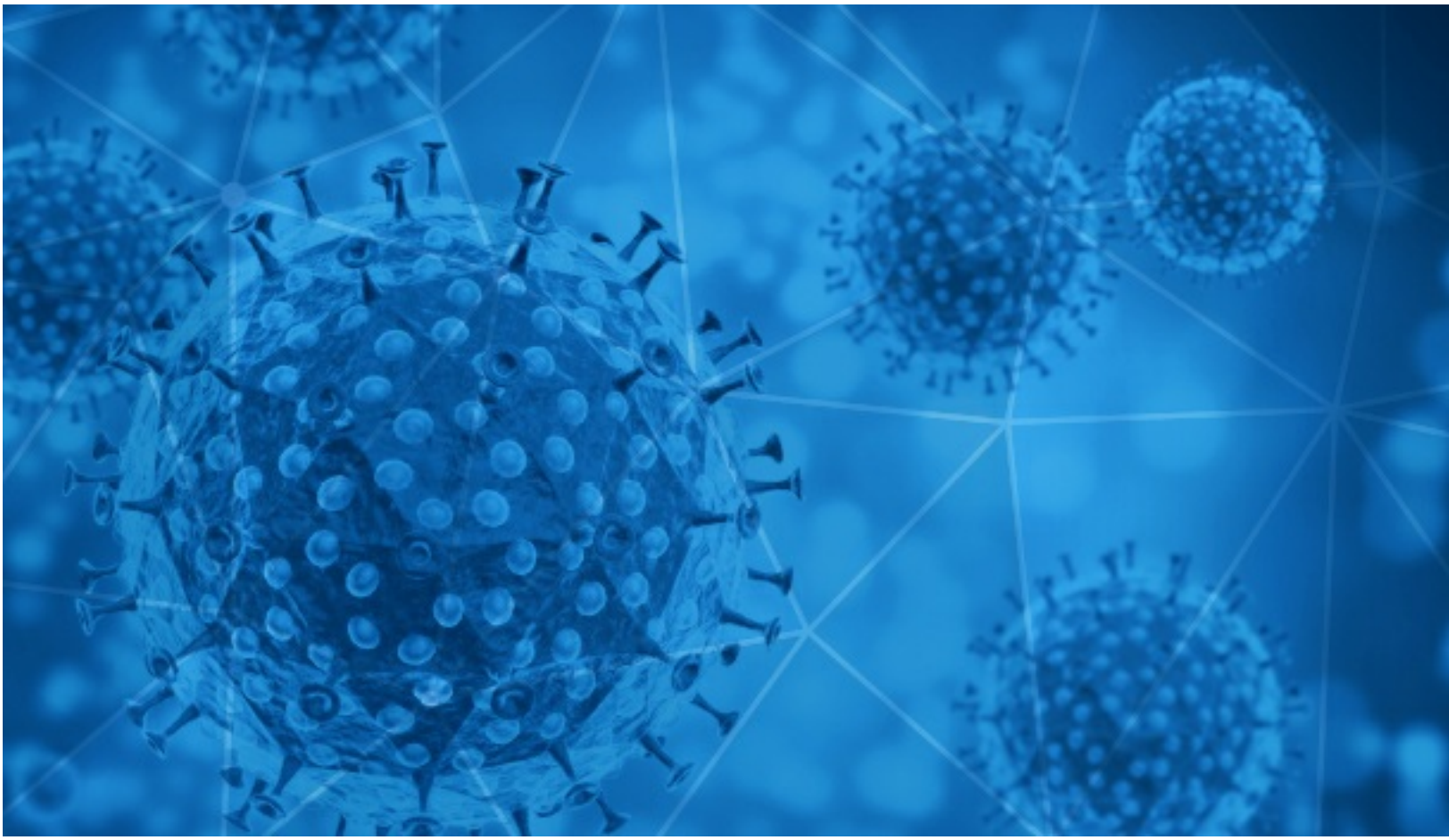
RISKIQ®

RiskIQ i3:

