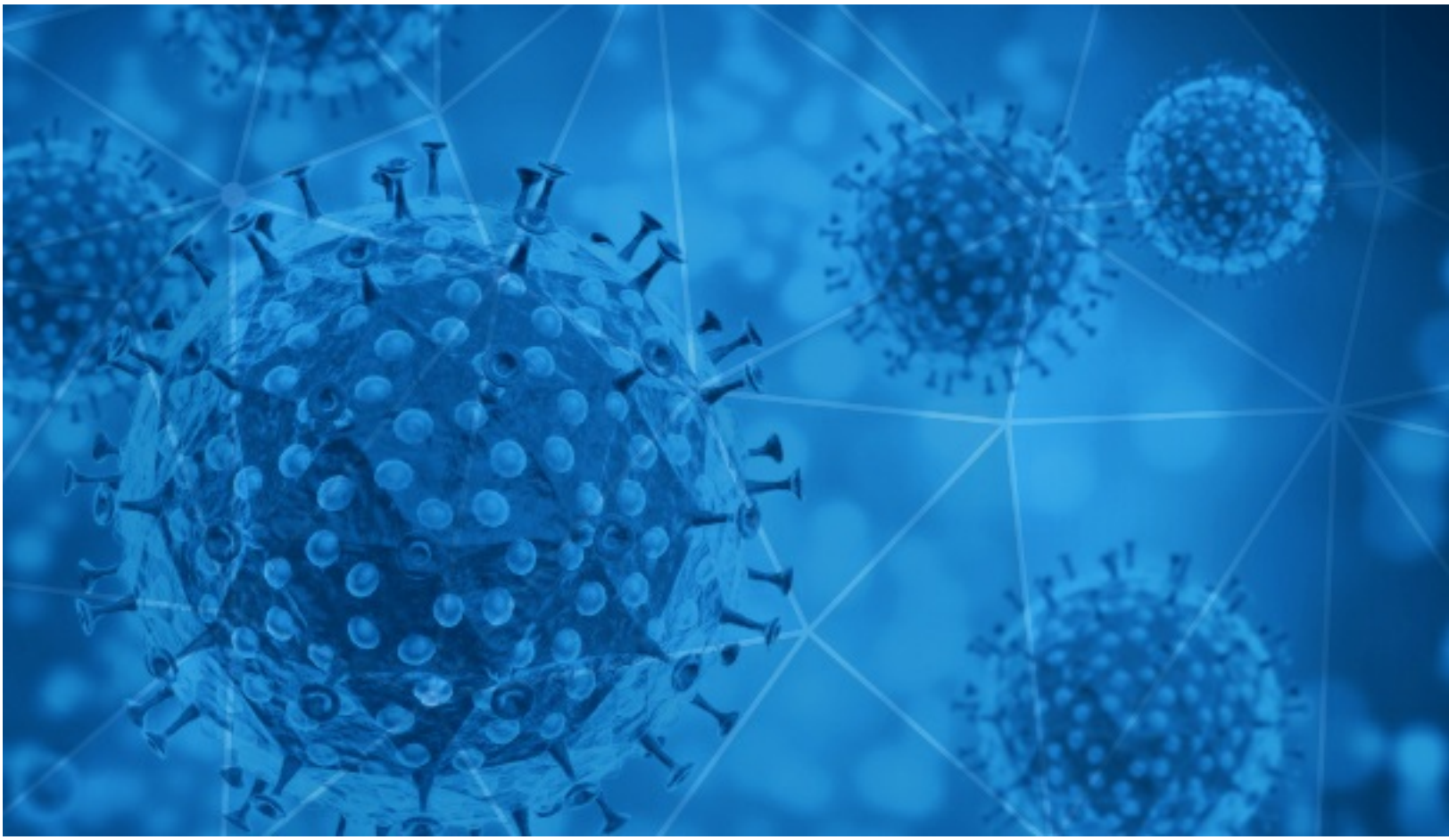
RiskIQ i3:

