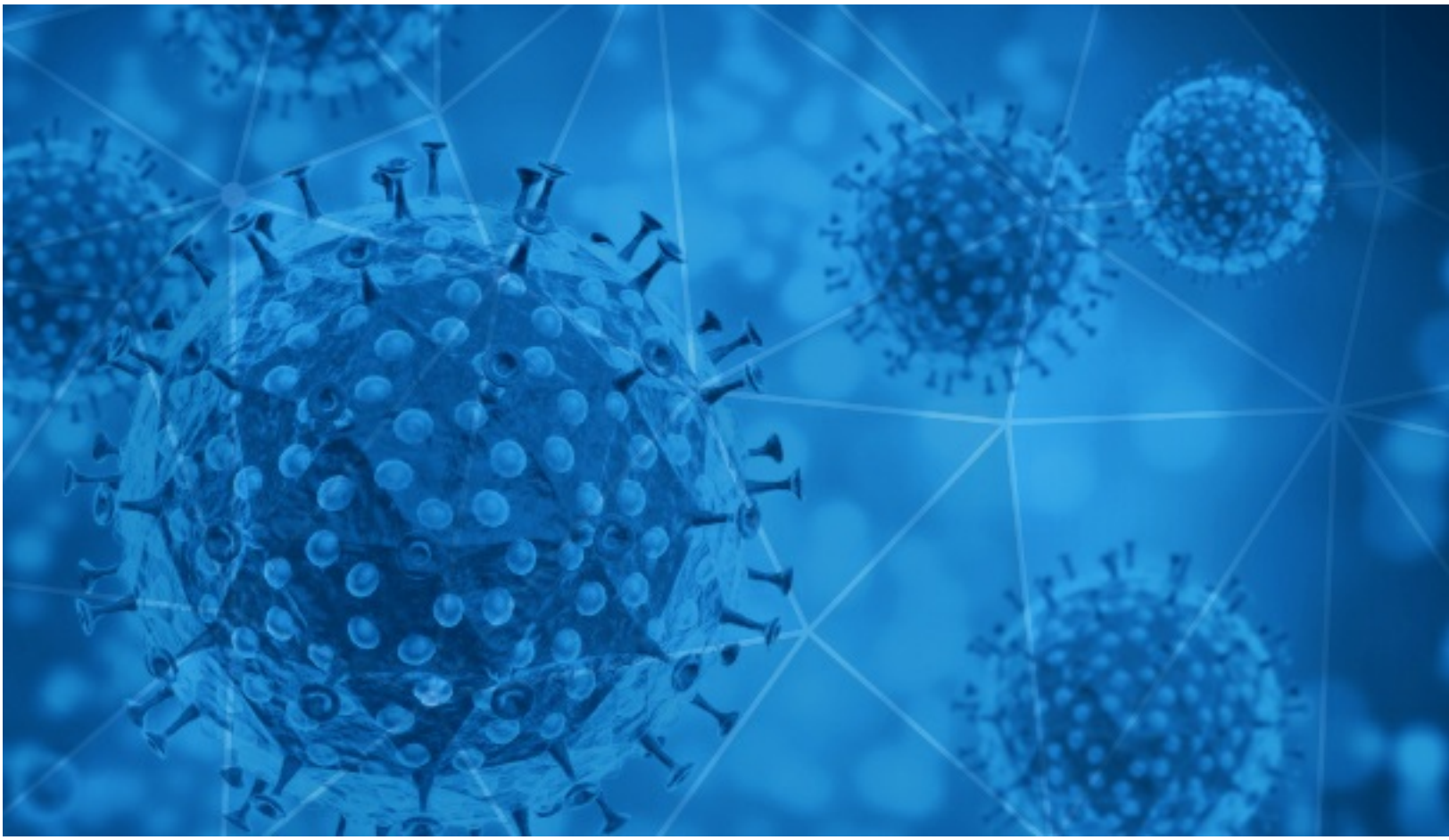
RISKIQ®

RiskIQ i3:

