/..VK..s.Y.!.~.Lq...`.9....!V..P.Y...Y.....b.E.f..|o..;....'...}~.."....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Microsoft Cabinet archive data, 59863 bytes, 1 file
Category:	dropped
Size (bytes):	119726
Entropy (8bit):	**7.99556910241083**
Encrypted:	**true**
SSDEEP:	3072:GNOqOrdDdJPAX1LHAeNOqOrdDdJPAX1LHA/:aOrdRyX1LH7OrdRyX1LHC
MD5:	BD3E93AD23BB0CA00C44D8774C63E84F
SHA1:	03FB85A6B46615FAEB2D3E29FBC399593D7B5D15
SHA-256:	3526E251E631B67BC547442F85BFE5DD97A109CBC0189F04E1BD40D988EE18B5
SHA-512:	49571828C169BDC5D526D1A48A84002F075F846091DCB26032951EDB1D0A01FCCB0A66646E153B976F048F540009B6A368AFD830531A3F8E2F9CC7E5AFCE6AC
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....b.....R.i .authroot.stl.qqp.4..CK..8T....c_.d....A.F....m"...AH)-.%.QIR..$t)Kd.-QQ*..~.L.2.L.....sx.}...~....$....yy.A.8;....|.%OV.a0xN... .9..C..t.z.,X...,..1Qj,.p.E.y..ac`.<.e.c.aZW..B.jy....^]..+)..!...r.X:.O.. ..Y..j.^.8C.....n7R....p!|_.+..<...A.Wt.=. .sV..`.9O...CD./.s.\#.t#..s..Jeiu..B$.....8..(g..tJ....=,...r.d.].xqX4.....g. lF...Mn.y".W.R....K\..P.n._..7.....@pm.. Q....(#.....=.)...1..kC.`.....AP8.A..<....7S.L....S...^.R.).hqS...DK.6.j....u_.0.(4g.....!,.L`.....h:.a]?.....J9.\..Ww.....%.....4E... ....q.QA.0.M<.&.^*aD.....,.]*....5.....\../ d.F>.V....._.J....".....wI..'..z...j..Ds....Z...[.....N<.d.?<....b.,...n.....;....YK.X..0..Z.....?...9.3.+9T.%.l...5.YK.E.V...aD.0...Y../e.7...c. .g....A..=.....+..u2..X.~....O....\=...&...U.e...?...z....$.)S..T...r.!?M..;....r,QH.B <.(t..8s3..u[.N8gL.%...v....f...W.y...cz-.EQ.....c...o..n.....D*.....2.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\2D85F72862B55C4EADD9E66E06947F3D	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	384
Entropy (8bit):	2.795653095363692
Encrypted:	false
SSDEEP:	6:kKJaq1w3NMa8Rdy+UKcX8KJXsq1KJdNMa8Rdy+UKcXP:Racxzdy+Ba8cPzdy+Ba
MD5:	2F2070DDCA87113D184595C04FA48C0A
SHA1:	FF9F1B29799709D99F4A08F45E4B99D87675D2C8
SHA-256:	8CDE5D886D51A38BE01B3A2F08F060A391C9CCABE78733E675D1A7986E8971DB
SHA-512:	28CAFE37B441E32C0AC61D3526EDFB2182C8F0B25B3B55C5C155D074455BBF9AF5CB91F43FA9AC0C233DEA2CBF859033C4AA4B32297030FA37BEABB161FDE 53
Malicious:	false
Reputation:	low
Preview:	p..... .....Q..(..... .....~.....o...h.t.t.p.:././.x.1...i...l.e.n.c.r...o.r.g./...".5.a.6.2.8.1.5.c.-.5.6.f."...p..... .....c....Q..(..... ....~.....o...h.t.t.p.:././.x.1...i...l.e.n.c.r...o.r.g./...".5.a.6.2.8.1.5.c.-.5.6.f."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1542702081198217
Encrypted:	false
SSDEEP:	12:70fEphZkPlE99SNxAhUeSKz03PEphZkPlE99SNxAhUeSKO:JhZkPcUQUjK5hZkPcUQUjKO
MD5:	F874BD1F540D11B0C180ED798BB7E121
SHA1:	B70A02B017CD220E21FAE4146DC0393CB4295985
SHA-256:	8E877E29AD79B3C7CE9CFBEA05A26841A029EF649190538CB3CC49A25078782A
SHA-512:	B747556E58311711D59FE36C53B78276967657B3620E5267DAF0CE5D2D38060F12AB26BCA87EFF86143D95A083A28CEBA7D921CF75A271CA03438CBCF98CFF8
Malicious:	false
Reputation:	low
Preview:	p..... .....L..Q..(..... .....Y5.....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".8.0.f.8.8.3.5.9.3.5.d.7.1.:.0."...p..... .....SMQ..Q..(..... .....Y5.....$..... .h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".8.0.f.8.8.3.5.9.3.5.d.7 .1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\EQAWN5DV\www.corona-impftermine[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:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910F D
Malicious:	false
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{4A1F8618-BD75-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	39512
Entropy (8bit):	1.91943293480843
Encrypted:	false
SSDEEP:	96:rcZfZu2QWojtoXAfoiIs1MoYETo6KRo9+fo7I9lrov1joMOhoZ41f:rcZfZu2QW2tdf5VMA2dfcsr64p
MD5:	7F9BF70450521B5E1BAB457AE1DCCD65
SHA1:	3B5194509607AEE53AA68CBD0E348DC659D01D44
SHA-256:	9AFB50F3F8F1D90890136C2683CF664B7836A692DA01902E638AEB4F1838791F

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{4A1F8618-BD75-11EB-90E5-ECF4BB2D2496}.dat	
SHA-512:	0AC0AA2A37C3B8296863D4E13EB0EE707DAC0EECFE51D065D0B99B4423600A825F80240D1263A7AB70648478DF1853525B9DB711550386B5E66113D5ADF5D3B
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\{4A1F861A-BD75-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	100378
Entropy (8bit):	2.3301602083988193
Encrypted:	false
SSDEEP:	384:rk86CGAk3T08Gy6XxUFqpL7iej5TWLTt16w6qo/9r93qhgFEeyNMMx53bxzJxByK:VUF0TWy1bE
MD5:	19F6AB2AA118F5A38952EF512F030925
SHA1:	AEF3EBAC613BABDAB5C3B8BFA388A80E3A7D073A
SHA-256:	A1D9C6E2FCD5F68B1A76F284CF357A6AF214270C353877BC8C9E251EFE367CA7
SHA-512:	D4A609AACFD0966FC6C1048532868E3EE9F1E4D8AB5FEBB4166F2B75B10029744884E9935DD3966A13B237DA0D5B6743388C5875F209573FD61D7F73AB9E4D9
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\{50983A8B-BD75-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5662444458999185
Encrypted:	false
SSDEEP:	48:Iw2GcprzGwpaSG4pQuGrapbS0QGQpKqoG7HpR5TGIpG:rqZtQi6gBS0YAqzT/A
MD5:	CB1D5D2D16FD57F61C70A52D15244854
SHA1:	2928E150BC71551DFBC5FEECCA80A73884159DDC
SHA-256:	578A298C520C3114D83A2700A1EBBF04A8CB3D06EC77737A97E533AD11419CC2
SHA-512:	BCF8470E3B065EB6C74560997F373A0096C5F1D7FFCAF3BD4A4553FC18C508D439D476F15F97C9DD0B2889FFDA45E463314EA029B5234D444A44181EBF4AE7C
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	2452
Entropy (8bit):	7.784221833623408
Encrypted:	false
SSDEEP:	48:FDodDY7dYOFe4zz1eENwGQCn6cAutkajhNFbi70dRfBJdZi8wHVev9CyuKQxgAn:Ro+N9tNzUcA1ajLFWqRFZideE5R
MD5:	96C7427A43DDC4B2F74B5383FCDADF1A
SHA1:	D1C13F0361F96EC314EF24DCDF379C2B9C2FF79D
SHA-256:	CE15074C98C698225F4B6EC2B101EB0F0F246FB84A74D4B9D5BDF470A312A02D
SHA-512:	A01D1871FE7D03C361FCB81C0991BD355131510791816775DD5DAEFECC33E1296E635891A80E2A8428932F2B59E714CD5A9B22F8542E3C5D19FBCEBAF43C6F1
Malicious:	false
Reputation:	low
Preview:	6.h.t.t.p.s.:././.w.w.w...c.o.r.o.n.a.-.i.m.p.f.t.e.r.m.i.n.e...n.e.t./.i.m.a.g.e.s./.D.o.w.n.l.o.a.d...p.n.g.....PNG.....IHDR.....m"H....PLTE...Y...IvL.....>oR.....AqE.....Ftc... .....p...;n...Ot..4j....6k;f.1`.....0h.....Cr...#Y.....Cl.\}.....P{...{..f.....n)!...-IDATx..ic.8..c..54.. ihv.....@.%..H.....R.<...qw7h.A.....|..gl+...f>.?=..mG0}.....@.....M... .h...mL.....G..ls.K.|..m..I.1.C.0.-_....8x.....{.5v....`._..x..8..b..[..h..+.I~U.<!~.6.4.qyQ.....xQ....Q...|.G.X.&V..5.....vk.:J...6@.c.2..)T!....E.Mc.'g....2f...x.<!n}.I..tIA.....$..[..&.. E.0.]....#.....Q.....S.V[.UM.z...o.-..k.....Ym.d.k...k.,`C]...O...t..d.[T.[!...."Y...FD.../.....Z.....Sz.,U.L..\.3..Zvx....^ .....O.....OYpDa.,.S.{.....Q+O^Z..O.....B...X. ..w.y..|...x.Kg~.W.....|.}... .b.....Q.."j.q.....6.Q.&0..Z.....Qma?..fWU".,.B.D2....4....&.....8.?7....{..I. .%.....o.B6..bM..=.H(....|.{..\.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\S0BWZ157.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, 320x320, frames 3
Category:	downloaded
Size (bytes):	9336
Entropy (8bit):	7.8593362280594015
Encrypted:	false
SSDEEP:	192:Nh/UwrPm/zEKtL90deJRF/FkShAgIVjF6qWjwc1tRuiGFsZT:NtUwrmI89aeJD/Wc+ARvS2
MD5:	33F329887C30D8950003B7AB881E8402
SHA1:	442DCA298CA4CDB34467D578E6784AD8123C0426
SHA-256:	B98BC5284B18DEF121A47A7106C04DCE6515128BFC11A50E71873603FF4111E5
SHA-512:	4365CE23293B92DEFF19EDAD5C20D1AF833A6EB4B06BFB25A534ECCE9C9FAA72E20E55A70E843A47B55BC8242C87323B39BC3B6039ADB1F7E503BA41A85EC96F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tttttt.me/cdn4/file/P7FovyAGrMzdIdkvULg3nvuBJd0NxOw5MKIMZjgd-15vXz4c8tE0SMtW6-lkZjh3t1CaK2iDSfOtMHEkqBQxk-XJYUhN1AoQLfF01mAhKO0Mha09VqnQSz0DVeo9mCcvuArQApy0eb5yBzvkzLoYUODdzR5aY5K7oh57418UqcLr7iTUS-h1s7JOWekXo-1nPDqmv9149yH5yiKzR4S2jnPU9a2niPoJO-5_t6SBvxva4E6xvVBqVSDnGW3EtvwIj4KAJWoVB9dSKS06aAPakGQTItMbsuyALIijRMDFL5nj1k7McvdLci3byhS-ilcU5-cnIVY2swjZK2eIRGLsZQ.jpg
Preview:	......JFIF.....H.H.....C..C..@.@.."...B.........................!. .1A..Q"2Ra.#3Bq......$CSb.......4cr...................................<........................!1.AQa.q..2BR...."......#$4br..............?..." ..""...." ...."v\e.#..$.......t..j....1..c/.86.u.\R.Y}.UE.[S........>wp'.........[7.IY{.^f.]]= ..6s.....a..Q.{.e...|P....X.5...U...2.-..`...I...Hd.......R1...?.X.)..Orfi....5D...../.."-sp""...." ..""...." ..""...." ..""...." ....u.`..R.Hnys...O......nx....c.pw..`.bC.....xp..0.h.65'p.........s.2V..$... ..VH...Mz.]z$<n..f.e....sk#.mE....-...x.:.....o..W.8].x..f...u.V..i%q.RC.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\beacon.min[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):	13262
Entropy (8bit):	5.29561400679935
Encrypted:	false
SSDEEP:	192:xHieCibtXWC2DvMaxvqbAFpMpL21Z7bpRRMIhN7IkWVXpOrWB8rAN3mZaNeEdBc:HCibB0YRMcy1JdRRxTIkWAw7fj2
MD5:	3BC9671B61A2CEC10EC5D9C65BD2074E
SHA1:	37B185BDBF3482AE94ADD386D6C0B41DCEA351CB
SHA-256:	198EEDF9D8A1AD8D85E2D631EA8667A47A66B7CE838847359045BEB4E8F3A635
SHA-512:	FCC00D089271AE480176A0B4F69D0EBEC3AAFF67392F0E002B226B8C16F0F458E72F2BDBA051F7EB328E2B5954019190891A7C7E44BDA5B935061187BE667CE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.cloudflareinsights.com/beacon.min.js
Preview:	!function(e){function t(i){if(n[i])return n[i].exports;var r=n[i]={i:i,l:!1,exports:{}};return e[i].call(r.exports,r,r.exports,t),r.l=!0,r.exports}var n={};t.m=e,t.c=n,t.d=function(e,n,i){t.o(e,n)||Object.defineProperty(e,n,{configurable:!1,enumerable:!0,get:i})},t.n=function(e){var n=e&&e.__esModule?function(){return e.default}:function(){return e};return t.d(n,"a",n),n},t.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},t.p="",t(t.s=0)}([function(e,t,n){"use strict";function i(e){var t="";if(t=window.location.origin?window.location.origin:window.location.protocol+"://"+window.location.host,e&&"string"==typeof e)if(0===e.indexOf("/"))t+=e;else try{var n=new URL(e);return n.protocol+"://"+n.host+n.pathname}catch(e){}else{var i=window.location.pathname;i&&i.length>0&&(t+=i)}return t}function r(e){return Object.keys(e).forEach(function(t){"number"==typeof e[t]&&(e[t]=String(e[t]))}),e}function o(e){if("function"==typeof performance.getEntriesByType){var t=performance.get

