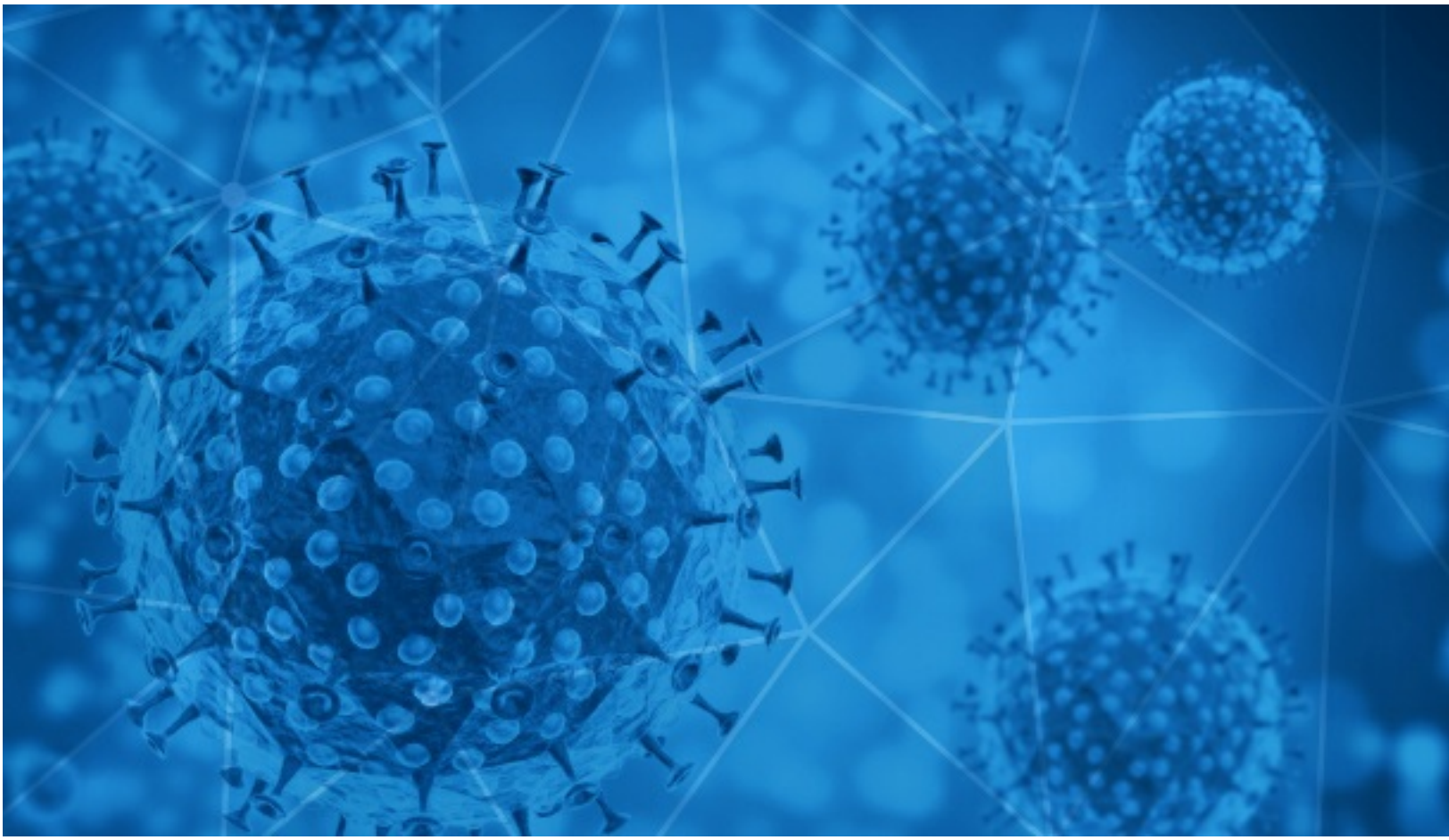
RISKIQ®

RiskIQ i3:

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

2020-08-03



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 2020-08-02 to 2020-08-03. During this period, RiskIQ analyzed 16,950 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,298 unique subject lines observed during the reporting period. The spam emails originated from 628 unique sending email domains and 2,462 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Study on transmission on a train	2290
Collect Your $500 Covid-19 check inside	1009
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	844
PyMEs contra el COVID19	720
Boost your internet speeds while you're quarantined from the CoronaVirus	502
Glimpses of our various COVID-19 relief activities	432
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	429
BEST way to manifest money in a post-corona world	408
Secret Corona Cash Manifestation Formula	382
RE: COVID 19 RELIEF FUND CLAIMS PROCEDURE/	378
COVID-19 EMERGENCY DELIVERY OF YOUR CONSIGNMENT BOX TODAY.	359
Re: keep away from Covid-19	342
COVID-19 Lastest News	300
Let’s fight together to get through the COVID-19	205
□ Corona-Leitfaden für den Tourismus, Voting der 100 BEST CHEFS Germany und vieles mehr	204
Hittegolf in aantocht - Op stap in dé Vlaamse corona-broeihaard - Twee meisjes aangerand op Lijnbus	203
Re:□coronavirus civil mask / Chinese qualified manufacturer	191
Proteção do COVID-19	172
Re: Hay que adaptarse a la nueva situacion Covid-19	170
Re: Estamos adaptados a la nueva situacion Covid-19	161
Receive Share With Your Community because of covid-19 favour From W.H.C.O	159
Re: Adaptados a la nueva situacion Covid-19	149
Re: Surgical & Medical Mask for Coronaviruse / China Qualified	147
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	146
Re: Nos adaptamos a la nueva situacion Covid-19	140

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	2299
gmail.com	1974
126.com	1509
marktplace.icu	1009
manifmagics.com	790
countermail.com	720
163.com	597
muthootgroup.com	432
yahoo.com	396
studyrailroad.xyz	327

Top-15 IPs Sending COVID Spam

181.46.136.168	844
69.94.156.10	790
139.59.86.103	432
177.53.146.10	378
45.136.7.54	327
201.231.6.121	311
223.38.18.184	303
113.77.146.252	270
201.231.19.3	212
80.98.112.214	209

Top-15 Countries Sending COVID Spam

US	3135
IN	2854
CN	2519
AR	1599
FR	1349
DE	1308
--	584
BR	439
BE	404
KR	401

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	17
Informe Epidemiológico Coronavírus 02/8/2020	4
COVID Update August 2	2
PARTE COVID-19 DEL 02AGO2020 EESTP PNP TRUJILLO	2
Safety, Security at Work Training(Post Covid 19 Preparedness Course)	2
Un artículo sobre Covid y totalitarismo	2
COVID 19 Update - 2nd Aug	2
Test Result of COVID 19 on 02.08.2020 at MMC	1
COVID Authorised Absence Form JULY 2020W	1
RV: Las Mascaras transparentes faciales como un eficaz protector al contagio de Covid -19 (29 de abril de 2020. doi: 10.1001 / JAMA.2020.7477)	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: 117,641
Domains with Potential Mail Servers: 2,860
Email-Capable Domains and Hosts: 44,340
Live Hosts and Domains Not Parked: 66,989

Mobile Apps

Apps in Official Stores: 368

by Store

Apple	195
Google	164
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 944

by Store Type:

Hybrid	607
Secondary	297
Affiliate	40

Blacklisted Mobile Apps: 23

by Store Type:

Secondary	20
Official	2
Hybrid	1