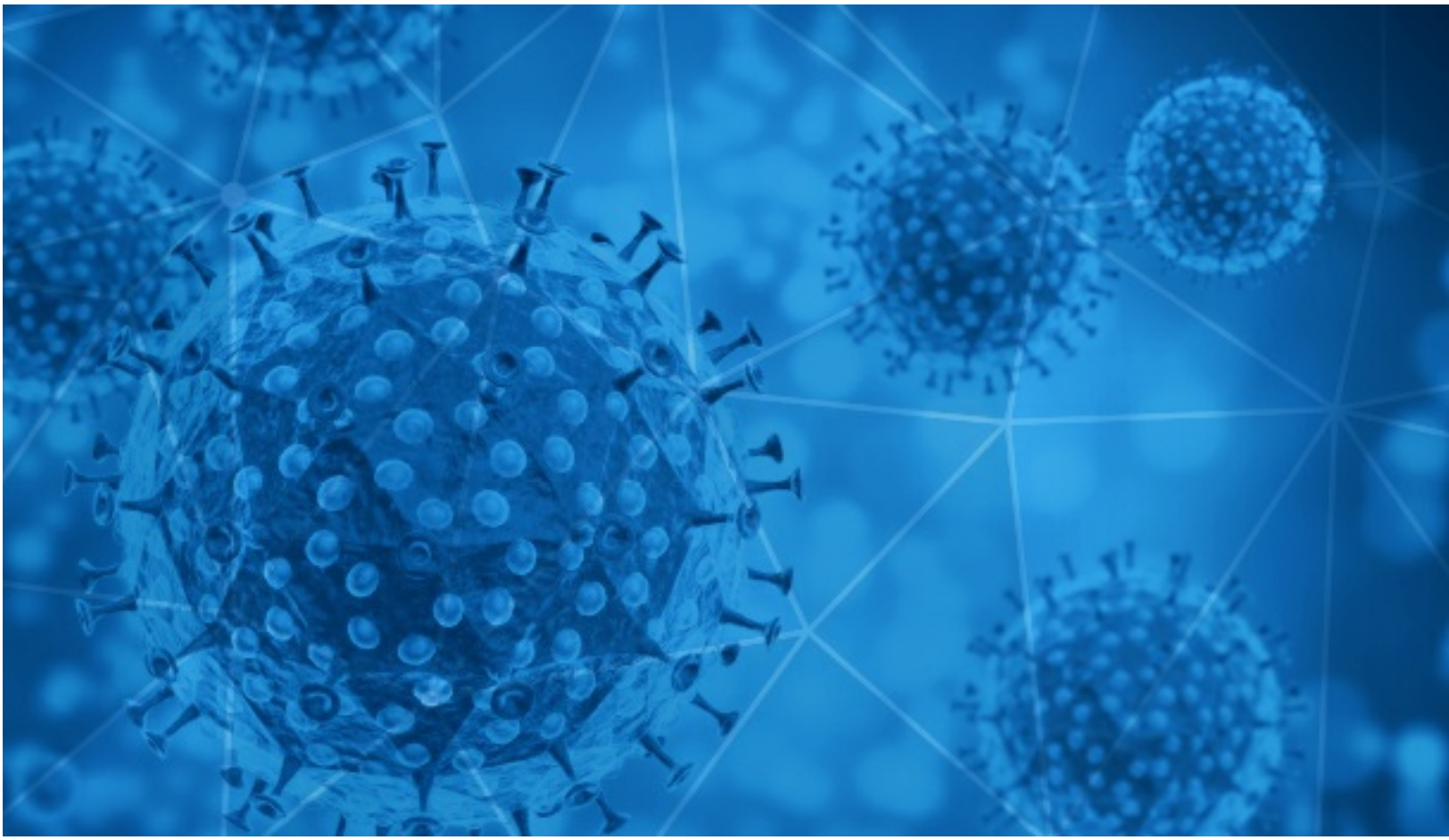
RiskIQ i3:

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

2021-03-03



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 2021-03-02 to 2021-03-03. During this period, RiskIQ analyzed 41,694 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,522 unique subject lines observed during the reporting period. The spam emails originated from 2,066 unique sending email domains and 3,991 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

