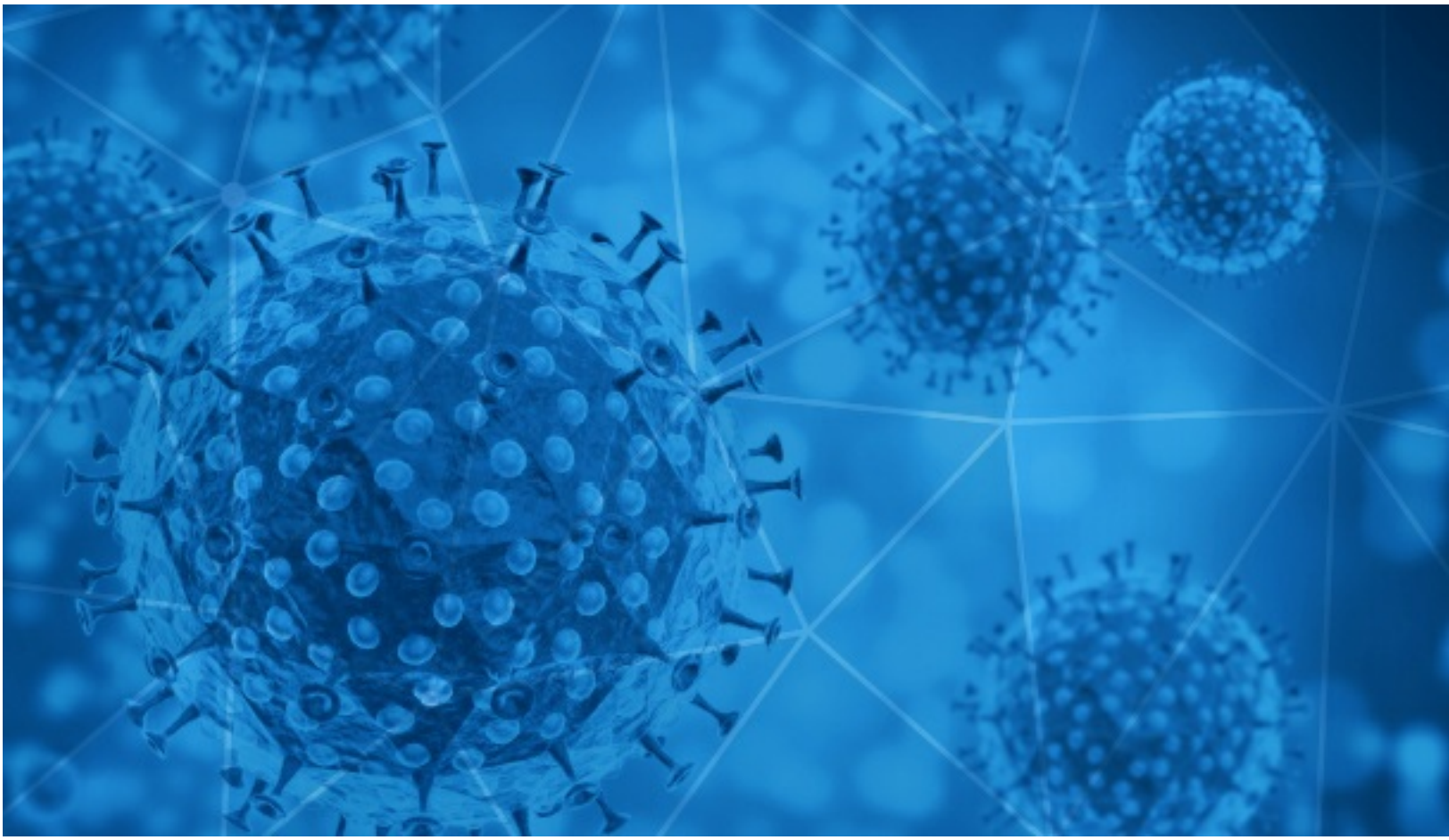
RiskIQ i3:

