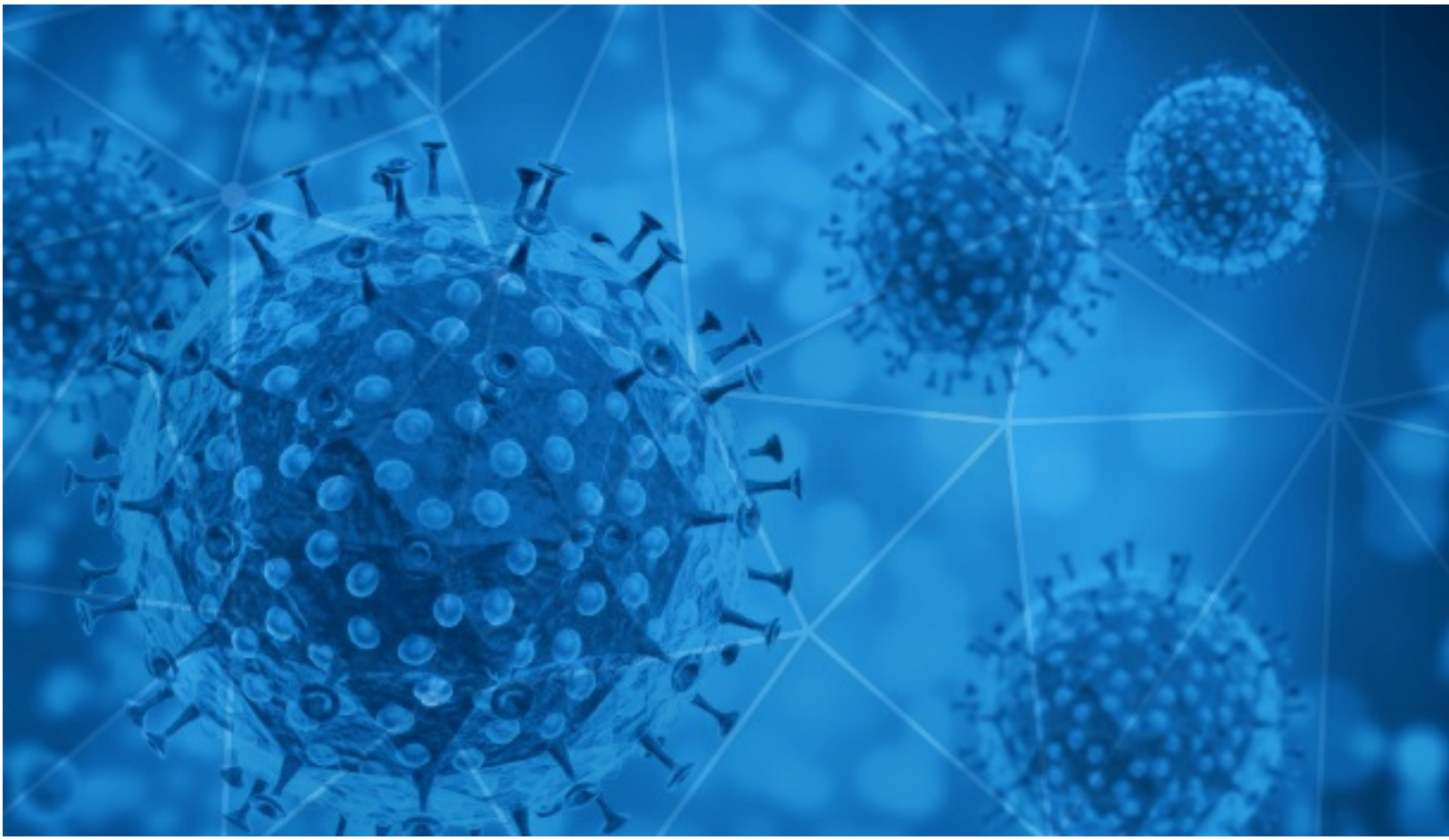
RiskIQ i3:

Finished Intelligence Indicator of Compromise (IOC) COVID-19 Report

2020-08-17



RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

Methodology

The information provided in this report is limited to open source and publicly available data discovered through standard, commonly known browsing techniques and keyword searches. To provide efficient results, RiskIQ may use websites that require payment in exchange for aggregation of data that is otherwise publicly available without payment and could be obtained by anyone accessing the correct sites or engaging the correct third parties to obtain the information. Information presented in this report is cross-checked against multiple sources for full verification; however, some assessments and conclusions are based on incomplete information and represent the RiskIQ analyst's judgment based on patterns and data available.

Disclaimer

The information provided in this report is "AS-IS" and Customer acknowledges and agrees that RiskIQ makes no representation or warranty, express or implied, as to the accuracy or completeness of the information. The customer agrees that RiskIQ shall not have any liability resulting from their use of this information.

