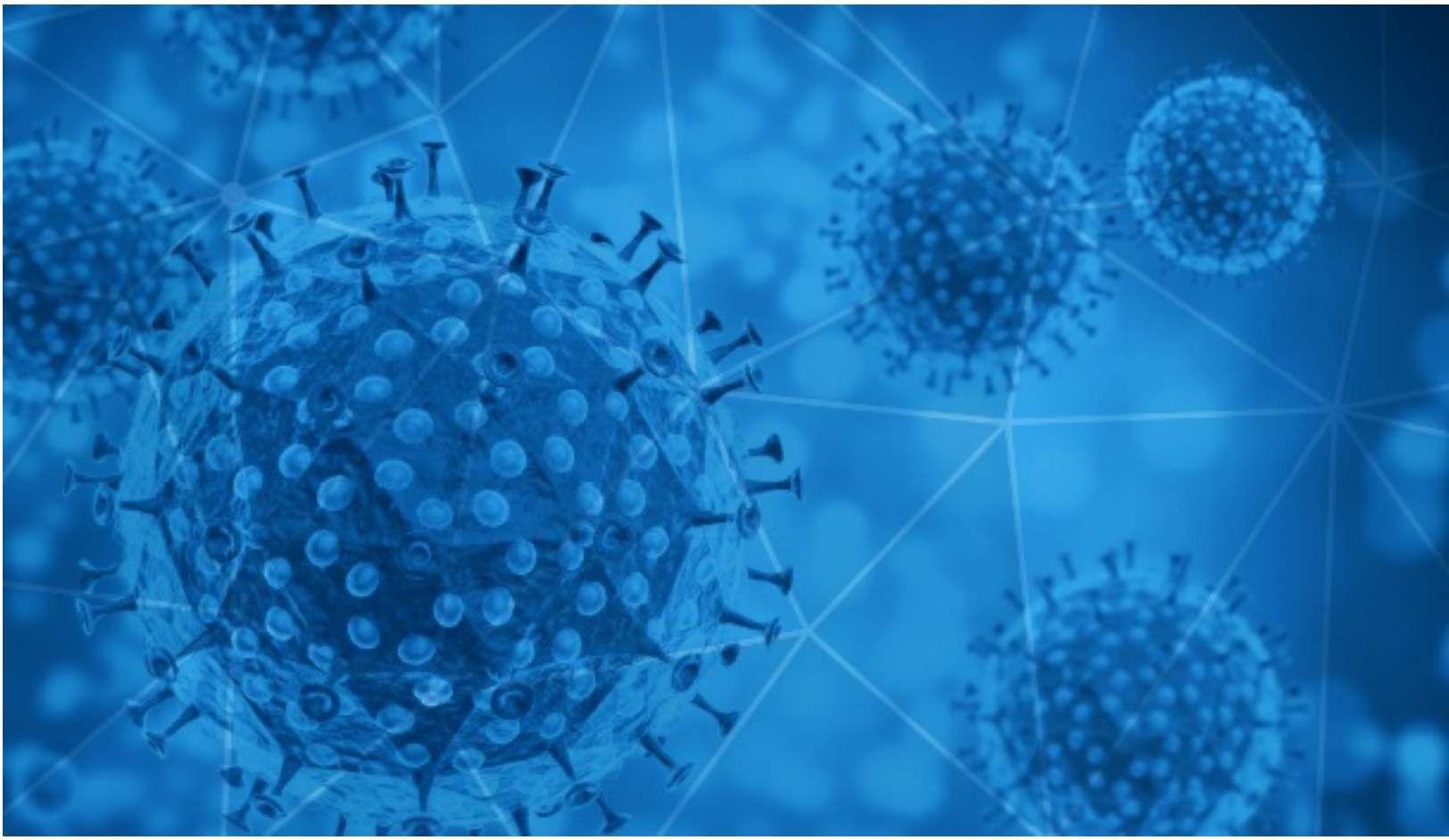
RiskIQ i3:

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

2020-07-07



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 2020-07-06 to 2020-07-07. During this period, RiskIQ analyzed 35,288 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,608 unique subject lines observed during the reporting period. The spam emails originated from 2,515 unique sending email domains and 4,267 unique SMTP IP Addresses. Analysts identified 2 emails which sent an executable file for Windows machines.