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\corona_impftermine_muc[1].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):	93116
Entropy (8bit):	5.596119690341562
Encrypted:	false
SSDEEP:	1536:eH3D+KD+5296sk9CD+QyM3kPDDDYvsDVVDV2DRMkL1YaDGK:wz+g+Q96x94+QyMUPPDYvCVZVsRRL1Yy
MD5:	97A9936D2F731B194E8842244FBA9605
SHA1:	0690E1ADAEF6B7E2875EE3A6024BEC8A67EAB84A
SHA-256:	6CC530AE63D4FC477ACEDF817FB5A2E228DF0FD220A7CD5C4AABC40FB78B02E9
SHA-512:	B858E20B840FE83E10160DCAF3FB3BE72CB73BDA1CA3D826247B2404D0784C950F446946C398070E198820879735FE8D67C0CC4BAB7F6670A095BF6B2B2E8D8
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>. <head>. <meta charset="utf-8">. <title>Corona Impftermine M.nchen & Umgebung . Telegram</title>. <meta name="viewport" content="width=device-width, initial-scale=1.0, minimum-scale=1.0, maximum-scale=1.0, user-scalable=no" />. <meta name="format-detection" content="telephone=no" />. <meta http-equiv="X-UA-Compatible". content="IE=edge" />. <meta name="MobileOptimized" content="176" />. <meta name="HandheldFriendly" content="True" />. .<meta property="og:title" content="Corona Impftermine M.nchen & Umgebung">.<meta property="og:image" content="https://cdn4.telesco.pe/file/LfekFXXO2DQSrc3ldOK4ODQ_elHefA0r6trM-qwkMHrTlH1dZMnG3fGqkm_0LtpGUipVaY7L_MHPCRRK-yjUKPoqtmUTBkI69Jv61LXXAPAoJVkMS6I4pEXng5gQ08y0jiehOK5aepXthGSxdjRV7qmk8iHaBRkT7PdrbJiaFYlyWA9iR7gFjSE5PmprT6EuGRxvamREec7Vyd0CCnRItGmTP6qE18v_KAAVUOL9dYZN-Kx_gM1ngCdCv1mFrPF6rOYbBGhkPz5FpbyzGn0VNk4-oHCcubrI6R6AbaaC3Y5U2bB0g3JApVmd2T9qB7-aRAwA6T8fik571p9B1IIqxQ.jpg">.<meta pr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\css2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	826
Entropy (8bit):	5.29682973030963
Encrypted:	false
SSDEEP:	24:5JY3QY7aGVqvmgsJY3QYN0aGVqvmgOJOY7aGVUDDAJOYN0aGVTP:XY3QEaGVqtwY3QpaGVqt+OEaGVUMOpa2
MD5:	ED976DB7ADAEBC5B28B9285CB7E0C609
SHA1:	3B5E5C8EF2F2B7DEF46B2E78A6740DDD3DB8AEDB
SHA-256:	247AA5B17C4A9A5549A9F7881F6BFBCA8E99BC6098F460C7C3F49575510AE23F
SHA-512:	EDC30C71EC460F5C0C0EF5C8F83DA1CAEC7BF3EF92B0E3DA73E69DD3142ED424284ACD7983A38575620A2CDAA5605746AC299D929D8BBEEFA039CDA2333CED6
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Lora';. font-style: italic;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/lora/v17/0QI8MX1D_JOuMw_hLdO6T2wV9KnW-MoFkqs.woff) format('woff');.}.@font-face {. font-family: 'Lora';. font-style: italic;. font-weight: 700;. font-display: swap;. src: url(https://fonts.gstatic.com/s/lora/v17/0QI8MX1D_JOuMw_hLdO6T2wV9KnW-C0Ckqs.woff) format('woff');.}.@font-face {. font-family: 'Lora';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/lora/v17/0QI6MX1D_JOuGQbT0gvTJPa787weuyJF.woff) format('woff');.}.@font-face {. font-family: 'Lora';. font-style: normal;. font-weight: 700;. font-display: swap;. src: url(https://fonts.gstatic.com/s/lora/v17/0QI6MX1D_JOuGQbT0gvTJPa787z5vCJF.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.08714471092212
Encrypted:	false
SSDEEP:	6:0IFFli+56ZRWHTizlpdAxInVuNijFFli+56ZXizlpdAxILiJNin:jF/iO6ZRoT6pixUEqF/iO6ZX6pix5JY
MD5:	67A7912F5FB9605F40B01A6AAC341D57
SHA1:	19272A97FDE0596D8ABDEFED18B201E5E077C300
SHA-256:	64FC8DAD1EF311A568BE67CDCEA4C9D9823F00AB8539E0ECD2BA33E1D1B3B964
SHA-512:	250E74178E433F8F91FA8BB0A047A66C1574491E3A6AD4F36FC197F674E5BFB741B7CEF439FE9A976D0FDB0CC6BD278518F4B388743B58F4F6E6A6893973D262
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmEU9fBBc-.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\hamburg[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):	52360
Entropy (8bit):	5.064076572126328
Encrypted:	false
SSDEEP:	768:86n4u9JK2adhMRMV7J8RBwkzKLKb5ApeJ8pC/kKpJ7PuKRM1EJt+SzAoSxsKXXmm:RmVKcfIaF607G/53rYh
MD5:	693025B84D9963220DDB7F41784CFF0F
SHA1:	10DEC42382FA4769CD84A3E5CA3A983574077757
SHA-256:	D2F6090948EC9D1F6AA4F62B2B37FC3882C594F22879AE93753D755BAFD1E7D9
SHA-512:	CBA872C7F0E2AE17251BB4B6FD5B9D8F25B19964F833A09991894C2F468FE2EADBDAB19D7F167C7369E6E3188008BE9A22AECF86FE698E37B44EF7E5DF6D22B6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.corona-impftermine.net/hamburg/
Preview:	<!DOCTYPE html><html><head><link data-react-helmet="true" href="https://fonts.googleapis.com/css2?family=Lora:ital,wght@0,400;0,700;1,400;1,700&display=swap" rel="stylesheet"/><link data-react-helmet="true" rel="icon" href="/images/Download.png"/><meta data-react-helmet="true" charSet="utf-8"/><meta data-react-helmet="true" name="viewport" content="width=device-width, initialScale=1.0"/><meta data-react-helmet="true" name="google" content="notranslate"/><meta data-react-helmet="true" name="description" content="Finde freie Corona Impftermine f.r den Umkreis Hamburg"/><meta data-react-helmet="true" name="robots" content=""/><title data-react-helmet="true">Corona Impftermine Hamburg</title><meta charSet="utf-8"/><meta name="viewport" content="width=device-width"/><link rel='preload' as='style' href='https://d33wubrfki0l68.cloudfront.net/css/f32e8963c988162755fb15c930cba39355a7da17/_next/static/css/06e00db3ad673e94378c.css'/><link rel='stylesheet' data-n-g href='https://d33wubrfki0l6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\jquery-ui.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\jquery-ui.min[1].js	
Size (bytes):	98729
Entropy (8bit):	5.12041479546023
Encrypted:	false
SSDEEP:	1536:CPua844bxcytfiWLOpoqrauzoKQ7eSXOVXQ1UnCjjv8wvSHVNPdX1YnFf2qZZ1Jy:mvUtLLOVevjSHnQnAqn1Jy
MD5:	FCF956F8FD2371FEF081125FBD1CD1B0
SHA1:	59DC043C3191C85C23244CC5B09F422585296ABF
SHA-256:	EB46D82EF6F86859F18E379660E0F45B85C6F69FA97111905F0C125A08506376
SHA-512:	D76C58B45D0850A29B28D0A1E0CBD01DE0CF789918079F01E6F78BCE32011A1E111460C7852803140236974BC3570699DB4850422BA64880BD70A0CA4D707E17
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tlgr.org/js/jquery-ui.min.js
Preview:	/*! jQuery UI - v1.11.4 - 2017-08-30.* http://jqueryui.com.* Includes: core.js, widget.js, mouse.js, draggable.js, resizable.js, sortable.js, slider.js, effect.js, effect-slide.js.* Copyright jQuery Foundation and other contributors; Licensed MIT */..(function(t){"function"==typeof define&&define.amd?define(["jquery"],t):t(jQuery)})(function(t){function e(e,s){var n,o,a,r=e.nodeName.toLowerCase();return"area"===r?(n=e.parentNode,o=n.name,e.href&&o&&"map"===n.nodeName.toLowerCase()?(a=t("img[usemap='#"+o+"']")[0],!!a&&i(a)):!1):(/^(input|select|textarea|button|object)$/.test(r)?!e.disabled:"a"===r?e.href||s:s)&&i(e)}function i(e){return t.expr.filters.visible(e)&&!t(e).parents().addBack().filter(function(){return"hidden"===t.css(this,"visibility")}).length}t.ui=t.ui||{},t.extend(t.ui,{version:"1.11.4",keyCode:{BACKSPACE:8,COMMA:188,DELETE:46,DOWN:40,END:35,ENTER:13,ESCAPE:27,HOME:36,LEFT:37,PAGE_DOWN:34,PAGE_UP:33,PERIOD:190,RIGHT:39,SPACE:32,TAB:9,UP:38}}),t.fn.extend({scrollParent:fun

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\munchen[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):	52376
Entropy (8bit):	5.064516857606515
Encrypted:	false
SSDEEP:	768:0Un4u9JK2adhMRMVfRMPBwkzKLKb5ApeJ8pC/kKpJ7PuKRM1EJt+SzAoSxsKXXme:5mVm2fIaF607G/53DYh
MD5:	D5608EDF2E84186494FBEA29643069A0
SHA1:	59CEA1BD24A9BD5E42F6750AD3D3EB18078A7A30
SHA-256:	C6DFB17C420765DA3352CFAFF1188B344F4263D36D2DB306DA3A53E461A35CFE
SHA-512:	D421FBE4B8478B3FDB369FAFFA17F14EE963728B93D344A164586296D744AF46D785275AEA950A0EF1443240CB0EFC2C814424BAA4EC0002050C2FBFD06AA7E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.corona-impftermine.net/munchen/
Preview:	<!DOCTYPE html><html><head><link data-react-helmet="true" href="https://fonts.googleapis.com/css2?family=Lora:ital,wght@0,400;0,700;1,400;1,700&display=swap" rel="stylesheet"/><link data-react-helmet="true" rel="icon" href="/images/Download.png"/><meta data-react-helmet="true" charSet="utf-8"/><meta data-react-helmet="true" name="viewport" content="width=device-width, initialScale=1.0"/><meta data-react-helmet="true" name="google" content="notranslate"/><meta data-react-helmet="true" name="description" content="Finde freie Corona Impftermine f.r den Umkreis M.nchen"/><meta data-react-helmet="true" name="robots" content=""/><title data-react-helmet="true">Corona Impftermine M.nchen</title><meta charSet="utf-8"/><meta name="viewport" content="width=device-width"/><link rel='preload' as='style' href='https://d33wubrfki0l68.cloudfront.net/css/f32e8963c988162755fb15c930cba39355a7da17/_next/static/css/06e00db3ad673e94378c.css'/><link rel='stylesheet' data-n-g href='https://d33wubrfki0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\tgsticker[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	13923
Entropy (8bit):	4.738865175740892
Encrypted:	false
SSDEEP:	192:XahNN9aaOWUbiYyaiEpi1BaSi9OwFqLJiH718PFxjKsVGA3UbGrNixnsvZTmdQet:oiboUvxnue1
MD5:	A994D2F95F1CB8F75FB890B729516839
SHA1:	C0E8476E73753C6529B6A3E02C10CA8803788845
SHA-256:	7AF53D7077C16F6AD9EFD63A975749C4835CE6E495C337FA4176F15ED385F80B
SHA-512:	98B337532E38FB9E08A4B62549472B761B69882C1F4300E0AF8F1C7790DEB49D9BAB59E8504782721BBDE0D93D584B0021DB8E1CD3916AFB1AD9598145781EAE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tlgr.org/js/tgsticker.js?24
Preview:	var RLottie = (function () {. var rlottie = {}, apiInitStarted = false, apiInited = false, initCallbacks = [];. var deviceRatio = window.devicePixelRatio || 1;. var rlottieWorkers = [], curWorkerNum = 0;.. var startTime = +(new Date());. function dT() {. return '[' + ((+(new Date()) - startTime)/ 1000.0) + '] ';. }.. rlottie.Api = {};. rlottie.players = Object.create(null);;. rlottie.WORKERS_LIMIT = 4;.. var reqId = 0;. var mainLoopTO = false;. var checkViewportDate = false;. var lastRenderDate = false;.. var userAgent = window.navigator.userAgent;. var isSafari = !!window.safari ||. !!(userAgent && (/\b(iPad|iPhone|iPod)\b/.test(userAgent)) || (!!userAgent.match('Safari') && !userAgent.match('Chrome'))));. var isRAF = isSafari;. rlottie.isSafari = isSafari;.. function wasmIsSupported() {. try {. if (typeof WebAssembly === 'object' &&. typeof WebAssembly.instantiate === 'function') {. const module = new WebAssembly.Module(Uint

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\widget-frame[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	assembler source, ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\widget-frame[1].css	
Category:	downloaded
Size (bytes):	68403
Entropy (8bit):	5.309915119215391
Encrypted:	false
SSDEEP:	768:sU9x04zS3YUs0AWoWljn8uz/EuKOFDGlKrEkWekbDaWhzeFQEW+EJ:984OhtjnFrEuKOlGwEykbDuQ
MD5:	68E6986BC07CDF467F81DCA2A0DC4D60
SHA1:	F665C8EFF8D5B3CFEF32D181CD8430C729B2EA6F
SHA-256:	D73EFE70BE2927BA40FB4617468FFA04712439F55DD935568313CE4A09320418
SHA-512:	40B2A0A78132E0DA0564B49F5A4D628A4AC3007DB61F9418BD6FA183A836AE6C25EC1DADF79BEB17F2B758C4EF50DD9EF6735E607D263ABDEB590CB7BD154F 4F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tlgr.org/css/widget-frame.css?45
Preview:	body.widget_frame_base {. font-family: 'Roboto', sans-serif;. padding: 0;. margin: 0 auto;. font-size: 16px;.}..widget_frame_base a {. color: #2481CC;. text-decoration: none;.}..widget_frame_base a:hover {. text-decoration: underline;.}..widget_frame_base a:hover * {. text-decoration: inherit;.}.body.rtl {. direction: rtl;.}...no_transitio ns,..no_transitions * {. transition: none !important;.}..body.body_widget_post {. line-height: 0;. color: #212121;. min-width: 300px;. max-width: 500px;.}.mark.highlight {. background: #ffeeb8;. color: inherit;. border-radius: 2px;. padding: 0 1px;. margin: 0 -1px;.}..emoji {. font-style: normal;.}..emoji > b {. font-weight: normal;.}..emoji_defa ult .emoji {. background: none !important;.}..emoji_image .emoji {. width: 1.25em;. vertical-align: top;. display: inline-block;. white-space: nowrap;. overflow: hidden;. ba ckground: no-repeat 2px 50%;. background-position-y: calc(50% - 1px);. background-size: 1.25em 1.25em;. tex

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\widget-frame[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	83095
Entropy (8bit):	4.725584599445188
Encrypted:	false
SSDEEP:	768:x3+62J1uset391b6CwPHG+ARieDrxsyk7W9vwCiPZZ1LQayIw8JBgHAtD2:Fj2vet3jsyk7UW7e66
MD5:	41D9BA1330DBD6BCE65BF5290A10211E
SHA1:	E2852877E63C6C3AB2FF1C640016155143C66628
SHA-256:	7A519E16536569F67D43F1431D5A925C90BCF02B100CA2192260507DAD070916
SHA-512:	3C9FB06245585EC3F1EBC13E7D165E46A7D77B2C69AE90274493D317AFF433F241894AD3AEDA9E5C35C8F065D41EEEA88B648A7AB5374A4BD8BDF86DB07AA4 D7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tlgr.org/js/widget-frame.js?46
Preview:	// http://paulirish.com/2011/requestanimationframe-for-smart-animating/.// http://my.opera.com/emoller/blog/2011/12/20/requestanimationframe-for-smart-er-animating..// re questAnimationFrame polyfill by Erik M.ller. fixes from Paul Irish and Tino Zijdel..// MIT license..(function() {. var lastTime = 0;. var vendors = ['ms', 'moz', 'webkit', 'o'];. for(var x = 0; x < vendors.length && !window.requestAnimationFrame; ++x) {. window.requestAnimationFrame = window[vendors[x]+'RequestAnimationFrame'];. window.cancelAnimationFrame = window[vendors[x]+'CancelAnimationFrame']. || window[vendors[x]+'CancelRequestAnimationFrame'];. }.. if (! window.requestAnimationFrame). window.requestAnimationFrame = function(callback, element) {. var currTime = new Date().getTime();. var timeTo Call = Math.max(0, 16 - (currTime - lastTime));. var id = window.setTimeout(function() { callback(currTime + timeToCal