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

2020-12-11



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 2020-12-10 to 2020-12-11. During this period, RiskIQ analyzed 44,437 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,571 unique subject lines observed during the reporting period. The spam emails originated from 2,248 unique sending email domains and 4,807 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	12321
U.S. COVID-19 death toll hits single-day high, the most famous teen in America, and more from Apple News	4021
The Corona Letter: A bump in the road for India's vaccines	3720
Corona proof your life	1835
Respuestas gerenciales para el post Covid19	920
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	768
R&B singer Shot Her Boyfriend In The Head +COVID Vaccine Safe Because Black Woman Helped Develop It?	707
Comunicacion Urgente - COVID 19	583
Officials Are Using Pulse Oximeter To Detect COVID Early	407
Offering N95 FACE MASK (3M 1860,1860S, Makrite 9500 N95,N95S,HARLEY, SAMPLING SWAB AND TUBE KITS,Novel Coronavirus (COVID-19) Test ,quick delivery in a couple days	389
COVID FUNDS	387
Health Officials Say Pulse Oximeter Can Detect COVID In Blood	361
COVID Testing Made Simply- Pulse Oximeter Can Detect The Virus In Blood	350
CDC Update: No More Painful Testing, Pulse Oximeter Can Detect COVID Levels In Blood	343
Benefício Liberado - COVID 19	303
testy na covid-19	280
LIVE NOW - Executive Fireside Chat: Adapting to the Accelerated Demand for Data & Cloud in a Post-COVID World @ 3:00 PM	276
Let’s fight together to get through the COVID-19	263
Contactless infrared body temperature thermometer defeat Coronavirus	262
Re: Corona virus Protection Pills.Order confirmation	260
::: REG-#Season greetings [REDACTED_DOMAIN] #COVID-19*Relief Funds_From "WHO":::::	242
Shop Pulse Oximeter To Detect COVID Virus In Your Blood	232
Re: Defeat Coronavirus, non contact fever alarm device	213
Vaccin coronavirus : devenez virologue | Tous les jobs dans le Luxembourg | Un jobday virtuel pour recruter des techniciens : pari réussi !	211
Avoid Painful COVID Testing Using This Simple Device, Pulse Oximeter	205

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

epc-store.com	12321
insideapple.apple.com	4220
timesofindia.com	3724
manifestco.net	1835
gmail.com	1405
walla.co.il	920
militaryantidisciminationact.com	769
expjumaalsrreadyactivationtthird.com	768
caribbeanfever.com	707
makarksabeaches.com	693

Top-15 IPs Sending COVID Spam

69.94.130.182	1835
194.146.47.162	756
194.146.47.161	691
194.146.47.166	640
201.231.5.107	483
103.225.54.164	446
113.116.206.101	437
190.247.240.136	397
103.99.1.130	387
103.225.54.174	358

Top-15 Countries Sending COVID Spam

US	13897
JP	12786
IN	4393
--	2503
CN	1755
AR	1089
GB	856
FR	730
RU	604
DE	575

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

3M España y United Way España se unen para apoyar a comunidades afectadas por la COVID-19	7
Las enfermeras ofrecen claves y recomendaciones para evitar los contagios de coronavirus en las celebraciones navideñas en los domicilios	5
Covid 19- Return to Work and Workplace Preparedness Course 2021	4
NP Fundación Affinity_ Navidad & Covid-19. El 21% de los españoles se plantea regalar un animal de compañía	3
Lebanon: Health Workers' Safety Neglected during Covid-19	2
ARCOVID19 - Close Contact Packet	2
Beds Available TODAY!! COVID RECOVERD & COVID RECOVERED HD	2
Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	2
Tomorrow's Covid19 Testing	2
FAO SLT: ZOOM Webinars for the COVID-19 Era: Jennifer Nock Training and Consultancy	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: 135,705
Domains with Potential Mail Servers: 2,619
Email-Capable Domains and Hosts: 51,691
Live Hosts and Domains Not Parked: 45,127

Mobile Apps

Apps in Official Stores: 482

by Store

Apple	243
Google	224
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,871

by Store Type:

Hybrid	969
Secondary	843
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1