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

2020-07-20



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 2020-07-19 to 2020-07-20. During this period, RiskIQ analyzed 39,020 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,795 unique subject lines observed during the reporting period. The spam emails originated from 9,242 unique sending email domains and 2,028 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

Worried about your bills due to COVID-19?	14742
We Produce Covid-19 (Face Mask,Isolation Gown,Head/Shoe/Sleeve Cover,Vinyl Gloves ,PE Gloves,Apron)	4485
Re: COVID-19 Give away	3098
The Corona Letter: Localised lockdown, national impact	2143
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	672
Re: How do we purchase after the COVID-19?	557
Cabinas para la prevencion del coronavirus?	550
Soluciones para la prevencion del covid19	522
Como volver a la actividad post coronavirus?	494
Test Rapido Covid 10.000 CLP	477
COVID-19 - Projects | Website | Mobile Application | E-Commerce | SEO (Results Guaranteed) [REDACTED_DOMAIN]	472
COVID-19 - Web Maintenance / PHP, Magento, Drupal, E-Commerce / SEO (100%!R(MISSING)esults Guaranteed) [REDACTED_DOMAIN]	432
Second Wave of Covid-19	357
COVID-19 - Web Maintenance / PHP, Magento, Drupal, E-Commerce / SEO (100% Results Guaranteed) [REDACTED_DOMAIN]	341
Re: BT earbuds/ How do we purchase after the COVID-19?	340
Re: BT earbuds/ How to do the purchase after COVID-19?	325
COVID-19 FINANCIAL UPDATE	260
Chinese protective products of COVID-19	243
My COVID-19 Donation	232
COVID-19 Chinese protective products	229
China Supply Chain of COVID-19	224
(COVID19)PANDEMIC !!!	216
Register Now | Being Productive in The Age of New Normal Amid COVID-19	204
Features: Lessons from Elders; Rethinking Life Purpose?; Caretaker's Financial Guide; Your Covid Go-Bag	183
Let’s fight together to get through the COVID-19	180

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

protonmail.com	4485
gmail.com	3310
onet.eu	3098
163.com	2416
timesofindia.com	2145
countermail.com	1726
timesjobs.com	772
trendingtopic.cl	548
126.com	355
crestinvestingcapitals.com	275

Top-15 IPs Sending COVID Spam

216.223.71.246	4485
103.141.137.241	3098
113.116.70.198	782
223.73.108.112	696
181.46.136.165	672
190.247.227.27	639
157.119.122.139	518
190.247.241.46	488
201.231.83.82	460
113.118.93.152	440

Top-15 Countries Sending COVID Spam

US	7673
CA	4560
IN	4362
AU	3496
--	3265
BR	3034
CN	3014
AR	2415
JP	2344
FR	1283

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	22
COVID-19 RELIEF FUNDING	3
COVID -19 DUTY SCHEDULE OF DNB/CPS RESIDENTS	2
PARTE COVID-19 DEL 19JULIO2020 EESTP PNP TRUJILLO	2
White Paper Commentary on a Solution to the Shortages of Proper Respiratory Protection in the Coronavirus Crisis	1
RV: Reenviar: PLAN PARA LA VIGILANCIA, PREVENCION Y CONTROL DE COVID-19 EN EL TRABAJO	1
Here is the info on COVID for course	1
MIDWEEK COVID-19 17-07-2020.docx_ (003).docx	1
IMPORTANT TO READ THIS! Unity Group COVID 19 Milestone and School Reopening	1
CONSOLIDADO DE LLAMADA CASO COVID-19	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: 115,274
Domains with Potential Mail Servers: 2,824
Email-Capable Domains and Hosts: 43,594
Live Hosts and Domains Not Parked: 65,049

Mobile Apps

Apps in Official Stores: 349

by Store

Apple	187
Google	153
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 900

by Store Type:

Hybrid	573
Secondary	289
Affiliate	38

Blacklisted Mobile Apps: 22

by Store Type:

Secondary	19
Official	2
Hybrid	1