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\06e00db3ad673e94378c[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):	59808
Entropy (8bit):	5.140018340718868
Encrypted:	false
SSDEEP:	768:jxWPmXQRTZxfJD/bT/rnLNH64NZ6kPwB/u:FWPmXQRTRLNH64NZ6kPwW
MD5:	AEF437146D02279B374936D91B791999
SHA1:	F32E8963C988162755FB15C930CBA39355A7DA17
SHA-256:	424FE02D861393EC0B598678EF3F7FA4B7C840D549B9C97E7F96828743AE161C
SHA-512:	AD75BB9E6B5844DE2FEDA161BA701A4A9409053389C2F906F5A958883B6C56F8C056C0D0C6BAE399D0811347BD81FD4DBE86EF5E8127E46CA3E9F452EC3FC2 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d33wubrfki0l68.cloudfront.net/css/f32e8963c988162755fb15c930cba39355a7da17/_next/static/css/06e00db3ad673e94378c.css
Preview:	html{line-height:1.15;-webkit-text-size-adjust:100%}body{margin:0}main{display:block}hr{-webkit-box-sizing:content-box;-moz-box-sizing:content-box;box-sizing:content-box;height:0;overflow:visible}a{background-color:transparent}abbr[title]{border-bottom:none;text-decoration:underline;-moz-text-decoration:underline dotted;text-dec oration:underline dotted}b,strong{font-weight:700}code,kbd,pre,samp{font-family:SFMono-Regular,Menlo,Monaco,Consolas,Liberation Mono,Courier New,monospace;font-size:1em}small{font-size:80%}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}sub{bottom:-.25em}sup{top:-.5em}img{border-style:none}button,input,optgroup,select,textarea{font-family:inherit;font-size:100%;line-height:1.15;margin:0}button,input{overflow:visible}button,select{text-transform:none}[type=button],[type=reset],[type=submit],button{-webkit-appearance:button}[type=button]::-moz-focus-inner,[type=reset]::-moz-focus-inner,[type=submit]::-moz-focus-inner,button::-moz-focu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\Arrow_1x[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 8 x 12, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	988
Entropy (8bit):	6.026446478258165
Encrypted:	false
SSDEEP:	12:6v/7ady1TbpOia9jXuR2cDPilYwlfxD82lY2E23IlBJKVL6p/6WLVTE6oyJiKVLS:dy1he91Wwjx82lY2T3ouVo8yJ3VPXGp
MD5:	5BD43F48F3411D4DF3CA18B291269E25
SHA1:	7D7A23DBEDC370B4C60615D2BC956AA112060F40
SHA-256:	3B2212EF1C4D336FBD7983A732D88FA83423A25453209F02F18AB878218D505D
SHA-512:	F905B3D4EC9D340FEB899A015DF7953746B87C83727C597CC0F05D220D5E2E4326F13534FA0276F301DDF7C7D4D894E929F2B89AF13C6531586D3FE904952DE(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tlgr.org/img/tgme/Arrow_1x.png
Preview:	.PNG.....IHDR.....,_.....tEXtSoftware.Adobe ImageReadyq.e<..."iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CS6 (Windows)" xmpMM:InstanceID="xmp.iid:C698B3B6EE8211E4A872B7095E16E28F" xmpMM:DocumentID="xmp.did:C698B3B7EE8211E4A872B7095E16E28F"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:C698B3B4EE8211E4A872B7095E16E28F" stRef:documentID="xmp.did:C698B3B5EE8211E4A872B7095E16E28F"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.."....PIDATx.b....,...t f@. ..?..cS.....cS..=H.2.)..f$EE...p"..IL...)V.u..|.$.Px.. ....#..l.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\DTS50CAQ.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, 160x160, frames 3
Category:	downloaded
Size (bytes):	3620
Entropy (8bit):	7.745128617392163
Encrypted:	false
SSDEEP:	96:pk45zekz+cvX8VxsZqln/LOegKXlStXt7c08:a45zSSMVxw89ez8
MD5:	ABB102E751D2C4962A28BE7F805EF620
SHA1:	100AB737142622C0CD8B5108E366D06C3A1A3544
SHA-256:	C0655445D5FBEECDF2C5EFD3DFD62781BB6C9750FAC2B22D4CB30F884DED1B87
SHA-512:	1A7C7AAC90760FAB77C35BB0E70D69C0B56B50467B41DE0D6E6FE87F397EEC9B0F2799E456918FCE4D0CAC8D7E404A49FF7A7CD357F5EFA8CA64F91049EC7(8F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn4.telesco.pe/file/If4Zr2ttuL_7uT0wdXVMydXgy_Nja4zvrsxqDp6LlQb7RMEdm67uWKgfvm7NECHzJlYx40XpFlSksaHUhO4C4U6CQxUKnHUL-3WjK8pywo-xQF_ssYqYh1z62LNETBMQG-5_acVnK261EGJqHIZkmzKbjoeLcqXfNm6Ygpz6oybPl7biyVmQg7L6XfUCZwATTZ2UE8UqW8Kw7jLMduo-BY-4dudNke4xlZ1AOkcCCvnK8HzmviwVYxzZ0OohpbZjdarYFqxIPMfr4M8XjROkf6zEZdNsV-Cs-Ydn0Y-xEGdj3hAHlpYxPXe8EpNq3xz62j785YZGgdHKrSkNdz04OQ.jpg
Preview:	......JFIF.....H.H.....C.....C.....".....8.....!1.A.."Q2B RaqC..#3...5r.....4.....!1AQ..aq.."2BR....b....Cr.....?.....}...e..C..s<....Id..x!g.....@'...I.mt.G3. <..w..7..z8.....Sq. .A....u..h.. .W.G.P....^9..*....j....+{L.Yh..a?...ke.-$...L.m....ZL.....U.S.e..2.Gh....._D.].8...m.....q.O}1...3.....{..s^.4.#.bGu.V).c..'..s...Z.:.(.SP.al:.KH'..}] {%..I.....:.F....k.....Y.....r"....:>~.v.B.m\."""""""""""""""""..Q.?4a<..U..op..p..GE..M..Y..'.y.....J..N_.x?.n..iU$V.^....oT.....q..`.q ..{9.'.ST.?...3_Q...[hae(s..H.w...9..~4.v.gQ`,h.. xi..\..0lN.?..?.....gDC.B.....R...9g.....@.....5I...q.T.l;.(...;.I.r;y=..c..u.k.<..v...<....q...>.B<.%.....K..x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\E299A5[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 40 x 40, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1685
Entropy (8bit):	7.854140237441285
Encrypted:	false
SSDEEP:	48:ZpCDMUj04Ug5ec6QXW9RXZpLvSBL3jyWtOhweoF56xaq4l1:ZpCXnV5EQXW9Rplv4bjpOhweoMaq4l1
MD5:	73F6A8C324FC3CBFD0FF53F01A303FA6
SHA1:	F7E500B162D67A9FA7A281577FCA89DA25E68F25
SHA-256:	540A8623C08E30373564916BD3B032123FB1B9974D0E430DAA8719BDAB60AE0C
SHA-512:	8641E250007697BAFD1D3ED16DA664BB855E4ED96E0993D62BFB904F53110C659AEB2BC414A332638CADF8A50D7ACDB951C4ADF7CEBCD55D556F995E313A1 C2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tlgr.org/img/emoji/40/E299A5.png
Preview:	.PNG.....IHDR...(...(.....m...\IDATx.....c.....>9I.iU.W.m.3..m.m..m.j.....\feUg*..U....>/..g:.....P>B..p._.:gqf..u.xN.c...x%^o.J...3p....=9oNx..Z.....M.....2.....T&'.A.hh-,h.i.. .r~.o1.....h..'&&.....T.^.....}.....>O..1.z.G6..m.....Q.VA..h.....1...X.tN&.....|K..\W.m.t.E.w.R....1y.i....7...8.....6.....H.....W]e.e...e!I.2 ..X..C..{.:y2m.…}..c.?.{w...o.Th....!.E..N.w ...w..R.?o./G..:....M.../7..n.V...S..E...Y.;.Pz.kK.....k.w..{.g....|.J.B.....{z..|..EL.{..H.... .;.g...[g..y...../n|\s~.W.....4O4...I.r.....*.6..+.d.:..W8~...6.cO./.G7D.o.....&!..9.I...<..7Z ./.....VS.....-y^h..m.Ok!.....7....Rt...6.....?.P4.....".rk..T.....t....2f.W..J%:.y...(..z..../.!.....w.E)..R.+.....;..q....J.lJ.i.f-.C....LejJm.V.H..j6G.h.n1'Kl.0....C....v...B..... .`nPG.$.GT.$'..TV.K.....0rj.c.u.,#.3.RV.nw].^.mD.odt.....X.W8^.`....3Y.jQ;B.p.:...j.O..7.B...}k..|z=....)...!.G.k...t.J..C...'C.....@..zB.I...~.....#txnce.{...Cu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\b979d43d3560770a058a4e5c8365a89b7a34bd97[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	4328
Entropy (8bit):	5.1670431696673855
Encrypted:	false
SSDEEP:	96:nd9+hThjG9Gy56j7r5OcZ0oDZyyXDZby9jo:dwTjwaN0wZyyTZby9jo
MD5:	2F3ED7C4108CC0BB865C1392C242B7D0
SHA1:	B979D43D3560770A058A4E5C8365A89B7A34BD97
SHA-256:	DFA5868B703E984D6D84711A4D4338BF5C073260BECF2BB6F03A6D824BBF9456
SHA-512:	59A2321A7A9FA60597C3F8B77E98AE515FFE7EB0BA43BBFB902410BB99A1FBAA1CAE0A8C9B7EBC2AD1751337976879BE9F7F4644421248AFC373696B9E9C311A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d33wubrfki0l68.cloudfront.net/bundles/b979d43d3560770a058a4e5c8365a89b7a34bd97.js
Preview:	window.onNextjsAppDidMount = function() {./*. * reframe.js - Reframe.js: responsive iframes for embedded content. * @version v2.2.7. * @link https://github.com/dollarshaveclub/reframe.js#readme. * @author Jeff Wainwright <jjwainwright2@gmail.com> (http://jeffry.in). * @license MIT.*/.!function(e,t){"object"==typeof exports&&"undefined"!=typeof module?module.exports=t():"function"==typeof define&&define.amd?define(t):(e=e||self).reframe=t()}(this,function(){"use strict";return function(e,t){var i="string"==typeof e?document.querySelectorAll(e):e,n=t||"js-reframe";"length"in i||(i=[i]);for(var o=0;o<i.length;o+=1){var r=i[o];if(!(-1!==r.className.split(" ").indexOf(n)||-1<r.style.width.indexOf("%"))){var d=(r.getAttribute("height")||r.offsetHeight)/(r.getAttribute("width")||r.offsetWidth)*100,f=document.createElement("div");f.className=n;var s=f.style;s.position="relative",s.width="100%",s.paddingTop=d+"%";var a=r.style;a.position="absolute",a.width="100%",a.height="100%",a.left="0"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\be74a27e28e7536c49244db9a205121ebc71e0d9[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1016490
Entropy (8bit):	5.570753960513642
Encrypted:	false
SSDEEP:	24576:s3G13TSZWkcSO2dp1vyUOPQvLgJAhVuhGLZcW6Hp5q+OFaGOgWdHxGcrAhVuhE2L:s3G+vyULZD61JlVDu
MD5:	A45769C3077808E86F330B4001B23ABA
SHA1:	BE74A27E28E7536C49244DB9A205121EBC71E0D9
SHA-256:	DCB0F46E837F7821AB0537F949B8626619B82E15820153365FE93B0EDBC8C7EF
SHA-512:	0C7E2A157F07842DF99E3FF1870F0E328C0AE56B5AAE3B0EB60E7336BDE9CC002606267846FBBE5F3F3CB3FD166CA616E0271A83080AF83794C44C8D3B94DC9D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d33wubrfki0l68.cloudfront.net/bundles/be74a27e28e7536c49244db9a205121ebc71e0d9.js
Preview:	_N_E=(window.webpackJsonp_N_E=window.webpackJsonp_N_E||[]).push([[6],{"0sNQ":function(e,t){"trimStart"in String.prototype||(String.prototype.trimStart=String.prototype.trimLeft),"trimEnd"in String.prototype||(String.prototype.trimEnd=String.prototype.trimRight),"description"in Symbol.prototype||Object.defineProperty(Symbol.prototype,"description",{get:function(){return/\((.+)\)/.exec(this)[1]}}),Array.prototype.flat||(Array.prototype.flat=function(e,t){return t=this.concat.apply([],this),e>1&&t.some(Array.isArray)?t.flat(e-1):t},Array.prototype.flatMap=function(e,t){return this.map(e,t).flat()}),Promise.prototype.finally||(Promise.prototype.finally=function(e){if("function"!=typeof e)return this.then(e,e);var t=this.constructor||Promise;return this.then((function(n){return t.resolve(e()).then((function(){return n}))}),(function(n){return t.resolve(e()).then((function(){throw n}))}))})},"7W2i":function(e,t,n){var r=n("SksO");e.exports=function(e,t){if("function"!=typeof t&&null!==t)thr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	42523
Entropy (8bit):	5.082709528800747
Encrypted:	false
SSDEEP:	384:6RvBBVkrJxvcwYBUQ7X85AUfvDUNeFUBOgBmjeYP4PSvSdlb1bGjpXJNNRyIrOM:2k0p38OBmjeYP4xb1bG/bRyIH
MD5:	C2656E265EF58A9CC9F4B70B15DA5FB9
SHA1:	85C5EBDB89D4574D72688C2650D4B84B9B09770A
SHA-256:	F1D083FFAA644C708F11DB29707AA57C19246E6D32643B03FEE3F82C17B224B3
SHA-512:	6417AADEBEEF4EE35381BFC7034148D57FD061D84DE9974D798468C6426C24A6BD1C9913CF517ACCF3E349FA06CBDD546D2883EA8391C595285FE0C6127E268
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tlgr.org/css/bootstrap.min.css?3
Preview:	/*!. * Bootstrap v3.2.0 (http://getbootstrap.com). * Copyright 2011-2014 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */../*!. * Generated using the Bootstrap Customizer (http://getbootstrap.com/customize/?id=92d2ac1b31978642b6b6). * Config saved to config.json and https://gist.github.com/92d2ac1b31978642b6b6. *//*! normalize.css v3.0.1 | MIT License | git.io/normalize */html{font-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,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:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:bold}dfn{font-style:italic}h1{font-size:2em;margin:0.67em 0}mark{background:#ff0;color:#000}small{font-size:80%}sub,sup{fo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\corona[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, 1250x650, frames 3
Category:	downloaded
Size (bytes):	81645
Entropy (8bit):	7.983446717339808
Encrypted:	false
SSDEEP:	1536:cjot9qHlPNRZc8f6cenndN+UMxF/ZFebqfL+Q7TMv4vSKk05bNZMR7hEeqb7aeYX:cjotAHldc8S5/+UmJrwqH/kC+05H2VoG
MD5:	D74ACCAC575AE64E6555F93DE5CF2B50
SHA1:	23A83DC287005A1BF14F577ED891C5B7A0F884F5
SHA-256:	5049DF08B5D6FFC14AEB22A8E6B3C8B742B34F7065DDF603801310FAC74D711E
SHA-512:	59382CCAC8B90EB7DFC485FC4230E54672710C8A639BB5CDCE517AEB1BB6AD00D29382A4A184362579DAEDD5C31557649E5617C7038B53900A2356514B6AC4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d33wubrfki0l68.cloudfront.net/23a83dc287005a1bf14f577ed891c5b7a0f884f5/2b818/images/corona.jpg
Preview:	......JFIF.....C.....!....."$".$.....C....."......./..1.....(...B...-,..-....,.,.,.....PT.....AR.JJP.R.E.P.K.E.DQ.@%.DXEY.b.L..RRb..T.b..U..,.L.%Y..L..Rc2...$..U.....(.J(.,..*....,...(.T.....J..)P...*.,.....JT...,.E.K(.J@)DQ.E..%.!...*.L.*".(..$. "..,"."b..)Re,...I2.&Q1.J...F3)f3)d.b.9....*.B...)@..J)R..*.T)*.....(.,...B...)PPR.....R.JAK..E,..E.DQ.E.DQ%.DQ%.I...H....)$.J.T.YRe.2.Ia&R.(.e,..(.e,.e..W1}>.@.X.QE.Ub.eQ TYeRRU!E..U.TX.U.L.t.\z}=..:.DU..v...._=.SQT.QIIJ...X.QIH)b.T."... .."...*..(..$....I%.UI.I*....&R..&+*J.K.2.b..(.e,../...J)(...(..R..@.,....(...*..I..y=..'...O...w.UQ..>..O...o....0...|<zz9 ..!neU.%.RU%%...% ..@.....J".(..*..,".L.@.eI.$.....&R...2..f+.,.J.V$Rr.....P..UYH.eX.U.H*R..T.R.RWn.M..|..s.....h|~..<^...W....G..._F.M...~.z.C..k..???mV.C...t. U.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\corona_impftermine_agb[1].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):	95569
Entropy (8bit):	5.565595223537657
Encrypted:	false
SSDEEP:	1536:FRHO4AsKAtsAEyANbAjUA0zAu2A1JAWeAIFAsaAKUMSfg1Fb2165+c:FBOYDcPwUVTza9wfauFs6cc
MD5:	C0EFEA7053664384A71619DF229652DE
SHA1:	3253EFBBA5EBDDDEEAED5A7219E28E2BA5AAB984
SHA-256:	08403F7D82E77CE14AC3F3D35E6DB5C4EAFDA4501C661898FF0FFA0102F2F0C8
SHA-512:	EC1DA7DBD6354918CC50317CCCE006A89334501F547068081F3D838119D09FC640EE762176980EB46DFEFB6C78D22D1804BFFD4EEA9A62CBDFC2AD048A5DC C
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>. <head>. <meta charset="utf-8">. <title>Corona Impftermine Augsburg & Umgebung . Telegram</title>. <meta name="viewport" co ntent="width=device-width, initial-scale=1.0, minimum-scale=1.0, maximum-scale=1.0, user-scalable=no" />. <meta name="format-detection" content="telephone=no" />. <meta http-equiv="X-UA-Compatible". content="IE=edge" />. <meta name="MobileOptimized" content="176" />. <meta name="HandheldFriendly" content="True" / >. .<meta property="og:title" content="Corona Impftermine Augsburg & Umgebung">.<meta property="og:image" content="https://cdn4.telesco.pe/file/W64IsBmms FuC9_GQAxZjWJM2xi_VDAdUZWx5uPYuDtdljMogWKJ6Ml4ZIRjw9UiHxwGyP00YDX3Xd5OXogA_vZwQ9NHz1Dy_ebt89yVhLSuf9Y9F6t6l0aAI19lQxaeE88ckBar_CBW VgiFp2Rx6gcTWkMVGTtlI-uBsQD4Qts6c-GL4iC2lAmMfJ5bBSaVyZlOCqq62tuBNJhmtETwaeGiPhW8yFkzXcq1FAunJuoF-mxZldVHJCuegqX6XRchwOajY4q8sNXsU8 luneIA6AxMy9ldEblDeHmY5yiyqjf5XswChzte3piiPqD8dEOR7PNUPT06olVvsUCd-vMwEHg.jpg">.<meta pr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\majestic-octopus[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1494 x 224, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	25958
Entropy (8bit):	7.893425904661911
Encrypted:	false
SSDEEP:	384:xlC1c2DYwNLyo5dkCezramculQGP3/t6CVwoXic84mV6HEUDC6Qe0qZ2L6lu7s03:xlCCwFuTcuNnsCyoT845EUOBs8C2Vt
MD5:	0A2A243CA6431D7DDC0A6B8FD052E440
SHA1:	011E84784814D6CC0B2D8FE255786117680FC476
SHA-256:	907EE21301B7351FA35CC6EEB5063C51A4460BA2D7E11797B3CE9B99678D08A6
SHA-512:	FBDF7B0E97C0CD33E02092E79674590F69DE24F6CB239CC48051DF1D2ABD2FFF1E5361CE10A011F78B49E5CE0A3A3C3F099BDB322BEDBC5D8F9921E5403C8 52
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d33wubrfki0l68.cloudfront.net/011e84784814d6cc0b2d8fe255786117680fc476/557b6/images/majestic-octopus.png
Preview:	.PNG.....IHDR.....sRGB.....gAMA.....a.....pHYs.....o.d..d.IDATx^...|.U.....z.#..U@.R_...J."EiJ...&.H...{. .....B*.w`...I63w...>...{6.2.;s..;w.ccc.....@O..... .."..... !..... "..... t.....y..W.;..t(....z..... X..E0..... Ni..\].^.....O.?..._..... pv...._.]u...:.`.9}j./.%..... '.I2.!.b..sm.H..... e'..Z._..... r..... `,{.`.._$..A.`..... Jl>..... lY. s..... X..... _".?.Q...K..... c..t.r..... Rys..... `,[...(.9.x0..... "..`../OBO-.\.`N..... ".e._..B..... Vgc..... -..... _..... F..... m.._..... (..... @..... `..... 0..G0..... ....0%SG0....C.F..... d..FA.B..G...m..... 1...../..*.3..3.K..... 0c.#..H.J..=.`..... `..... ;.j.l\..... F..._`..... F.h..... 1K.. .....n..>@..... &a..FA....a.....^..%IA..... ..a..FA..... M>,sm....H.0..... `+.<.....I.E.J..)U..}...x'O7'..R..*.3..3.K..... {f..|).....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\polyfills-fa276ba060a4a8ac7eef[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\polyfills-fa276ba060a4a8ac7eef[1].js	
File Type:	UTF-8 Unicode text, with very long lines, with LF, NEL line terminators
Category:	downloaded
Size (bytes):	91915
Entropy (8bit):	5.34010011478498
Encrypted:	false
SSDEEP:	1536:OCsSKc+khv9ZG2pq+bM+/9y2Bw9ew5AM3jM:Gb+1XbMuoo5
MD5:	85057EA5C52BB02A6BE4FCCC0CFC015D
SHA1:	17B4F4EF85574526E9BB7AE9C78BFFABE26B0E99
SHA-256:	55BE819EE91320D2EE025BDA40DD363BAB281C9395DB00AFB3F726E2E939C1B4
SHA-512:	04B91D1F472EC61D7DCF22E2FFE26285C64E25C9E2E921ABBCC047546A423476518E68B48B0DCA2C10FED9334EBF238D7E90DFFD15ED070CDBD42935220B342
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d33wubrfki0l68.cloudfront.net/js/17b4f4ef85574526e9bb7ae9c78bffabe26b0e99/_next/static/chunks/polyfills-fa276ba060a4a8ac7eef.js
Preview:	_N_E=(window.webpackJsonp_N_E=window.webpackJsonp_N_E||[]).push([[11],{Ri3X:function(t,e,r){(function(t){!function(){var e="undefined"!=typeof globalThis?globalThis:"undefined"!=typeof window?window:"undefined"!=typeof t?t:"undefined"!=typeof self?self:{};function r(t,e){return t(e={exports:{}},e.exports),e.exports}var n=function(t){return t&&t.Math==Math&&t},o=n("object"==typeof globalThis&&globalThis)||n("object"==typeof window&&window)||n("object"==typeof self&&self)||n("object"==typeof e&&e)||Function("return this")(),i=function(t){try{return!!t()}catch(t){return!0}},a=!i(function(){return 7!=Object.defineProperty({},1,{get:function(){return 7}})[1]}),u={}.propertyIsEnumerable,s=Object.getOwnPropertyDescriptor,c={f:s&&!u.call({1:2},1)?function(t){var e=s(this,t);return!!e&&e.enumerable}:u},f=function(t,e){return{enumerable:!(1&t),configurable:!(2&t),writable:!(4&t),value:e}},l={}.toString,h=function(t){return l.call(t).slice(8,-1)},p="".split,d=i(function(){return!Object("z").prope