Notice

As of 05/15/2020 RiskIQ changed the format and frequency of the COVID-19 Daily Update. Each Friday, RiskIQ will compile the week's major stories in the Notable Events, Facts and Figures at a Glance, Stay-At-Home/Shelter-In-Place Orders, and Governmental Guidance sections of the report.

The Digital Exploitation data will continue to be delivered daily with the COVID-19 Email Spam Statistics, COVID-19 Host, Domain, and Mobile App Tracking, and COVID-themed Blacklisted Domains included.

RiskIQ has established a microsite for COVID-19 coverage, located at https://www.riskiq.com/covid19-cybersecurity/.

Thank you for your continued readership!

Daily Blacklisted Hosts Feed

RiskIQ is making a blacklisted host feed from its COVID-themed scanning available to the public. Blacklisted hosts listed in the feed have been observed serving scammy/fraudulent content, phish, malware, or malicious code. This data is delivered "AS-IS".

https://covid-public-domains.s3-us-west-1.amazonaws.com/covid19_blacklist.html

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 2020-08-16 to 2020-08-17. During this period, RiskIQ analyzed 61,698 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,265 unique subject lines observed during the reporting period. The spam emails originated from 733 unique sending email domains and 2,422 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	23610
Insumos para Contingencia ANTI COVID-19	3160
The Corona Letter: Couples are postponing baby plans	2293
Charter Air Service/Fast Air service/Mask /Covid-19 test/Medical equipment	1887
Will COVID-19 Impact Your Credit Scores?	1792
COVID-19 And Your Credit Health	1760
Protect Scores During Coronavirus	1700
Help the world's response to Covid-19 with the most protective mask on the market.	1472
Wearing a KN95 mask is your best defense against coronavirus	1356
e-Conference on Accelerating New Business Model In Covid-19-Innovate,Transform and Grow	1220
Re: Maslahat Mutual Capital Relief (COVID-19).	1106
Desinfeccion Preventiva Covid19	943
Desinfeccion covid19 mediante termoniebla	913
Desinfectamos su ambiente de coronavirus	892
COVID-19 Compensation/Relief Funds.	871
Cuidate del COVID19 con nuestros productos	684
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	661
Your appointment for Covid Antibody IgG test is fixed at Rs 600 only.	607
RE :Covid-19 / Vanity upon Vanity (Covid-19 is real. Stay Safe!)	594
e-Conference on Accelerating New Business Model in Covid-19-Innovate,Transform and Grow	529
Soluciones para la prevencion del covid19	511
Re: Protective products related to COVID-19.	506
Como volver a la actividad post coronavirus?	468
Cabinas para la prevencion del coronavirus?	454
COVID-19 - Send Requirements + SEO (Results Guaranteed) [REDACTED_DOMAIN]	407

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

toyotacarrr.com	23611
countermail.com	4181
trendingtopic.cl	3348
vadencene.casa	2754
vadencene.cyou	2499
newgcmfordeventdel.in.net	2390
timesofindia.com	2293
126.com	1922
oceanbridgecargo.com	1888
gmail.com	1792

Top-15 IPs Sending COVID Spam

201.231.83.149	3702
23.231.110.239	2748
23.231.110.240	2499
203.86.233.195	1887
23.231.110.225	1505
23.231.110.226	1320
51.77.33.44	1221
51.77.33.43	1003
201.231.8.36	941
51.38.159.218	895

Top-15 Countries Sending COVID Spam

JP	23802
US	14385
AR	4971
FR	3624
CN	3234
IN	2978
HK	1934
PH	1107
CA	1054
--	702

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

ANC Weekly COVID-19 Reports	21
Covid-19 compensation fund	6
COVID-19 RELIEF FUNDING	4
Covid-19 compensation fund	3
COVID-19 Bhutanese respond survey	2
Y también les envío un video con una poesía rimada e ilustrada sobre el coronavirus para l@s más peques	2
Line List Form COVID-19 (1) 8-15	1
Carta Solicita Atención Oportuna Apoyo COVID 19	1
PLANEACIONES COVID PANORAMA	1
MESURES COVID MEMO 1	1

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

COVID-19 Host, Domain, and Mobile App Tracking

RiskIQ gathers data relating to newly-observed hosts and domains containing COVID-19, COVID19, or Coronavirus in the host or domain name, and mobile apps containing COVID-19, COVID19, or Coronavirus in the title or description. A summary of data collected is contained in this section.

Domain Stats

Domains: 119,670
Domains with Potential Mail Servers: 2,892
Email-Capable Domains and Hosts: 44,301
Live Hosts and Domains Not Parked: 69,451

Mobile Apps

Apps in Official Stores: 391

by Store

Apple	204
Google	177
WindowsPhone	9
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,122

by Store Type:

Hybrid	691
Secondary	384
Affiliate	47

Blacklisted Mobile Apps: 26

by Store Type:

Secondary	23
Official	2
Hybrid	1