Top-25 Subjects

TIMES TOP10: India now third worst Covid hit nation	3367
{COVID-19} □□□□□□□□□□□□□□□□□	3330
The Corona Letter: An epidemic of plastics	1740
Kit test covid - Aprovechalo desde 5490	1577
re: Test Rapido de Diagnostico COVID-19	1130
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	1062
Corona-Finanz-Check	874
We Produce Covid-19 (Face Mask,Isolation Gown,Head/Shoe/Sleeve Cover,Vinyl Gloves ,PE Gloves,Apron)	619
Activos Fijos - Tratamiento Contable y Tributario en Tiempos de COVID-19	568
RE: COVID-19!!!	540
COVID-19 - Mobile App Development/ PHP, Magento, Drupal, E-Commerce -etc [REDACTED_DOMAIN]	534
High-quality Disposable Medical Kit, which are reliable products protecting from COVID-19	507
RE: COVID-19.	451
COVID-19 - Mobile App Development/ PHP, Magento, Drupal, E-Commerce -etc - [REDACTED_DOMAIN]	448
COVID-19 - Custom Projects | Mobile Application | SEO !! -etc [REDACTED_DOMAIN]	417
Productos Prevención Covid-19	354
MASCARA DE PROTECCION COVID-19	347
COVID protective gear in stock!	343
Ofertas COVID -19	314
Test Rapido Covid 10.000 CLP	309
Korea Trend News-COVID19(4)	287
COVID-19 - Mobile App Development/ PHP, Magento, Drupal, E-Commerce -etc texelglobal.com	282
Implacable contra el COVID-19 AMONIOX	264
PyMEs contra el COVID19	263
Earn extra income in this Covid-19	235

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmail.com	4746
bounce.indiatimes.com	3367
toyotacarrr.com	3331
timesofindia.com	1740
brandmed.cl	1590
126.com	1430
googlemail.com	991
flixkredit.de	874
countermail.com	680
protonmail.com	619

Top-15 IPs Sending COVID Spam

119.122.91.254	1062
133.223.65.52	990
200.112.32.34	900
46.228.192.33	874
5.56.22.142	819
5.56.22.141	769
82.70.113.62	619
157.119.122.137	614
157.119.122.134	580
190.210.162.21	346

Top-15 Countries Sending COVID Spam

IN	7407
US	7390
JP	4703
DE	3249
CN	2210
CL	1341
GB	1284
AR	1150
FR	945
RU	577

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

METERIALS EQUIPMENT NEEDED/COVID	1
COTA Survey - Coronavirus - checking in on the older person's experience - please support & circulate to communities	1

Top-15 Subjects Containing doc/xlsx Files

IMPORTANT : post-coronavirus	15
Covid-19 compensation fund	4
Investment of 16 million euros for growth post Corona: Ziehl-Abegg expands production for energy-saving fans in Kupferzell	3
IMPOERTANT : post-coronavirus	3
Excel training & Coping with COVID19 today & tomorrow webinar	3
Quick Survey Bank Indonesia -- Dampak COVID-19	2
Szczepienia a COVID-19_Wywiad z dr hab. E. Augustynowicz	2
COVID-19ari aurre egiteko jarduera ekonomikoentzako dirulaguntzak - Subveciones de actividades económicas para hacer frente al COVID-19	2
Invite: CII Session on "Tracking the Impact of COVID- 19 On Consumer Mind Set" on 10th July 2020,1600-1800 Hrs.	2
RE: PLANO DE TRABALHO COVID 19.xlsx	2

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: 112,108
Domains with Potential Mail Servers: 2,766
Email-Capable Domains and Hosts: 42,476
Live Hosts and Domains Not Parked: 54,311

Mobile Apps

Apps in Official Stores: 316

by Store

Apple	174
Google	133
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 848

by Store Type:

Hybrid	531
Secondary	281
Affiliate	36

Blacklisted Mobile Apps: 21

by Store Type:

Secondary	19
Hybrid	1
Official	1