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\0QI6MX1D_JOuGQbT0gvTJPa787weuyJF[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 56868, version 1.1
Category:	downloaded
Size (bytes):	56868
Entropy (8bit):	**7.99088107589825**
Encrypted:	**true**
SSDEEP:	768:OwvVA3GrndVK0xSPkSdZfOBLMjZnBTavFk4Izs6/4s5azWIoqMilof:bm4dVK0xzSNZBmtNIs6yCIoHilof
MD5:	157315714887E2D69FFB9F6A3E3145EC
SHA1:	FE07E44F6ED00C231BD9468BDBCDB5F289314FD8
SHA-256:	6C57A2969DC53695979E2FCA37D35E4F15913AEED5688E84F8681C52BF7B1C0B
SHA-512:	C0F3764F8EAD35914E7B800078B0BC5C09FEF123848AF7C7519B262C93A0356ED25DF95B0F5CB8FBF4EB6CB15E0F979D18EEC70721C12A9A152834A1DC59075
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lora/v17/0QI6MX1D_JOuGQbT0gvTJPa787weuyJF.woff
Preview:	wOFF.....$.....GDEF...l...-....m9q.GPOS.....;.....f..GSUB..><.....(..W.OS/2..B4...R...`.2\QSTAT..B....8...D...cmap..B.....n,..gasp..H.....glyf..H. ..\|.....W.L0head.....6...6....hhea..... ...$.b.bhmtx...<...y....y.]loca.....C[..maxp...\..... .{..name...x...5...f;y[.post.....l.....prep.....h...x.....p.....^.m7d.M.m.nlF...e. .ff....w..3..J.....d.$.?Y...E....5U.p.Y...A.....u..3d.#..Y..N.#.....d}"..Y..W.,LNX.%..+`uW.6n....;.3.vo...8..p.'.L..^.K..Wx...Z....q.w.~..c>..}./....-..{..o.?.....eSY..*a.....8<... ...b."&.d..JU.F..Y%.st.....\w..g.V....T9..H...7...T.I.E....x.l..l]Q....m.n.f.m.5.5..6...l3...6.y...n.;V.=...K.@..b.Rr.\.....0....`....0.*..v}e...z.^....\|J.....z.....r-.\..K..Q..i.U...y.[.%...,o . <...l.`."i..E.bw.....nr.dyN..z..\.\|.H`</....o..*.N.^.....M.i.##.....T~s .\.sF.S.R^GD.....M.h.\|dD.iT.....7.2.N...Y."..9..WGmf.....p..lu.{"9...$...t>....nae.+.KT..3*_..].i.4V

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\0QI6MX1D_JOuGQbT0gvTJPa787z5vCJF[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 57768, version 1.1
Category:	downloaded
Size (bytes):	57768
Entropy (8bit):	**7.991115765253452**
Encrypted:	**true**
SSDEEP:	1536:LbaRh4jgw9cjz8ikWAqKfht2FmvRdnQmB6xa9lof:LbaPjz5kZqAhUFGVs8k
MD5:	7539F03619F5DC85A432980B7B450021
SHA1:	489A394B14434955F8620891B7BF392B4FF355DA
SHA-256:	5B462AA803F595F15FA660103FD141A5A8CF1498FAFF3693DA398A8378FB93AC
SHA-512:	C6BD54BA1FD181FFEA5A7DDA199025360BDB09626A71E6E365063B332216D038ADB9613C4EB28010C62FC43AD9E30A69E58895648F25C0B089715F7F143E956C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lora/v17/0QI6MX1D_JOuGQbT0gvTJPa787z5vCJF.woff
Preview:	wOFF.....<.....GDEF...l...-....m9q.GPOS.....@....n..7EGSUB..B.....Z....OS/2..F....P...`.^\1STAT..G....8...D....cmap..GL.....n,..gasp..Mh.....glyf..Mp.. {.....f-head...t...6...6....hhea..... ...$.b.bhmtx.....x.....fr.loca...D.....E.maxp..... .{..name.....,....N8.X.post...4...l.....prep.....h...x.....p.....^.m7d.M.m.nlF...e..ff....w. .3..J.....d.$.?Y...E....5U.p.Y...A.....u..3d.#..Y..N.#.....d}"..Y..W.,LNX.%..+`uW.6n....;.3.vo...8..p.'.L..^.K..Wx...Z....q.w.~..c>..}./....-..{..o.?.....eSY..*a.....8<.....b."&.d ..JU.F..Y%.st.....\w..g.V....T9..H...7...T.I.E....x.l..l]Q....m.1..{k....y.V...5..`f0/.....|=u...w,..0G4.a..5m..kV-..QS.T.G..@O....A..ji1.k....Uk.....`@.`.#X..o...b...1e....z..T..!y.8D.CB ...PN..f.o.....&/.....`k.pl..{....!.D.-..x.X...X....A.I.H..OB.8.....\hmXm.0.....!..'..B>..>..#....g\...~....K.."d...o81Z...dw..[c.9..X....'.....ZvD.g.v...)...R...^.P..S..../).

