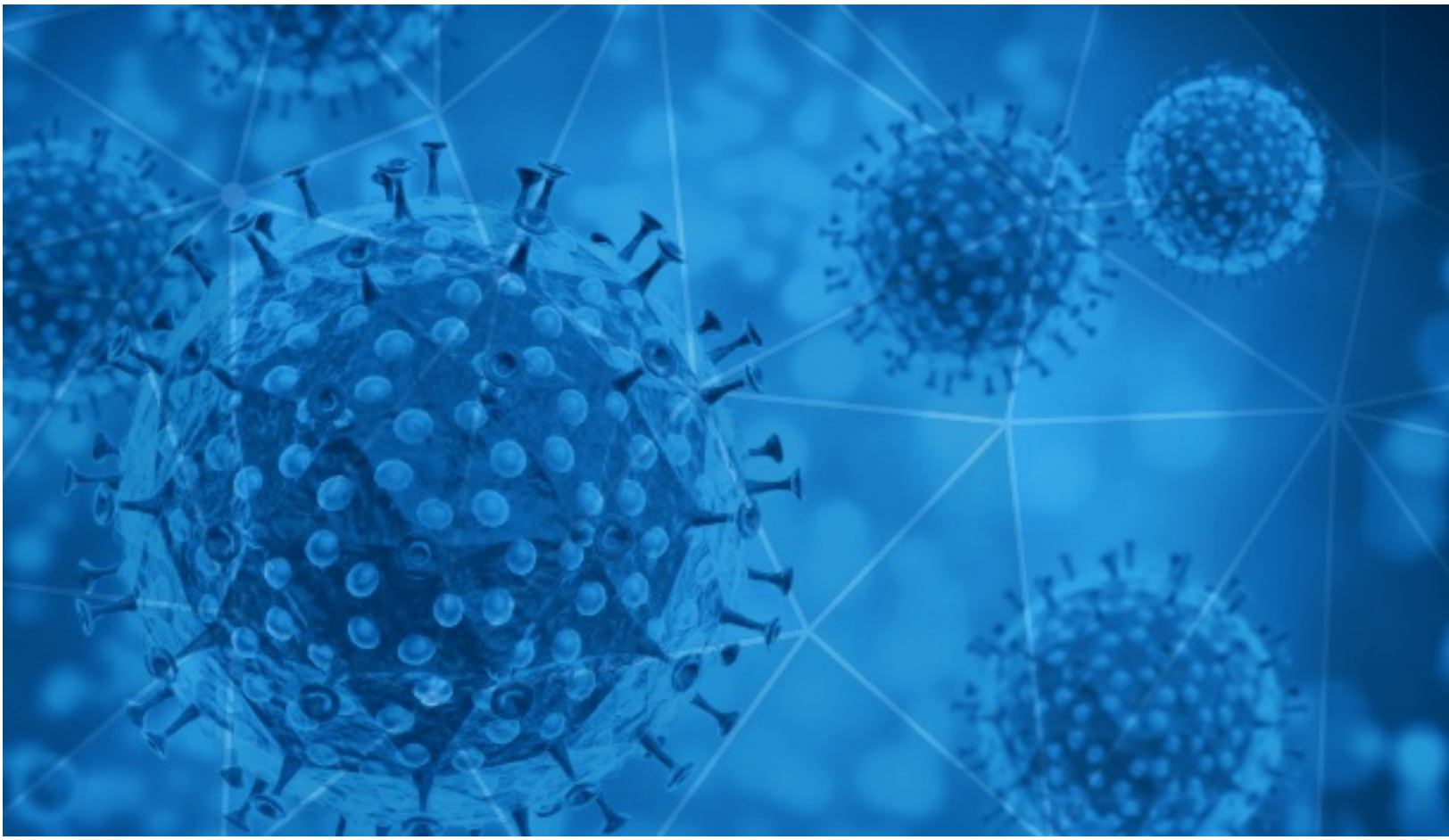
RiskIQ i3:

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

2021-03-16



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 2021-03-15 to 2021-03-16. During this period, RiskIQ analyzed 38,258 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,132 unique subject lines observed during the reporting period. The spam emails originated from 2,169 unique sending email domains and 3,962 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

Coronaschutzmasken 0,06 Euro (Schwarz, Rosa, Blau)	6149
[UK 000] The evil covid-19 seems in retreat Now is time to train your people!	5396
Sehr preiswert: Coronaschutzmasken 6 Cent (Schwarz, Rosa, Blau)	3702
The Corona Letter: AstraZeneca denies blood clot risk from vaccine	3443
[USA L01] WITH COVID-19 ON RETREAT- who should you train for leadership?	1301
COVID-19 PANDEMIC COMPENSATION FUND	1106
ATTN Beneficiary(COVID-19 pandemic Essential Worker Support Program (EWSP) WorldWide.	810
disponibili Kit di "test salivare" rapido screening covid nella tua azienda	646
COVID19 spot check	473
[L07] The world is recovering from covid-19 it is time to TRAIN your best people!	360
EEOC & CDC Guidance for Employers Mandating COVID Vaccines at Work	357
Google Alert - "You need this right nowfor fight Covid and Fun"	330
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove...etc.	319
Re: Digital signage solution for Covid-19	315
COVID-19 Update: We are open and now offering Free Virtual Consultations	281
Adhesivos Distanciamiento Social Covid-19	280
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	274
Dealing with a Covid-19 related loss.	224
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	220
Paneles de protección anti COVID-19	217
Descarte de Covid-19. Pruebas moleculares, antígeno y anticuerpos. publicidad	213
Trump says we should thank him for covid response (not kidding)	207
EEOC Guidance 2021 for Employers Mandating COVID Vaccines at Work	206
UNITED NATIONS COMPENSATION&COVID19 ASSISTED PROGRAM	203
Covid-19 deja secuelas emocionales diversas y Ãºnicas en cada individuo	185

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmx.net	9852
bizuk01.com	5416
timesofindia.com	3443
usab2bmail.com	1309
outlook.com	1125
megalotintl.com	1106
sicurezzanews.it	646
gmail.com	603
1treebridge.com	508
car-tdy9.com	473

Top-15 IPs Sending COVID Spam

178.63.199.212	7022
65.175.68.191	5416
185.203.41.151	1957
184.175.86.164	1309
50.198.21.133	1106
134.209.45.52	864
77.246.51.158	704
65.175.68.7	508
91.228.101.54	473
82.135.19.131	353

Top-15 Countries Sending COVID Spam

US	15372
DE	8747
IN	3595
CH	1996
GB	1212
CN	1077
ZW	708
FR	565
CA	407
IT	322

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

Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	6
UN Covid 19 Relief fund.	4
Re: Effects of COVID-19 on Sunflower	3
Patricia Walter covid negative	3
Corona Praxisinformation	3
NP - ¿Cómo ha cambiado el sector nupcial tras el Covid-19? Los expertos tienen la respuesta	2
CCS /11653 Continúa vacunación contra COVID-19 en Cuauhtémoc, Cusihuriachi, Bachíniva y Riva Palacio	2
Ricerca del lavoro online: cosa è cambiato nell'anno del covid secondo l'analisi di Semrush	2
szczepienia p/covid-19	2
Communication COVID-19 and Safety Guidelines	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: 149,803
Domains with Potential Mail Servers: 2,567
Email-Capable Domains and Hosts: 51,866
Live Hosts and Domains Not Parked: 46,367

Mobile Apps

Apps in Official Stores: 515

by Store

Apple	253
Google	245
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,199

by Store Type:

Hybrid	1122
Secondary	1009
Affiliate	68

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1