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

2021-02-25



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 2021-02-24 to 2021-02-25. During this period, RiskIQ analyzed 40,938 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,348 unique subject lines observed during the reporting period. The spam emails originated from 2,137 unique sending email domains and 3,877 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	13421
The Corona Letter: When tech is a hindrance	3810
New Corona-virus Mask!	1743
Traveling soon, wear this mask to fight chances of getting Corona-virus	1675
Get your Corona-virus Mask while supplies last!	1636
Reduce your risk of Corona-virus with this Mask	1591
my COVID-19 support loan at 3%	1154
(□□) 3□ 30□ □□□, "□4□ AI □□□ □□□□ □□□□ 2021: Post Corona, AI Contact Center in Life" □□ □□	480
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO ANTE EL COVID19	467
Daily Covid Questionnaire	451
my COVID-19 support loan at 3%!	426
Línea de prendas médicas anti covid, especialmente fabricadas para sentirse cómodo todo el día.	337
Re: Corona virus Protection Pills.Order confirmation	328
The Morning: ‘Covid zero’ isn’t happening	322
Re: Supply Medical supplies for Coronavirus	320
Covid-19 Aftermath	310
¡No dejemos de cuidarnos, Pruebas de detección Covid-19! | CLÍNICA SANENS	306
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	295
Equipos de limpieza, esterilización y desinfección de ambientes, elimina Covid, Bacterias, Moho, mal olor etc.	261
NCJ Daily - Humboldt's 33rd COVID Death. County Enters Red Tier. Largest Fraud Investigation in CA History.	243
Re: Personal, SME & Business Relief [COVID-19]	220
Re: Personal, SME & Business Relief (COVID-19)	204
What? The NBA Is Going To Be Using COVID Dogs?	191
COVID-19: Employer support – live webinars	178
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	176

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

giant-pw.com	13423
clrvisor.org	6645
timesofindia.com	3819
gmail.com	2914
163.com	554
millburn.org	510
etnews.com	480
nytimes.com	442
cmbmutualfunds.com	424
gajtek.com	328

Top-15 IPs Sending COVID Spam

63.81.84.59	6644
60.249.145.10	1576
103.225.53.107	685
103.225.55.96	557
181.46.136.168	467
103.225.55.76	454
103.225.55.83	376
103.225.55.163	349
103.225.53.140	346
67.219.150.138	328

Top-15 Countries Sending COVID Spam

US	14056
JP	13622
IN	4359
TW	1585
CN	682
KR	648
PE	608
AR	593
DE	511
FR	451

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

UN Covid 19 Relief fund	10
UN Covid 19 Relief fund.	4
comunicato stampa_ Bioarginina® controlla lo sviluppo dei danni endoteliali da COVID: Studio con Bioarginina® (EV & OS) nei pazienti COVID	3
COVID-19 Vaccine Update: J&J vaccine, allocations, educational opportunities, out-of-state vaccination	2
Fwd: triển khai cài đặt và sử dụng ứng dụng "An toàn COVID-19" trong trường học.	2
Міжнародний форум «Тренди медіа та тенденції реалізації Цілей сталого розвитку ООН в епоху пост COVID-19» відбувся за участі 10 країн. Прес-реліз, фото, відео	2
CCS/11470 Pide Salud a población urbana no acudir a zonas serranas para vacunación contra COVID-19	2
NP INDRA PERDIÓ 65 MILLONES DE EUROS EN 2020, IMPACTADA POR EL COVID, PESE A QUE AUMENTÓ SU CARTERA UN 16% Y REDUJO SU DEUDA AL MÍNIMO DE DIEZ AÑOS	2
Moderna COVID Vaccine Dose 2 Events	2
RV: RESUMEN VACUNACION COVID- PERSONAL DE SALUD MICRORED PEDREGAL- LA JOYA	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: 147,281
Domains with Potential Mail Servers: 2,561
Email-Capable Domains and Hosts: 53,708
Live Hosts and Domains Not Parked: 45,136

Mobile Apps

Apps in Official Stores: 515

by Store

Apple	255
Google	243
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,125

by Store Type:

Hybrid	1078
Secondary	979
Affiliate	68

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	26
Official	2
Hybrid	1