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\0QI8MX1D_JOuMw_hLdO6T2wV9KnW-C0Ckqs[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 61340, version 1.1
Category:	downloaded
Size (bytes):	61340
Entropy (8bit):	**7.990769641292479**
Encrypted:	**true**
SSDEEP:	1536:MAUXEJLrfYmIiSzjfQX7kR7l3li+hKNfhy2c:xJLDdLX7gnRKy2c
MD5:	1B9568024582152E9E74AF37D48DD6BD
SHA1:	BFD34BB13814126AF2454136A4C25073CD0C37A8
SHA-256:	E760AC48568E3A552C87B1E153DB96A82E12940F0F7B2A7C33C6BD33F1FED5A5
SHA-512:	F84D7C917DA6A34DC16A5A4DB002C4DCD923AF8FA64B6CC821B39C721477C870BDBD98EFD80F5A4D3A0868AB21C2D70359993FA4B2353AE10F7667D571328C2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lora/v17/0QI8MX1D_JOuMw_hLdO6T2wV9KnW-C0Ckqs.woff
Preview:	wOFF.....GDEF...I...I...8....GPOS.....>I...p.xz.GSUB..A.....OS/2..D....T...`..\BSTAT..D....6...@....cmap..E4...-...|.W..gasp..Kd.....glyf..Kl.....hJ6*.head...|...6...6.q..hhea.....''...$...ohmtx.....VGloca...X.....maxp..... .u..name...../...l:.Y\|post...@...S...u..Z.prep.....h...x.....@.D..9.m.m.m.F.A).....;..*..J*...{%..3U''..Yu.jGVG.....d.$k.Y..I.:.....d.#.<Y..L.U.n.u...d=%.%Yo..D.7}.-....u^,.''X....`s7..n....{....X...8..p...B/.e^.+...{=n.F..m..;p.w.~..c>..}....>..|.'.....?....7...9.....X(..b...H%.*..Sel..b.....89M..z.WD.h.Mb.B..\5.....>:D...=../.QfS.M[..n.Ce.W.T.../5d9.....J....x.l....Q...o..m..y+^.Y.mc.m.....`F.....3....3.@.$1q)9p..6...-.....).....4...[+.7.....>..P,.$..R....MY..ly.1L ..K.I\hN..U. ....m..1..K...-..}.H.B.B....1.6.@..?.....N.N..C..9M..=..>6.....s..sy.V.\.x...AYAK.....?...{./....X....$.e.<".M.7.7.B..F....p...7.!..F.<e.....0..:!.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\0QI8MX1D_JOuMw_hLdO6T2wV9KnW-MoFkqs[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 61540, version 1.1
Category:	downloaded
Size (bytes):	61540
Entropy (8bit):	**7.9910298710343435**
Encrypted:	**true**
SSDEEP:	1536:gkSskWFrpipze48RRXM6RkATaa4Da3/Oq1CbM4RJOe:rw6bRXMGxx4s/qZR0e
MD5:	38A9B97FC84C74D4FE3590E1CB139704
SHA1:	AB25883B16E8C5FF88A300D3065FE021A092AA20
SHA-256:	AA56B82317347E39F791C7975C00CD0BF1C51B6CD90F925A3D4334D42748FD37
SHA-512:	8DC47FD08BE1C3D5748AB20B7548A3DBE20716697FE584C7BF11F8CC130D8174594487AD07F545B45AD960EBADCA369D2C138CA14361246F83D820A4E8B811C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lora/v17/0QI8MX1D_JOuMw_hLdO6T2wV9KnW-MoFkqs.woff
Preview:	wOFF.....d.....4.....GDEF...I...I...8....GPOS.....>a.....0..GSUB..A.....{.]_OS/2..D....T...`.U\"STAT..D....6...@...cmap..E4...-...|.W..gasp..Kd.....glyf..Kl.....1.,.head... ...6...6.p..hhea...X...''...$...ohmtx...\|.....N+k.loca...,.....maxp..... .u..name.....<4.T.post.....S...u..Z.prep...\.....h...x.....@.D..9.m.m.m.F.A).....;..*..J*...{%..3U''..Yu.jGVG.....d.$k.Y..I.:.....d.#.<Y..L.U.n.u...d=%.%Yo..D.7}.-....u^,.''X....`s7..n....{....X...8..p...B/.e^.+...{=n.F..m..;p.w.~..c>..}....>..|.'.....?....7...9.....X(..b...H%.*..Sel..b.....89M..z.WD.h.Mb.B..\5.....>:D...=../.QfS.M[..n.Ce.W.T.../5d9.....J....x.l....Q.....8.....m.....n.FP..4.....!..._.A.....&.7.w...R.....bH..;....FX6767.....U.9.^!..a....|k..A$1'1EK.o3.+.zr.1.Q..r:...;...$.u...c:..:....p..+...>..MYJ.0.).g.w.....o....+fQ..-.?.u.....vUs..r.&.2.....&s.9N-_8._.n.....s..GH)..|K(^=.<.w..&....S.....7..Ie..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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\G62TDH9B\augsburg[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):	52382
Entropy (8bit):	5.0640768999901695
Encrypted:	false
SSDEEP:	768:UUn4u9JK2adhMRMVfBwPBwkzKLKb5ApeJ8pC/kKpJ7PuKRM1EJt+SzAoSxsKXXmy:dmVm2fIaF607G/53jYh
MD5:	57A674D976CE0B11C572BB8B69303F00
SHA1:	E08B846558DE23DDA2370155A48983B4FB41C1B7
SHA-256:	2B52D6E1506E328229D24A62DF48292F0BF75CC410D027482F32F910084686D0
SHA-512:	0A7D80E5DEA622E23D980EED307467FAB722A1F041F28477CCD41F125F36060D1620D5AF6A332EE39D498D1FEE1601C11E15C442CD34A2DA235426DD70587C3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.corona-impftermine.net/augsburg/
Preview:	<!DOCTYPE html><html><head><link data-react-helmet="true" href="https://fonts.googleapis.com/css2?family=Lora:ital,wght@0,400;0,700;1,400;1,700&display=swap" rel="stylesheet"/><link data-react-helmet="true" rel="icon" href="/images/Download.png"/><meta data-react-helmet="true" charSet="utf-8"/><meta data-react-helmet="true" name="viewport" content="width=device-width, initialScale=1.0"/><meta data-react-helmet="true" name="google" content="notranslate"/><meta data-react-helmet="true" name="description" content="Finde freie Corona Impftermine f.r den Umkreis Augsburg"/><meta data-react-helmet="true" name="robots" content=""/><title data-react-helmet="true">Corona Impftermine Augsburg</title><meta charSet="utf-8"/><meta name="viewport" content="width=device-width"/><link rel='preload' as='style' href='https://d33wubrfki0l68.cloudfront.net/css/f32e8963c988162755fb15c930cba39355a7da17/_next/static/css/06e00db3ad673e94378c.css'/><link rel='stylesheet' data-n-g href='https://d33wubrfki0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\corona_impftermine_hh[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	6482
Entropy (8bit):	5.491640256060032
Encrypted:	false
SSDEEP:	96:6oYvTl4oYvTDStM1O4fT5298oYvT1Q1WMzz9cdcSqj70GqLTt:fgZ5gHSCXSgi4MzHZ8t
MD5:	04BE7D66AC6B68DB557612364B7BAD5B
SHA1:	85801F40B24345AC43F9D56A0DA618A58916DB86
SHA-256:	972B7F88C0A81B2FF17B7CE6B0797CA7174CD5CC86C67F0A125EB78AC8CAC6D1
SHA-512:	BD16693A2FDB8E8B7E6B0FA55A6B5A3D2684AC4B05BC3FE5100755A57E6052E96685E22A6E7BF7207CE9141CD72DC90708A9D03D22FB1ECC44E50CB42882C06
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>. <head>. <meta charset="utf-8">. <title>Telegram: Contact @corona_impftermine_hh</title>. <meta name="viewport" content="width=device-width, initial-scale=1.0">. .<meta property="og:title" content="Corona Impftermine Hamburg & Umgebung">.<meta property="og:image" content="https://ttttt.me/cdn4/file/WMPWzsM8W37tnne6-j1xjcoxulxwfB2wwds_UyVJOQ8yH9ng3jtjihpzXs1AWj23fkkYir6-dmLKK3u8FlMkoaMttuyAMfs3HQPeu7N8suZGx3Z6mooWFEHVSyGlkpU6cpVGwoemP8xlaHiW4JCz8hz546gijsi-a_UAwnElg3ce6POWmxMNnao8motGFAsKKfTQ0NrTMHMcMbRNOdRZ_WVLXOruSXXYuHCxn9mXqnFJXltxulVmWOjJ7YiOAVZ4m4OTCdWPsAKFpSiRPIOHPphRa1sMyu-NlOojagAHqalleIbQdVgwOUI7xFoOvDr5WuXdW66-_w3lvszOnqpFHw.jpg">.<meta property="og:site_name" content="Telegram">.<meta property="og:description" content="In diesem Channel werden automatisch freie Covid-19 Impftermine im Raum Hamburg gepostet.">..<meta property="twitter:title" content="Corona Impftermine Hamburg & Umgebung">.<meta property="twitter:image" content="ht

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\nurnberg[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):	52390
Entropy (8bit):	5.064158345504589
Encrypted:	false
SSDEEP:	768:h9n4u9JK2adhMRMVQEJRBwkzKLKb5ApeJ8pC/kKpJ7PuKRM1EJt+SzAoSxsKXXm1:NmVfcfIaF607G/53OYh
MD5:	F2306222DF9BF5E63F4C60D7F618A057
SHA1:	BBF6576F98C724CBEEB040B9647439B7AB75CB01
SHA-256:	9F3BC41D5242B45B10F71A7BCF77EFBC3FAB2DBF091B18961279657DC0FA440F
SHA-512:	CDDF1AEBE6B493532129038CE24EBAD214C78DE1C5DE3A5BC6B7C6B3C1F378088FB300C77A4FE5855EA947BEC01DCCFEEFC7AD54A682C1C51C32A6759FA3729
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.corona-impftermine.net/nurnberg/
Preview:	<!DOCTYPE html><html><head><link data-react-helmet="true" href="https://fonts.googleapis.com/css2?family=Lora:ital,wght@0,400;0,700;1,400;1,700&display=swap" rel="stylesheet"/><link data-react-helmet="true" rel="icon" href="/images/Download.png"/><meta data-react-helmet="true" charSet="utf-8"/><meta data-react-helmet="true" name="viewport" content="width=device-width, initialScale=1.0"/><meta data-react-helmet="true" name="google" content="notranslate"/><meta data-react-helmet="true" name="description" content="Finde freie Corona Impftermine f.r den Umkreis N.rnberg"/><meta data-react-helmet="true" name="robots" content=""/><title data-react-helmet="true">Corona Impftermine N.rnberg</title><meta charSet="utf-8"/><meta name="viewport" content="width=device-width"/><link rel='preload' as='style' href='https://d33wubrfki0l68.cloudfront.net/css/f32e8963c988162755fb15c930cba39355a7da17/_next/static/css/06e00db3ad673e94378c.css'/><link rel='stylesheet' data-n-g href='https://d33wubrfk

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\telegram-web[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	21613
Entropy (8bit):	5.013434709455319
Encrypted:	false
SSDEEP:	384:TNJ7JEw2M9bx3M2D5j2Bu4dCDAqyDBSSdJr8siJqv:TNJFE1M9bx3hD5j2Bu4dCDAqyESdJr8K
MD5:	F39F05A7730D83C2B724E1E113A29E16
SHA1:	00C8E55038BC934212E73F0798E2E7325966E759
SHA-256:	2892A779CEE25C3A681F6C8D4C779F0E8632741AEC6485A87DA48000D84B96C5
SHA-512:	4C9C1E06688DCA91736183A9B304560BC598160C8F0ED6C1FB0AFE34CA1A5AF521F4F1EC26F19D57AC3E4B9B2E72A531C30154515A501EFC033F001C84287E4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tlgr.org/css/telegram-web.css?19
Preview:	body {. background-color: #e5ebef;.}...tgme_container {. position: relative;. max-width: 820px;. margin: 0 auto;. padding: 0 6px;.}..tgme_header_right_column {. pos ition: absolute;. width: 312px;. top: 48px;. right: 0;. margin: 0 12px;. z-index: 1;.}..tgme_header {. position: fixed;. left: 0;. right: 0;. top: 0;. z-index: 100;. background- color: #fff;. height: 48px;.}..tgme_header:after {. background: #b5c0c8;. position: absolute;. left: 0;. right: 0;. top: 100%;. height: 1px;. transform-origin: 50% 0;. z-ind ex: 1;.}..tgme_header_search {. position: absolute;. left: calc(100% - 336px);. right: 0;. margin: 0 12px;. padding: 7px 0;. height: 48px;. background: #fff;. box-sizing: b order-box;. z-index: 1;.}..tgme_header_search_form_icon {. position: absolute;. pointer-events: none;. margin: 7px 9px;.}..tgme_header_search_form_input {. font-fami ly: 'Roboto', sans-serif;. font-size: 14px;. line-height: 21px;. padding: 6px 11px 5px 36px;. margin: 0;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\telegram-web[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	10952
Entropy (8bit):	4.751080759527913
Encrypted:	false
SSDEEP:	192:UtvqJJLo5eKyGKcalfalueKPfzDYwrLWKulvR/8pCXzalaRDX/2she2eUKaUcxpj:USf/fLAsU3Lb9kLCP
MD5:	497DC99EEA741A8ACC1F98E9E7FE7604
SHA1:	D573CADDA161B2C5566E68B0584370A65250DD07
SHA-256:	0F661B180CB5EC06A2458D8BE5C013A37ABE06A0D446945709010132CA813D15
SHA-512:	C60324FEBF3C2B4236DE4B5323C134EC436F2823F03A297E1E5177C21877CAA558DEC678FC43AD8238DB2F33BA5596E4AE75280BAB5B75F2F839A7BE3E5D1F9 E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tlgr.org/js/telegram-web.js?10
Preview:	(function($) {. $.fn.redraw = function() {. return this.map(function(){ this.offsetTop; return this; });. };. $.fn.scrollIntoView = function(options) {. options = options || {}. return this.first().each(function() {. var position = options.position || 'auto',. padding = options.padding || 0,. duration = options.duration || 0;. var $item = $(this),. $cont = $item.scrollParent(),. scrollTop = $cont.scrollTop(),. positionTop = 0,. paddingTop = 0,. itemHeight = $item.o uterHeight(),. isBody = false;. if ($cont.get(0) === document) {. isBody = true;. $cont = $(window);. positionTop = $item.offset().top;. paddingTop = $('header').height() + 1;. } else {. positionTop = $item.offset().top - $cont.offset().top + scrollTop;. }. if (options.slidedEl) {. if (options. slidedEl === 'this') {. options.slidedEl