COVID-19 Financial Relief to receive your R23,400 government issued financial relief	11287
COVID-19 Financial Relief to receive your R35,400 government issued financial relief	4605
The Corona Letter: Vaccination & your viral load	2908
Free Recorded WebinarHow can you keep sales grow under Covid-19? Get prepared for the digital trend!	1988
Medicare covers the COVID-19 vaccine at no cost to you	1806
ANCHE IN ITALIA test COVID19 salivare…	1081
YOU ARE LUCKY WINNER OFPALLIATIVE PROMO OF COVID19	937
Contactless infrared body temperature thermometer defeat Coronavirus	656
Defeat Coronavirus, Thermographic Camera	644
Re: Defeat Coronavirus, non contact fever alarm device	628
Thermographic Automation Camera defeat Coronavirus	610
UN COVID-19 Response and Recovery Fund of $1,500,000.00 US Dollars	457
COVID FUNDS	380
Venta de Pruebas Suizas Spring Healthcare para descarte de Covid-19.	372
Дарим скидку 15% на обязательный ПЦР-тест на Covid-19	280
Retrogen is now performing diagnostic testing for COVID-19	254
Gran Venta Outlet - Productos Covid 19	231
Re: Digital signage solution for Covid-19	227
[QC] ATALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID -19	218
LJC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation	188
Coronavirus briefing: Hunt for ‘patient X’ narrows	180
"En vivo: ¿Cómo manejar el estrés en los niños por la COVID-19?"	159
Ofertas Test Rapido Covid 19	159
Session | 2021 EEOC Issues Guidance for Employers Mandating COVID Vaccines at Work	148
NCJ Daily - New State Vax System. 30 New COVID Cases. NCJ Recipe Contest. A Museum Worth Saving. A Healing Conversation.	143

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

standardbank.co.za	15892
timesofindia.com	2909
keyable.net	2538
service.alibaba.com	1988
subscriptions.medicare.gov	1821
sicurezzanews.it	1081
gmail.com	1014
vivaldi.net	937
unremittanceoffice.us	380
hospiramedical.co.uk	374

Top-15 IPs Sending COVID Spam

109.199.69.21	8091
178.22.234.45	7395
113.116.205.0	2387
161.47.81.122	937
82.135.19.130	545
82.135.19.131	536
91.103.25.74	457
88.202.186.250	406
45.117.210.137	380
23.254.229.176	374

Top-15 Countries Sending COVID Spam

US	9870
PL	8183
NL	7608
CN	5202
IN	3512
DE	1616
GB	982
AM	457
FR	428
RU	381

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

REGISTER NOW! Living in an Anxious World: COVID-19, Substance Misuse, and the Impact on Families	3
COVID REINFECTION REPORTING FORMAT	3
COVID VACCINATION INFORMATION FOR CHILD CARE PROVIDERS	2
WEB OnLine COVID 19 Appalti e subappalti: direzione e controllo, gestione cantieri e tutela dei lavoratori 25/3/21	2
Buletin de presa 02.03.2021 + comunicat actiuni COVID	2
Calabria: Covid, la sindaca e l'assessore alla Salute del Comune di San Giovanni in Fiore scrivono ai commissari Longo e La Regina, "bisogna vaccinare subito gli anziani e i più fragili"	2
WEB COVID 19 Superbonus 110%: Legge Bilancio 2021, Circolare 30/E AdE, procedure per cessione bonus fiscale 11/3/21 4 CFP Odcec	2
AVISO FORMATO NUEVO COVID-19	2
Â NHS Test and Trace: COVID-19 testing for students returning from Mon 8 Mar - Reminder.	2
Maski FFP3 z zaworem i bez, FFP2, KN95, Testy Covid i inne produkty - NAJNIŻSZE CENY NA RYNKU APTECZNYM!!!	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: 148,114
Domains with Potential Mail Servers: 2,545
Email-Capable Domains and Hosts: 52,879
Live Hosts and Domains Not Parked: 45,398

Mobile Apps

Apps in Official Stores: 513

by Store

Apple	253
Google	243
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,150

by Store Type:

Hybrid	1091
Secondary	991
Affiliate	68

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	26
Official	2
Hybrid	1