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

2021-03-05



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 2021-03-04 to 2021-03-05. During this period, RiskIQ analyzed 25,539 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 5,165 unique subject lines observed during the reporting period. The spam emails originated from 2,176 unique sending email domains and 4,164 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Can you skip the mask after vaccination?	3814
COVID - 19 Vaccination for Employees of Dr. B. C. Roy Group of Institutions (all 4 (four) Colleges under Dr. B. C. Roy Engineering College Society	631
Covid19 Relief Fund	594
Venta de Pruebas Suizas Spring Healthcare para descarte de Covid-19.	407
Gran Venta Outlet - Productos Covid 19	382
Re: Personal, SME & Business Relief [COVID-19]	368
Adhesivos Distanciamiento Social Covid-19	349
Retrogen is now performing diagnostic testing for COVID-19	328
COVID-19 Update: We are open and now offering Free Virtual Consultations	300
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	296
Fiscalizacion Laboral últimos Cambios en Entorno covid	288
Re: Defeat Coronavirus, non contact fever alarm device	286
Re: Digital signage solution for Covid-19	281
Thermographic Automation Camera defeat Coronavirus	279
Defeat Coronavirus, Thermographic Camera	279
Contactless infrared body temperature thermometer defeat Coronavirus	268
Adapting to accelerated technology shift in a post- covid world | AI is challenging human decision-making: Bajaj Allianz Life CIDO	254
ICO Covid Inversión	206
Ofertas Test Rapido Covid 19	189
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	186
Eva.cz: Respirátory FFP2 doporučené na ochranu před COVID-19 od 10 Kč za 1 ks	184
Donation For Covid Relief	174
Register Now. Women at work in the post-Covid era	164
Coronavirus briefing: UK ‘ripe’ for variants	163
Pasaporte Covid europeo: ¿obligatorio u opcional? / Epcot florece con el Flower and Garden Festival	163

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	3814
gmail.com	2526
keyable.net	1112
bcrec.ac.in	631
undisbursementcentre.org	594
cmbmutualfunds.com	503
auttoiinz.com	503
126.com	422
oxigenoyderivados.con.pe	407
transiente.cl	349

Top-15 IPs Sending COVID Spam

157.245.42.150	1876
113.116.205.85	1112
149.56.110.130	594
91.228.101.154	502
192.241.128.11	349
50.30.46.201	328
120.89.46.34	233
219.65.85.21	189
219.65.85.14	189
219.65.85.16	188

Top-15 Countries Sending COVID Spam

US	10234
IN	4694
CN	1944
DE	1155
CA	809
GB	704
FR	642
PH	506
IT	425
BR	420

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

NOTA DE PRENSA: Obesidad, enfermedad que empeora con la entrada de la COVID-19 en nuestras vidas	17
netzwerkdraht Corona Auswirkungen	3
Covid-19 Community testing begins in Lanarkshire	2
COVID 19 Webinar Erogazioni in essere e scadenza moratorie: valutazioni e comportamenti banche/finanziarie 26/3/21 4 CFP Odcec	2
our mat kill COVID 19 virus effectively	2
SBA PPP Webinars for Minority Businesses, COVID-19 Business Update, &\tMore	2
Croydon Primary Care Winter Resilience & COVID vaccination planning group	2
Amazon pone en marcha un programa de testeos de COVID-19 regulares y gratuitos para trabajadores de sus centros logísticos en España	2
Agendamiento VacunaciÃ³n Covid-19 Marzo 4/2021	2
I am sharing 'COVID-19 Immunization letter' with you	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: 148,256
Domains with Potential Mail Servers: 2,516
Email-Capable Domains and Hosts: 52,489
Live Hosts and Domains Not Parked: 45,346

Mobile Apps

Apps in Official Stores: 513

by Store

Apple	253
Google	243
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,158

by Store Type:

Hybrid	1095
Secondary	995
Affiliate	68

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1