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\telegram[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	110204
Entropy (8bit):	5.154627925179138
Encrypted:	false
SSDEEP:	1536:NyLkfDxm6Xt3iw93BC2oadm7Z1WoDYzdLV7EJJMOTNONwstox6rjxQDpZLE689d2:NyLk7xm6IwyxakO0YzXuYL9I
MD5:	EF37148841BB7A7DEC7B4D4AF1A63504
SHA1:	162F85A8C2DF9D9A9F0873723C2642A2E4D0AEA4
SHA-256:	5B9398BCAF041C4ED994C96AD2BECE7F60025417797254D34EDCF22D98B6BA00
SHA-512:	3A63AA0591232EC905E08DB1734F67ADBE7A733D8F7E3EED88C0ACC768FACE5B4CCF8EC68269B08EC6AABA66384BC57FFBF6A09E912AC8B5D779C7825B99E EA1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tlgr.org/css/telegram.css?212
Preview:	body {. font: 12px/18px "Lucida Grande", "Lucida Sans Unicode", Arial, Helvetica, Verdana, sans-serif;. /*-webkit-font-smoothing: antialiased;*/.}.html.lang_rtl {. direction: rtl;.}..a,.a:hover {. color: #0088cc;.}.a:focus {. text-decoration: none;.}.a:hover {. text-decoration: underline;.}...container {. margin-right: auto;. margin-left: auto;. padding- left: 15px;. padding-right: 15px;.}.@media (min-width: 768px) {. .container {. width: 750px;. }.}.@media (min-width: 992px) {. .container {. width: 970px;. }.}.@media (min-width: 1200px) {. .container {. width: 1170px;. }.}..container-fluid {. margin-right: auto;. margin-left: auto;. padding-left: 15px;. padding-right: 15px;.}..row {. margin-left: -15px;. margin-right: -15px;.}...container:before {. content: " ";. display: table;.}..container:after {. content: " ";. display: table;. clear: both;.}..@media (min-wi dth: 1px) {. .lang_rtl .navbar-nav,. .lang_rtl .navbar-nav > li {. float: right;. }.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\7c883d82dc35c1abaf98cbc00c7fda239ba0d096[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1016247
Entropy (8bit):	5.5706494475736426
Encrypted:	false
SSDEEP:	24576:s3G13TSZWkcSO2dp1vyUOPQvLgJAhVuhGLZcW6Hp5q+OFaGOgWdHxGcrAhVuhE2Q:s3G+vyULZD61JlVDD
MD5:	676B59957ED81CE19B9A407C85587004
SHA1:	7C883D82DC35C1ABAF98CBC00C7FDA239BA0D096
SHA-256:	D3DBD097D392D7CEB24719281DE0AC49E4793FC9D5BE822DE3111AA11FCCB1B9
SHA-512:	B9E8AD6CDC6F648D212C793CE62E80BB3D1B8ACBDC5350C558B478FDDB3F25E8C8E90ECEBC9873E15429E96DA6BAE89AEF18F31BDA3A1CF4BC0B4D77FE1(B84C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d33wubrfki0l68.cloudfront.net/bundles/7c883d82dc35c1abaf98cbc00c7fda239ba0d096.js
Preview:	 _N_E=(window.webpackJsonp_N_E=window.webpackJsonp_N_E||[]).push([[6],{"0sNQ":function(e,t){"trimStart"in String.prototype||(String.prototype.trimStart=String.prototype.trimLeft),"trimEnd"in String.prototype||(String.prototype.trimEnd=String.prototype.trimRight),"description"in Symbol.prototype||Object.defineProperty(Symbol.prototype,"description",{get:function(){return/\((.+)\)/.exec(this)[1]}}),Array.prototype.flat||(Array.prototype.flat=function(e,t){return t=this.concat.apply([],this),e>1&&t.some(Array.isArray)?t.flat(e-1):t},Array.prototype.flatMap=function(e,t){return this.map(e,t).flat()}),Promise.prototype.finally||(Promise.prototype.finally=function(e){if("function"!=typeof e)return this.then(e,e);var t=this.constructor||Promise;return this.then((function(n){return t.resolve(e()).then((function(){return n}))}),(function(n){return t.resolve(e()).then((function(){throw n}))}))}),"7W2i":function(e,t,n){var r=n("SksO");e.exports=function(e,t){if("function"!==typeof t&&null!==t)thr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\Download[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 225 x 225, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	2306
Entropy (8bit):	7.871155160089189
Encrypted:	false
SSDEEP:	48:r7dYOFe4zz1eENwGQCn6cAutkajhNFbi70dRfBJdZi8wHVev9CyuKQxM:rN9tNzUcA1ajLFWqRFZideE5+
MD5:	B4D0B7BDB3297FF446E7B2C7F05831F3
SHA1:	3AF8FF792AC113107F5A2A1BD4AF2F93DE1382B1
SHA-256:	155114DCE95D6969A85AC0B65B47AE5B65EC397CFEF676B380FD3E2808773255
SHA-512:	6D724F38335D51A41E22A3DF129E7ABF7F2D33CAB619067AD915D5DBC20789E1BED853B241C77D81E67A1740837DCE98C1E1791A23F6557A29DF2854CDA2A5A B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.corona-impftermine.net/images/Download.png
Preview:	 .PNG.....IHDR.....m"H....PLTE...Y...IvL.....>oR.....AqE.....Ftc.....p...;n...Ot..4j....6k;f.1`.....0h.....Cr...#Y.....Cl.\}.....P{...{..f.....n)!...-IDATx..ic.8..c..54.. ihv.....@.%..H.....R.<...qw7h.A.....|..gl+...f>.?=..mG0}.....@.....M....h...mL.....G..Is.K.|..m..I.1.C.0.-_....8x.....{.5v....`._..x..8..b..[..h..+.I~U.<!~.6.4.qyQ.....xQ....Q. ..|.G.X.&V..5.....vk.:J...6@.c.2..)T!....E.Mc.'g....2f...x.<!n}.I..tIA.....$..[..&..E.0.]....#.....Q.....S.V[.UM.z...o.-..k.....Ym.d.k...k.,`C]...O...t..d.[T.[!...."Y...FD.../..... .Z.....Sz.,.U.L..\.3..Zvx....^ .....O.....OYpDa.,.S.{.....Q+O^Z..O.....B...X...w.y..|...x.Kg~.W.....|.}... .b.....Q.."j.q.....6.Q.&0..Z.....Qma?..fWU",,.B.D2....4....&.....8.?7....{..I. .%.....o.B6..bM..=.H(....|.{..\.....^.<x.#bcF.9..w.'M....E.s...6....: ...t.8.....A.M.e../.....j..m.hQ6....Vu.>"Z.~..h]....C._.N..>!:6_(!...)!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\HFJ43SQZ.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, 160x160, frames 3
Category:	downloaded
Size (bytes):	3620
Entropy (8bit):	7.745128617392163
Encrypted:	false
SSDEEP:	96:pk45zekz+cvX8VxsZqln/LOegKXlStXt7c08:a45zSSMVxw89ez8
MD5:	ABB102E751D2C4962A28BE7F805EF620
SHA1:	100AB737142622C0CD8B5108E366D06C3A1A3544
SHA-256:	C0655445D5FBEECDF2C5EFD3DFD62781BB6C9750FAC2B22D4CB30F884DED1B87
SHA-512:	1A7C7AAC90760FAB77C35BB0E70D69C0B56B50467B41DE0D6E6FE87F397EEC9B0F2799E456918FCE4D0CAC8D7E404A49FF7A7CD357F5EFA8CA64F91049EC7(8F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn4.telesco.pe/file/ICVK3nG1WQZ2PlqPX2EgfYssz-2u_Ih8AK1GV_WiJLXKs8fTJCLPFTELhERyPjmktublhsElspSdOUVRudzZKo1EbE_vb3NeBcqj- sKkBi9LEIuRTO_SoDexfwcncyWJWKofQzOl6uVtw-yBXQAEzBr7WuKZlTA5tKW0GYYlqGeDRj- Rf_Qohnt8f4NmJymVCK5PxJrVWV6efSnEroXGj0K3rVqR2mktAf46xIDvBm8F8uQlNoLl3PkEg6lrwl5wzAdQzGBazgbrvSpcyFOmUpYleCYu66zjaVjPTjC0EP9Vl61wE4kYM PeN7mnZ5PU3HPYIByqYHdRYYmd5e2efPQ.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\HFJ43SQZ.jpg	
Preview:	......JFIF.....H.H.....C.....C.....".....8.....!1.A.."Q2B RaqC..#3...5r.....4.....!1AQ..aq.."2BR....b....Cr.....?.....}...e..C..s<....Id..x!g.....@'...I.mt.G3. <..w..7..z8.....Sq. .A....u..h.. .W.G.P....^9..*....j....+{L.Yh..a?...ke.-$...L.m....ZL.....U.S.e..2.Gh....._D.].8...m.....q.O}1...3.....{..s^.4.#.bGu.V).c..'..s...Z.:.(.SP.al:.KH'..}] {%..I.....:.F....k.....Y.....r"...:>~.v.B.m\."""""""""""""""""..Q.?4a<..U..op..p..GE..M..Y..'.y.....J..N_.x?.n..iU$V.^....oT.....q..`.q ..{9.'.ST.?...3_Q...[hae(s..H.w...9..~4.v.gQ`,h.. xi..\..0lN.?..?.....gDC.B.....R...9g.....@.....5I...q.T.l;.(...;.I.r;y=..c..u.k.<..v...<....q...>.B<.%.....K..x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\KFOlCnqEu92Fr1MmEU9fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20532, version 1.1
Category:	downloaded
Size (bytes):	20532
Entropy (8bit):	7.966425322589798
Encrypted:	false
SSDEEP:	384:tfEIIA0zhnegvIQxhXmqd8lpP/FwL0cV8yP1JSRHbNHlZL7qwZkoEu3HTbpXcyKd:tr0zhnewHxRmqd8PdwLLeR/ZLGwZLbTA
MD5:	DA2721C68B4BC80DB8D4C404F76B118C
SHA1:	3A32E8B7EFBC9DFB52F024D657B8C8C0A80E5804
SHA-256:	BD811625271ACCA47F7DAC48B460F13E08EE947B2A8E17E278C4D5CCB5D9323C
SHA-512:	5110656E41A261BD2A06F8B5B2A362FF8836B4289E1DE0777D83DB8E9D709C4C4248B67653A28FA47AD4AE823021ADBFC587900E142BF6887C2A7C936F7F4C33
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmEU9fBBc-.woff
Preview:	wOFF.....P4.....l.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...Q...`t...cmap.....#cvt .....\...\1..Kfpgm...8...2.....$.gasp...l.....glyf... x..<e..n..W..hdmx..H....m....+1.3head..IP...6...6...rhhea..I.... ...$....hmtx..I.....S.loca..L8.....maxp..N4... ... .4..name..NT.....:.post..O0..... .m.dprep..OD.....S.. .)x...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\OTUW0Q90\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20396, version 1.1
Category:	downloaded
Size (bytes):	20396
Entropy (8bit):	7.974131663185347
Encrypted:	false
SSDEEP:	384:SfXdUIIA0zhyKR28ePpAwxZ5M3py8wtshtdf45DEVTGdYb7H2Q/VEgm:Svdj0zhbRmjIQ8wtsV4lEVGdY3/i/
MD5:	68D6DABFE54E245E7D5D5C16C3C4B1A9
SHA1:	7FDAB895EAEBECEDB3FB5473EAB94A1B292CEF19
SHA-256:	A01A632E56731A854F35701AA8C3A6A19A113290D9032FF9048F8064C45383BD
SHA-512:	44EB151F85178A2F9600E85AD43FAE470FABE0F247C9A03E67931B36028E600C7550D9DE2D69B3576A06577A5DEAF54822EE4BDC9DCBB47588D1972C8A959D4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...Q...`u...cmap.....#cvt .....H...H+~..fpgm...$...3...._...gasp...X..... ...glyf...d..< ..l..C^]hdmx..H....m....03#7head..H....6...6...\hhea..I,... ...$.&..hmtx..IL....."J.loca..K.....maxp..M.... ... .4..name..M.....~..9.post..N..... .m.dprep..N.....)* v60x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m...../.& /6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D.._OK.$.Z.(..JR...\..\..\..\.\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....Hy.F.Jez....._? 7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20332, version 1.1
Category:	downloaded
Size (bytes):	20332
Entropy (8bit):	7.970235088150752
Encrypted:	false
SSDEEP:	384:U0iwaxoOUPVkOJJSu6SsCKTIRDqG9oHKwZh98OSv+MsgkAOY:75mlUmOSu1guh+fZhLSxkAr
MD5:	DC3E086FC0C5ADDC09702E111D2ADB42
SHA1:	B1138B84FF19EAC5F43C4202297529D389BD09B7
SHA-256:	EA50AC7FDDB61A5CE248A7F8B3A31A98FE16285E076B16E6DA6B4E10910724BB
SHA-512:	10123C785C396CF0844751A014413ECF4D058AD0C00CAAEF5F8FFEF504C370F03EACD0B3C2A49211EEE0877B7AE7D0EF6E01264F04FC910C2660584B5E943BE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Preview:	wOFF.....Ol.....x.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...P...`t...cmap.....#cvt .....T...T+...fpgm.....5....w.`.gasp...@.....glyf.. .L.;...m.&.x.hdmx..H....m....'/./head..H....6...6.j.zhhea..H.... ...$....hmtx..H.....]uloca..Kp.....m,maxp..Mp... ... .4..name..M.....t.U9.post..N`..... .m.dprep..Nt.....I .f..x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a\|.....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.\|.k..NF.....mox.;...7&.Y. .C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..").).[...._.T..T.. ...+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.I..F.$.2#.e..].[.....yR...e.\{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\W7YU039Z.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):	64617
Entropy (8bit):	5.1423836905924905
Encrypted:	false
SSDEEP:	768:on4u9JK2adhjRMVXEKpJqBwkzKLKb5ApeJ8pC/kKpJ7PuKRM1EJt+SzAoSxsKXX7:pmVvfIaF607G/533Yh
MD5:	B6A61770ED9FDD8256C86C89094338B5
SHA1:	D5967C4413311C2C9EAF58FF401CFB9B23F3EA76
SHA-256:	B2787B90EE5543FBFB46209051E2529F33E431100DF7CF9B21C08F2157E20DD7
SHA-512:	3C9CEE54CC19AF09DC520B4D4FB67125076741DA5F6363923BD6D1A248AD3C6F4A57E5991B8A79191B727B29546E097C22B7E5AAFBA30DE5A6B4919E9920B28E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.corona-impftermine.net/
Preview:	<!DOCTYPE html><html><head><link data-react-helmet="true" href="https://fonts.googleapis.com/css2?family=Lora:ital,wght@0,400;0,700;1,400;1,700&display=swap" rel="stylesheet"/><link data-react-helmet="true" rel="icon" href="/images/Download.png"/><meta data-react-helmet="true" charSet="utf-8"/><meta data-react-helmet="true" name="viewport" content="width=device-width, initialScale=1.0"/><meta data-react-helmet="true" name="google" content="notranslate"/><meta data-react-helmet="true" name="description" content="Finde schnell & unkompliziert sofort buchbare Covid-19 Impftermine in deiner Stadt!"/><meta data-react-helmet="true" property="og:type" content="website"/><meta data-react-helmet="true" property="og:title" content="Corona Impftermine"/><meta data-react-helmet="true" property="og:description" content="Finde schnell & unkompliziert Covid-19 Impftermine in deiner Stadt!"/><meta data-react-helmet="true" property="og:image" content="https://www.corona-impftermine.net/imag

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\corona_impftermine_nue[1].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):	6507
Entropy (8bit):	5.533845659659879
Encrypted:	false
SSDEEP:	96:8GKDFcxqCGvDFcxqCCStcjc8dcncuwwAg29cYDFcxqCX+3ucVMKkz2cGscSqj703:ZKDFcJGvDFcJCSgeEDFcJS7MF2Z8L
MD5:	270DBB135731A787DD43C45205EB5FF4
SHA1:	CC14F8FEF8D90488143B852E9C8B9865762E69EB
SHA-256:	C0A0A1A3B5D9D4A24330EE668D99DB0D09351A50E7C68760E4625C77797DAAD9
SHA-512:	2968AB179B8C0D85CBEB30939B889BC4837AE3852C1D80BD6812BAE7019ADD31C84051D6062C21E021FC903508D9D6B55F89EDA47F894C004797EF07C938AD6
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>. <head>. <meta charset="utf-8">. <title>Telegram: Contact @corona_impftermine_nue</title>. <meta name="viewport" content="width=device-width, initial-scale=1.0">. .<meta property="og:title" content="Corona Impftermine N.rnberg & Umgebung">.<meta property="og:image" content="https://tttttt.me/cdn4/file/P7FovyAGrMzdIdkvULg3nvuBJd0NxOw5MKIMZjgd-15vXz4c8tE0SMtW6-lkZjh3t1CaK2iDSfOtMHEkqBQxk-XJYUhN1AoQLfF01mAhKO0Mha09VqnQSz0DVeo9mCcvuArQApy0eb5yBzvkzLoYUODdzR5aY5K7oh57418UqcLr7iTUS-h1s7JOWekXo-1nPDqmv9149yH5yiKzR4S2jnPU9a2niPoJO-5_t6SBvxva4E6xvVBqVSDnGW3EtvwIj4KAJWoVB9dSKS06aAPakGQTltMbsuyALIijRMDFL5nj1k7McvdLci3byhS-ilcU5-cnIVY2swjZK2eIRGLsZQ.jpg">.<meta property="og:site_name" content="Telegram">.<meta property="og:description" content="In diesem Channel werden automatisch freie Covid-19 Impftermine im Raum N.rnberg gepostet.">..<meta property="twitter:title" content="Corona Impftermine N.rnberg & Umgebung">.<meta property="twitter:image" cont

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.0816784159115835
Encrypted:	false
SSDEEP:	6:0IFFli+56ZRWHTizlpdAxInVuNijFFli+56ZN7izlpdAxILFJpJNin:jF/iO6ZRoT6pixUEqF/iO6ZN76pixQvK
MD5:	9C9679FCBB922B0C21F98BC20203B3F5
SHA1:	01B69CF7821C2593D00044336000145AAF2D23199
SHA-256:	7A2780E564582B20A74BD95E9DE66D7E88C1CE67021C9F31C130B159730BDB9A
SHA-512:	058C1E5065AA0A4CCE6B13007FB0DC4349640BB7C9B5648FDE6234A78B591B8DD2A7AECA884C509D08CAE614CFB3774D6A16795EB0D28C5174ED13DDC64A728
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\css[1].css	
Preview:	@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.@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\OTUW0Q90\init[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2486
Entropy (8bit):	5.061809620162091
Encrypted:	false
SSDEEP:	48:D03eTUWlHKBBSoGv5qzPzF6Hh9NQSuZVM0hjDqxkzPPorAezflpw721z6U:DMeTUWlOwkzQqzhBDMkjho
MD5:	9AB88387EB3734FF2004580E2089D592
SHA1:	C6019F14655B5A8A594E830619661F6D7A2C9615
SHA-256:	D57457AD6CBB585B9446283DFE53D43FC330EE07EC2DAA6FE39138ADEC5E766B
SHA-512:	C02FA8E25402CC11FFE093B0D6E76ED024E43A1DDF1D754CD483606D0D42D6807D6A6DB12AE1EBD8AA2CB7B382F9D136020082F9F5B6C0DC533CB9949F984 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://widget.stackbit.com/init.js
Preview:	!function(){var t="https://widget.stackbit.com",e="https://app.stackbit.com";function r(t,e){return function(t){if(Array.isArray(t))return t}(t)||function(t,e){var r=[],i=!0,n=!1,c=void 0;try{for(var a,o=t[Symbol.iterator]();!(i=(a=o.next()).done)&&(r.push(a.value),!e||r.length!==e);i=!0);}catch(t){n=!0,c=t}finally{try{i||null==o.return||o.return()}finally{if(n)throw c}}return r}(t,e)||function(){throw new TypeError("Invalid attempt to destructure non-iterable instance")}()}var i,n,c=/[?&](widget|stackbit)(=|&|$)/i.test(location.search),a=/\/admin(?:\/\|$)/i.test(location.pathname),o=!0,s=!1,u=!1;try{s=localStorage.getItem("stackbit-widget.show"),u=sessionStorage.getItem("stackbit-widget.snippet")}catch(t){o=!1,t.toString().includes("SecurityError")&&(u=!0)}if(!a){var l=function(t){var e=t.href,r=t.as,i=document.createElement("link");i.setAttribute("rel","preload"),i.setAttribute("href",e),i.setAttribute("as",r),document.head.appendChild(i)};if(c||s||u){var d=(i=location.search,(n="?"==

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	95786
Entropy (8bit):	5.393689635062045
Encrypted:	false
SSDEEP:	1536:/PEkjP+iADIOr/NEe876nmBu3HvF38sEeLHFoqqhJ7SerN5wVI+xcBmPv7E+nzm6:ENMyqhJvN32cBC7M6Whca98HrB
MD5:	8101D596B2B8FA35FE3A634EA342D7C3
SHA1:	D6C1F41972DE07B09BFA63D2E50F9AB41EC372BD
SHA-256:	540BC6DEC1DD4B92EA4D3FB903F69EABF6D919AFD48F4E312B163C28CFF0F441
SHA-512:	9E1634EB02AB6ACDFD95BF6544EEFA278DFDEC21F55E94522DF2C949FB537A8DFEAB6BCFECF69E6C82C7F53A87F864699CE85F0068EE60C56655339927EEB DB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tlgr.org/js/jquery.min.js
Preview:	/*! jQuery v1.11.1 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l="1.11.1",m=function(a,b){return new m.fn.init(a,b)},n=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,o=/^-ms-/,p=/-([\da-z])/gi,q=function(a,b){return b.toUpperCase()};m.fn=m.prototype={jquery:l,constructor:m,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=m.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return m.each(this,a,b)},map:function(a){return this.pushStack(m.map(this,function(b,c){ret

C:\Users\user\AppData\Local\Temp\~DF5FDD67D587003693.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13173
Entropy (8bit):	0.5756918764000456
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo7L9lo7L9lW7JS/y8wa6g:kBqoI7s7y7e
MD5:	A1A8947B99A7EE27E727C192C4C418B6
SHA1:	2E5B6CE3C45AEA5B4F8556A74C902AA99A720959
SHA-256:	5A38041BEC98BE1C326C9531A6BFB779A165C4533121A4418C9ED131C6B7F81E
SHA-512:	3494299875B35455D8CF337117EAC908CDB97AF86F0BB100518821BDAD4529DBED4EF99B28C891C95FE2E2BB21B8E6DCAC7527B032BC5ABCC6983547E875F1 1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF5FDD67D587003693.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFDFE4C505CF6BDA58.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFF1CF27BECECB5F3A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	93721
Entropy (8bit):	1.2106117259535143
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+2wqDwkk2twxUF9tz5TWid5TWq+hB9rgYK4wdcpEFiEIIxiV9:HUFhTWUTWFp
MD5:	55B4CA4167EF2A175F323F1171EEA42B
SHA1:	B3766D0FCEA6F1FD95447840DFB9A015A98BB89B
SHA-256:	7CAE436A8292E76C73593AD0F740308BF764BC455E46CA5281D1E19E65E35060
SHA-512:	9350CC4B4DDF4C33970F91443989E35C7FF590B340BB28A5DA7BD8245C88B7D6447E3923AC63F4743700E3D055D6C42EEAE366498CC7C236F7902D09796AF4A
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

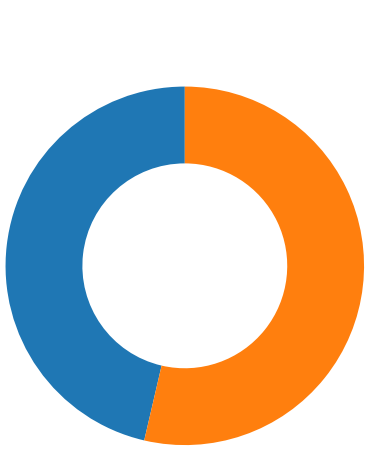
No static file info

Network Behavior

Network Port Distribution

Total Packets: 110

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 25, 2021 09:21:45.074239016 CEST	49714	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.074261904 CEST	49715	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.129518986 CEST	443	49714	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.129667997 CEST	49714	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.129842043 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.129945040 CEST	49715	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.137547970 CEST	49714	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.137744904 CEST	49715	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.192514896 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.192650080 CEST	443	49714	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.193336964 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.193355083 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.193371058 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.193391085 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.193497896 CEST	49715	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.193535089 CEST	49715	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.193578005 CEST	443	49714	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.193595886 CEST	443	49714	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.193624973 CEST	443	49714	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.193643093 CEST	443	49714	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.193661928 CEST	49714	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.193698883 CEST	49714	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.248291969 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.248456001 CEST	49715	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.248872995 CEST	443	49714	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.249006033 CEST	49714	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.292500019 CEST	49714	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.293545008 CEST	49715	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.301156044 CEST	49715	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.301295042 CEST	49714	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.301501989 CEST	49715	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.347776890 CEST	443	49714	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.347928047 CEST	443	49714	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.348043919 CEST	49714	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.348287106 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.348434925 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.348560095 CEST	49715	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.355927944 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.356034040 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.356483936 CEST	443	49714	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.357089996 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.357120037 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.357144117 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.357165098 CEST	443	49715	206.189.50.60	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 25, 2021 09:21:45.357187986 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.357209921 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.357229948 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.357248068 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.357268095 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.357269049 CEST	49715	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.357331991 CEST	49715	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.357438087 CEST	49715	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.358063936 CEST	49715	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.403240919 CEST	443	49714	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.403283119 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.403305054 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.403352976 CEST	49714	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.403425932 CEST	49715	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.404448986 CEST	49714	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.411958933 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.412086964 CEST	49715	443	192.168.2.6	206.189.50.60
May 25, 2021 09:21:45.457592010 CEST	443	49715	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.459521055 CEST	443	49714	206.189.50.60	192.168.2.6
May 25, 2021 09:21:45.587949991 CEST	49717	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.589247942 CEST	49718	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.597342014 CEST	49719	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.597959042 CEST	49720	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.599751949 CEST	49721	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.600162983 CEST	49722	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.629873037 CEST	443	49717	13.225.84.15	192.168.2.6
May 25, 2021 09:21:45.630012035 CEST	49717	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.631046057 CEST	443	49718	13.225.84.15	192.168.2.6
May 25, 2021 09:21:45.631171942 CEST	49718	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.636375904 CEST	49718	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.636708021 CEST	49717	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.641555071 CEST	443	49719	13.225.84.15	192.168.2.6
May 25, 2021 09:21:45.641801119 CEST	49719	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.641823053 CEST	443	49720	13.225.84.15	192.168.2.6
May 25, 2021 09:21:45.641916990 CEST	49720	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.642432928 CEST	443	49721	13.225.84.15	192.168.2.6
May 25, 2021 09:21:45.642455101 CEST	443	49722	13.225.84.15	192.168.2.6
May 25, 2021 09:21:45.642590046 CEST	49721	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.643448114 CEST	49722	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.644246101 CEST	443	49718	13.225.84.15	192.168.2.6
May 25, 2021 09:21:45.644355059 CEST	49718	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.646461964 CEST	49722	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.647588015 CEST	49721	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.648575068 CEST	49720	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.649792910 CEST	49719	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.652585983 CEST	443	49717	13.225.84.15	192.168.2.6
May 25, 2021 09:21:45.652668953 CEST	49717	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.654637098 CEST	443	49719	13.225.84.15	192.168.2.6
May 25, 2021 09:21:45.654745102 CEST	49719	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.655690908 CEST	443	49721	13.225.84.15	192.168.2.6
May 25, 2021 09:21:45.655802011 CEST	49721	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.661803961 CEST	443	49722	13.225.84.15	192.168.2.6
May 25, 2021 09:21:45.661921024 CEST	49722	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.663300991 CEST	443	49720	13.225.84.15	192.168.2.6
May 25, 2021 09:21:45.663400888 CEST	49720	443	192.168.2.6	13.225.84.15
May 25, 2021 09:21:45.678098917 CEST	443	49718	13.225.84.15	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 25, 2021 09:21:35.629494905 CEST	63791	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:35.678775072 CEST	53	63791	8.8.8.8	192.168.2.6
May 25, 2021 09:21:36.432425022 CEST	64267	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:36.481703043 CEST	53	64267	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 25, 2021 09:21:37.328572035 CEST	49448	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:37.335607052 CEST	60342	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:37.378012896 CEST	53	49448	8.8.8.8	192.168.2.6
May 25, 2021 09:21:37.393604994 CEST	53	60342	8.8.8.8	192.168.2.6
May 25, 2021 09:21:38.120249033 CEST	61346	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:38.178586960 CEST	53	61346	8.8.8.8	192.168.2.6
May 25, 2021 09:21:39.144234896 CEST	51774	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:39.194041014 CEST	53	51774	8.8.8.8	192.168.2.6
May 25, 2021 09:21:40.050422907 CEST	56023	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:40.099998951 CEST	53	56023	8.8.8.8	192.168.2.6
May 25, 2021 09:21:40.896075010 CEST	58384	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:40.945414066 CEST	53	58384	8.8.8.8	192.168.2.6
May 25, 2021 09:21:41.912477970 CEST	60261	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:41.962172985 CEST	53	60261	8.8.8.8	192.168.2.6
May 25, 2021 09:21:42.976942062 CEST	56061	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:43.029040098 CEST	53	56061	8.8.8.8	192.168.2.6
May 25, 2021 09:21:43.594777107 CEST	58336	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:43.655184984 CEST	53	58336	8.8.8.8	192.168.2.6
May 25, 2021 09:21:45.001102924 CEST	53781	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:45.060712099 CEST	53	53781	8.8.8.8	192.168.2.6
May 25, 2021 09:21:45.397512913 CEST	54064	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:45.446995974 CEST	53	54064	8.8.8.8	192.168.2.6
May 25, 2021 09:21:45.486617088 CEST	52811	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:45.504591942 CEST	55299	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:45.565640926 CEST	53	52811	8.8.8.8	192.168.2.6
May 25, 2021 09:21:45.567564964 CEST	53	55299	8.8.8.8	192.168.2.6
May 25, 2021 09:21:45.630613089 CEST	63745	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:45.635956049 CEST	50055	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:45.693053007 CEST	53	63745	8.8.8.8	192.168.2.6
May 25, 2021 09:21:45.707531929 CEST	53	50055	8.8.8.8	192.168.2.6
May 25, 2021 09:21:46.118645906 CEST	61374	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:46.170821905 CEST	53	61374	8.8.8.8	192.168.2.6
May 25, 2021 09:21:46.933825970 CEST	50339	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:47.000673056 CEST	53	50339	8.8.8.8	192.168.2.6
May 25, 2021 09:21:47.974956989 CEST	63307	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:48.027700901 CEST	53	63307	8.8.8.8	192.168.2.6
May 25, 2021 09:21:48.747441053 CEST	49694	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:48.809372902 CEST	53	49694	8.8.8.8	192.168.2.6
May 25, 2021 09:21:48.858707905 CEST	54982	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:48.910810947 CEST	53	54982	8.8.8.8	192.168.2.6
May 25, 2021 09:21:49.678946972 CEST	50010	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:49.728255033 CEST	53	50010	8.8.8.8	192.168.2.6
May 25, 2021 09:21:50.963165998 CEST	63718	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:51.012623072 CEST	53	63718	8.8.8.8	192.168.2.6
May 25, 2021 09:21:51.903703928 CEST	62116	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:51.957003117 CEST	53	62116	8.8.8.8	192.168.2.6
May 25, 2021 09:21:53.857933998 CEST	63816	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:53.907470942 CEST	53	63816	8.8.8.8	192.168.2.6
May 25, 2021 09:21:55.244075060 CEST	55014	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:55.293477058 CEST	53	55014	8.8.8.8	192.168.2.6
May 25, 2021 09:21:57.118813992 CEST	62208	53	192.168.2.6	8.8.8.8
May 25, 2021 09:21:57.179486990 CEST	53	62208	8.8.8.8	192.168.2.6
May 25, 2021 09:21:59.996522903 CEST	57574	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:00.046307087 CEST	53	57574	8.8.8.8	192.168.2.6
May 25, 2021 09:22:04.838628054 CEST	51818	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:04.923681974 CEST	53	51818	8.8.8.8	192.168.2.6
May 25, 2021 09:22:12.020553112 CEST	56628	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:12.078429937 CEST	53	56628	8.8.8.8	192.168.2.6
May 25, 2021 09:22:12.331935883 CEST	60778	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:12.345911980 CEST	53799	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:12.392658949 CEST	53	60778	8.8.8.8	192.168.2.6
May 25, 2021 09:22:12.395219088 CEST	53	53799	8.8.8.8	192.168.2.6
May 25, 2021 09:22:13.611701965 CEST	54683	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:13.663867950 CEST	53	54683	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 25, 2021 09:22:13.905747890 CEST	59329	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:13.976392031 CEST	53	59329	8.8.8.8	192.168.2.6
May 25, 2021 09:22:14.426826954 CEST	64021	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:14.484560013 CEST	53	64021	8.8.8.8	192.168.2.6
May 25, 2021 09:22:14.615755081 CEST	54683	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:14.667843103 CEST	53	54683	8.8.8.8	192.168.2.6
May 25, 2021 09:22:15.427423000 CEST	64021	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:15.485166073 CEST	53	64021	8.8.8.8	192.168.2.6
May 25, 2021 09:22:17.707438946 CEST	64021	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:17.757002115 CEST	53	64021	8.8.8.8	192.168.2.6
May 25, 2021 09:22:18.093514919 CEST	54683	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:18.146444082 CEST	53	54683	8.8.8.8	192.168.2.6
May 25, 2021 09:22:18.820594072 CEST	56129	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:18.881208897 CEST	53	56129	8.8.8.8	192.168.2.6
May 25, 2021 09:22:20.057228088 CEST	64021	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:20.106681108 CEST	53	64021	8.8.8.8	192.168.2.6
May 25, 2021 09:22:20.190052986 CEST	54683	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:20.242213964 CEST	53	54683	8.8.8.8	192.168.2.6
May 25, 2021 09:22:20.834638119 CEST	58177	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:20.892623901 CEST	53	58177	8.8.8.8	192.168.2.6
May 25, 2021 09:22:24.074546099 CEST	64021	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:24.123972893 CEST	53	64021	8.8.8.8	192.168.2.6
May 25, 2021 09:22:24.274408102 CEST	54683	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:24.334707975 CEST	53	54683	8.8.8.8	192.168.2.6
May 25, 2021 09:22:46.817934036 CEST	50700	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:46.883546114 CEST	53	50700	8.8.8.8	192.168.2.6
May 25, 2021 09:22:49.288562059 CEST	54069	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:49.342464924 CEST	53	54069	8.8.8.8	192.168.2.6
May 25, 2021 09:22:50.304692984 CEST	61178	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:50.366911888 CEST	53	61178	8.8.8.8	192.168.2.6
May 25, 2021 09:22:50.895220995 CEST	57017	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:50.953078032 CEST	53	57017	8.8.8.8	192.168.2.6
May 25, 2021 09:22:51.909037113 CEST	56327	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:51.967372894 CEST	53	56327	8.8.8.8	192.168.2.6
May 25, 2021 09:22:52.087738037 CEST	50243	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:52.162998915 CEST	53	50243	8.8.8.8	192.168.2.6
May 25, 2021 09:22:52.647075891 CEST	62055	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:52.707968950 CEST	53	62055	8.8.8.8	192.168.2.6
May 25, 2021 09:22:53.162098885 CEST	61249	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:53.220241070 CEST	53	61249	8.8.8.8	192.168.2.6
May 25, 2021 09:22:54.015408039 CEST	65252	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:54.076035976 CEST	53	65252	8.8.8.8	192.168.2.6
May 25, 2021 09:22:54.854970932 CEST	64367	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:54.904314995 CEST	53	64367	8.8.8.8	192.168.2.6
May 25, 2021 09:22:55.608815908 CEST	55066	53	192.168.2.6	8.8.8.8
May 25, 2021 09:22:55.658149004 CEST	53	55066	8.8.8.8	192.168.2.6
May 25, 2021 09:23:13.522038937 CEST	60211	53	192.168.2.6	8.8.8.8
May 25, 2021 09:23:13.581562996 CEST	53	60211	8.8.8.8	192.168.2.6
May 25, 2021 09:23:15.105815887 CEST	56570	53	192.168.2.6	8.8.8.8
May 25, 2021 09:23:15.170505047 CEST	53	56570	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 25, 2021 09:21:45.001102924 CEST	192.168.2.6	8.8.8.8	0x6fb5	Standard query (0)	www.corona-impftermine.net	A (IP address)	IN (0x0001)
May 25, 2021 09:21:45.504591942 CEST	192.168.2.6	8.8.8.8	0x43e8	Standard query (0)	d33wubrfki0l68.cloudfront.net	A (IP address)	IN (0x0001)
May 25, 2021 09:21:45.630613089 CEST	192.168.2.6	8.8.8.8	0xaa9e	Standard query (0)	static.cloudflareinsights.com	A (IP address)	IN (0x0001)
May 25, 2021 09:21:45.635956049 CEST	192.168.2.6	8.8.8.8	0x298	Standard query (0)	widget.stackbit.com	A (IP address)	IN (0x0001)
May 25, 2021 09:21:46.933825970 CEST	192.168.2.6	8.8.8.8	0x7011	Standard query (0)	x1.i.lencr.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 25, 2021 09:21:48.747441053 CEST	192.168.2.6	8.8.8.8	0xbc9	Standard query (0)	cloudflare insights.com	A (IP address)	IN (0x0001)
May 25, 2021 09:22:04.838628054 CEST	192.168.2.6	8.8.8.8	0x389c	Standard query (0)	www.corona-impftermine.net	A (IP address)	IN (0x0001)
May 25, 2021 09:22:12.020553112 CEST	192.168.2.6	8.8.8.8	0x62d9	Standard query (0)	xn--r1a.website	A (IP address)	IN (0x0001)
May 25, 2021 09:22:12.331935883 CEST	192.168.2.6	8.8.8.8	0x2d9b	Standard query (0)	tlgr.org	A (IP address)	IN (0x0001)
May 25, 2021 09:22:12.345911980 CEST	192.168.2.6	8.8.8.8	0xaf76	Standard query (0)	cdn4.telesco.pe	A (IP address)	IN (0x0001)
May 25, 2021 09:22:18.820594072 CEST	192.168.2.6	8.8.8.8	0xe765	Standard query (0)	ttttt.me	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 25, 2021 09:21:45.060712099 CEST	8.8.8.8	192.168.2.6	0x6fb5	No error (0)	www.corona-impftermine.net		206.189.50.60	A (IP address)	IN (0x0001)
May 25, 2021 09:21:45.060712099 CEST	8.8.8.8	192.168.2.6	0x6fb5	No error (0)	www.corona-impftermine.net		3.125.252.47	A (IP address)	IN (0x0001)
May 25, 2021 09:21:45.567564964 CEST	8.8.8.8	192.168.2.6	0x43e8	No error (0)	d33wubrfki0l68.cloudfront.net		13.225.84.15	A (IP address)	IN (0x0001)
May 25, 2021 09:21:45.567564964 CEST	8.8.8.8	192.168.2.6	0x43e8	No error (0)	d33wubrfki0l68.cloudfront.net		13.225.84.180	A (IP address)	IN (0x0001)
May 25, 2021 09:21:45.567564964 CEST	8.8.8.8	192.168.2.6	0x43e8	No error (0)	d33wubrfki0l68.cloudfront.net		13.225.84.188	A (IP address)	IN (0x0001)
May 25, 2021 09:21:45.567564964 CEST	8.8.8.8	192.168.2.6	0x43e8	No error (0)	d33wubrfki0l68.cloudfront.net		13.225.84.170	A (IP address)	IN (0x0001)
May 25, 2021 09:21:45.693053007 CEST	8.8.8.8	192.168.2.6	0xaa9e	No error (0)	static.cloudflareinsights.com		104.16.95.65	A (IP address)	IN (0x0001)
May 25, 2021 09:21:45.693053007 CEST	8.8.8.8	192.168.2.6	0xaa9e	No error (0)	static.cloudflareinsights.com		104.16.94.65	A (IP address)	IN (0x0001)
May 25, 2021 09:21:45.707531929 CEST	8.8.8.8	192.168.2.6	0x298	No error (0)	widget.stackbit.com		3.65.48.84	A (IP address)	IN (0x0001)
May 25, 2021 09:21:45.707531929 CEST	8.8.8.8	192.168.2.6	0x298	No error (0)	widget.stackbit.com		35.234.85.218	A (IP address)	IN (0x0001)
May 25, 2021 09:21:47.000673056 CEST	8.8.8.8	192.168.2.6	0x7011	No error (0)	x1.i.lencr.org	crl.root-x1.letsencrypt.org.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 25, 2021 09:21:48.809372902 CEST	8.8.8.8	192.168.2.6	0xbc9	No error (0)	cloudflare insights.com		104.16.95.65	A (IP address)	IN (0x0001)
May 25, 2021 09:21:48.809372902 CEST	8.8.8.8	192.168.2.6	0xbc9	No error (0)	cloudflare insights.com		104.16.94.65	A (IP address)	IN (0x0001)
May 25, 2021 09:22:04.923681974 CEST	8.8.8.8	192.168.2.6	0x389c	No error (0)	www.corona-impftermine.net		206.189.50.215	A (IP address)	IN (0x0001)
May 25, 2021 09:22:04.923681974 CEST	8.8.8.8	192.168.2.6	0x389c	No error (0)	www.corona-impftermine.net		206.189.50.60	A (IP address)	IN (0x0001)
May 25, 2021 09:22:12.078429937 CEST	8.8.8.8	192.168.2.6	0x62d9	No error (0)	xn--r1a.website		95.216.186.40	A (IP address)	IN (0x0001)
May 25, 2021 09:22:12.392658949 CEST	8.8.8.8	192.168.2.6	0x2d9b	No error (0)	tlgr.org		95.216.186.40	A (IP address)	IN (0x0001)
May 25, 2021 09:22:12.395219088 CEST	8.8.8.8	192.168.2.6	0xaf76	No error (0)	cdn4.telesco.pe		149.154.164.24	A (IP address)	IN (0x0001)
May 25, 2021 09:22:12.395219088 CEST	8.8.8.8	192.168.2.6	0xaf76	No error (0)	cdn4.telesco.pe		149.154.164.25	A (IP address)	IN (0x0001)
May 25, 2021 09:22:12.395219088 CEST	8.8.8.8	192.168.2.6	0xaf76	No error (0)	cdn4.telesco.pe		149.154.165.133	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 25, 2021 09:22:18.881208897 CEST	8.8.8.8	192.168.2.6	0xe765	No error (0)	ttttt.me		95.216.186.40	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 25, 2021 09:21:45.248291969 CEST	206.189.50.60	443	192.168.2.6	49715	CN=*.corona-impftermine.net CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon May 17 21:01:13 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Aug 15 21:01:13 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
May 25, 2021 09:21:45.248872995 CEST	206.189.50.60	443	192.168.2.6	49714	CN=*.corona-impftermine.net CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon May 17 21:01:13 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Aug 15 21:01:13 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
May 25, 2021 09:21:45.681124926 CEST	13.225.84.15	443	192.168.2.6	49718	CN=*.cloudfront.net CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Feb 22 01:00:00 CET 2021 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Tue Feb 22 00:59:59 CET 2022 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 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 Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
May 25, 2021 09:21:45.684366941 CEST	13.225.84.15	443	192.168.2.6	49717	CN=*.cloudfront.net CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Feb 22 01:00:00 CET 2021 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Tue Feb 22 00:59:59 CET 2022 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 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 Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
May 25, 2021 09:21:45.693802118 CEST	13.225.84.15	443	192.168.2.6	49719	CN=*.cloudfront.net CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Feb 22 01:00:00 CET 2021 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Tue Feb 22 00:59:59 CET 2022 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 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 Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
May 25, 2021 09:21:45.695710897 CEST	13.225.84.15	443	192.168.2.6	49722	CN=*.cloudfront.net CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Feb 22 01:00:00 CET 2021 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Tue Feb 22 00:59:59 CET 2022 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
May 25, 2021 09:21:45.697057009 CEST	13.225.84.15	443	192.168.2.6	49721	CN=*.cloudfront.net CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Feb 22 01:00:00 CET 2021 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Tue Feb 22 00:59:59 CET 2022 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 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 Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
May 25, 2021 09:21:45.701704025 CEST	13.225.84.15	443	192.168.2.6	49720	CN=*.cloudfront.net CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Feb 22 01:00:00 CET 2021 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Tue Feb 22 00:59:59 CET 2022 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 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 Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
May 25, 2021 09:21:45.800175905 CEST	3.65.48.84	443	192.168.2.6	49725	CN=*.stackbit.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	Tue May 11 21:32:19 CEST 2021 Fri Sep 04 02:00:00 CEST 2020	Mon Aug 09 21:32:19 CEST 2021 Mon Sep 15 18:00:00 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
May 25, 2021 09:21:45.823700905 CEST	3.65.48.84	443	192.168.2.6	49726	CN=*.stackbit.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	Tue May 11 21:32:19 CEST 2021 Fri Sep 04 02:00:00 CEST 2020	Mon Aug 09 21:32:19 CEST 2021 Mon Sep 15 18:00:00 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=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
May 25, 2021 09:21:45.844474077 CEST	104.16.95.65	443	192.168.2.6	49728	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 11 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sun Jul 11 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
May 25, 2021 09:21:45.844513893 CEST	104.16.95.65	443	192.168.2.6	49727	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 11 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sun Jul 11 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
May 25, 2021 09:21:48.897190094 CEST	104.16.95.65	443	192.168.2.6	49737	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 11 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sun Jul 11 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
May 25, 2021 09:21:48.900343895 CEST	104.16.95.65	443	192.168.2.6	49738	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 11 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sun Jul 11 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 25, 2021 09:22:12.224674940 CEST	95.216.186.40	443	192.168.2.6	49749	CN=xn--r1a.website CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 01 10:37:07 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jul 30 10:37:07 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 25, 2021 09:22:12.227365971 CEST	95.216.186.40	443	192.168.2.6	49748	CN=xn--r1a.website CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 01 10:37:07 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jul 30 10:37:07 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 25, 2021 09:22:12.517381907 CEST	149.154.164.24	443	192.168.2.6	49757	CN=*.telesco.pe, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 10 16:16:32 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Wed Apr 13 19:10:01 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

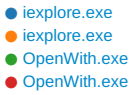
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 25, 2021 09:22:12.517853022 CEST	149.154.164.24	443	192.168.2.6	49756	CN=*.telesco.pe, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 10 16:16:32 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Wed Apr 13 19:10:01 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
May 25, 2021 09:22:12.544326067 CEST	95.216.186.40	443	192.168.2.6	49750	CN=tlgr.org 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 Apr 29 06:36:18 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jul 28 06:36:18 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 25, 2021 09:22:12.546200037 CEST	95.216.186.40	443	192.168.2.6	49752	CN=tlgr.org 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 Apr 29 06:36:18 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jul 28 06:36:18 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 25, 2021 09:22:12.546382904 CEST	95.216.186.40	443	192.168.2.6	49753	CN=tlgr.org 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 Apr 29 06:36:18 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jul 28 06:36:18 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 25, 2021 09:22:12.549227953 CEST	95.216.186.40	443	192.168.2.6	49751	CN=tlgr.org 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 Apr 29 06:36:18 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jul 28 06:36:18 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 25, 2021 09:22:12.551455021 CEST	95.216.186.40	443	192.168.2.6	49754	CN=tlgr.org 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 Apr 29 06:36:18 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jul 28 06:36:18 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 25, 2021 09:22:12.553371906 CEST	95.216.186.40	443	192.168.2.6	49755	CN=tlgr.org 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 Apr 29 06:36:18 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jul 28 06:36:18 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 25, 2021 09:22:20.260885000 CEST	95.216.186.40	443	192.168.2.6	49762	CN=ttttttt.me CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 01 10:37:14 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jul 30 10:37:14 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 25, 2021 09:22:20.268465042 CEST	95.216.186.40	443	192.168.2.6	49761	CN=ttttttt.me CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 01 10:37:14 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jul 30 10:37:14 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		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5792 Parent PID: 792

General

Start time:	09:21:42
Start date:	25/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5100 Parent PID: 5792

General

Start time:	09:21:43
Start date:	25/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5792 CREDAT:17410 /prefetch:2
Imagebase:	0x40000
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

Analysis Process: OpenWith.exe PID: 6164 Parent PID: 792

General

Start time:	09:22:41
Start date:	25/05/2021
Path:	C:\Windows\System32\OpenWith.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\OpenWith.exe -Embedding
Imagebase:	0x7ff78eda0000
File size:	111120 bytes
MD5 hash:	D179D03728E95E040A889F760C1FC402
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	Completion	Count	Source Address	Symbol

Analysis Process: OpenWith.exe PID: 7060 Parent PID: 792

General

Start time:	09:23:24
Start date:	25/05/2021
Path:	C:\Windows\System32\OpenWith.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\OpenWith.exe -Embedding
Imagebase:	0x7ff78eda0000
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