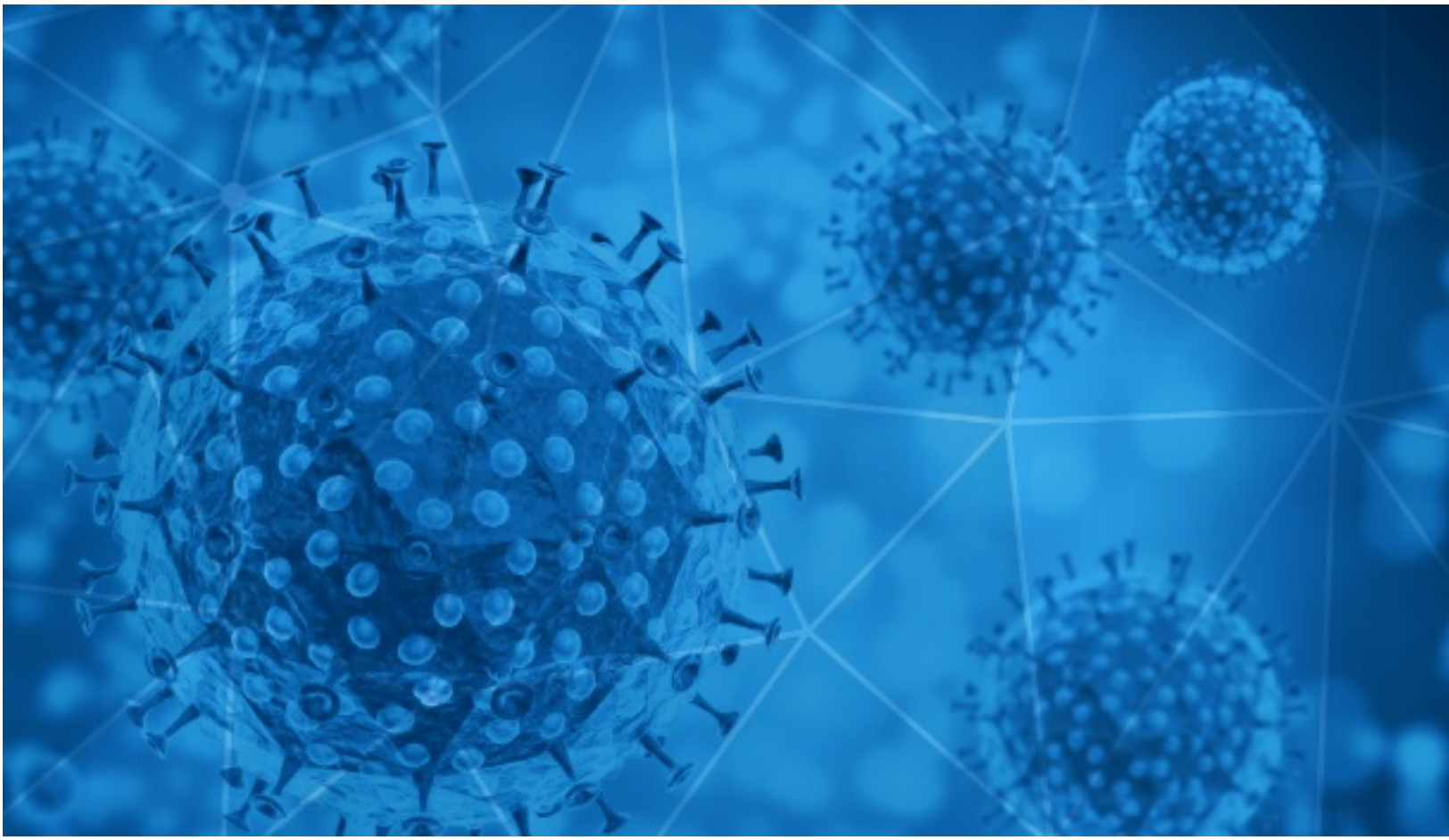
RiskIQ i3:

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

2021-03-04



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 2021-03-03 to 2021-03-04. During this period, RiskIQ analyzed 58,117 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,381 unique subject lines observed during the reporting period. The spam emails originated from 2,124 unique sending email domains and 4,640 unique SMTP IP Addresses. Analysts identified 6 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	18209
COVID-19 Financial Relief to receive your R35,400 government issued financial relief	8446
Biden speeds up vaccination timeline, what life is like for New York's COVID "patient zero," and more from Apple News	6036
The Corona Letter: Is bridging trial a regulatory roadblock?	3109
Covid19 Relief Fund	1061
YOU ARE LUCKY WINNER OFPALLIATIVE PROMO OF COVID19	951
COVID-19 ALLEVIATION STIMULUS PROGRAM [International Monetary Fund]	857
COVID FUNDS	819
ICO Covid Inversión	752
COVID Vaccine Update	445
VENETO: entro il 27 marzo le domande per il contributo a fondo perduto una tantum a favore di agricoltori particolarmente colpiti dalla crisi Covid-19.	442
Gran Venta Outlet - Productos Covid 19	372
Eva.cz: Respirátory FFP2 doporučené na ochranu před COVID-19 od 10 Kč za 1 ks	330
Re: Digital signage solution for Covid-19	322
COVID-19 vaccine - Things to know	294
Additional COVID-19 financial support announced – what you need to know	282
Defeat Coronavirus, Thermographic Camera	230
Re: Defeat Coronavirus, non contact fever alarm device	213
Thermographic Automation Camera defeat Coronavirus	212
Contactless infrared body temperature thermometer defeat Coronavirus	200
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove...etc.	189
Venta de Pruebas Suizas Spring Healthcare para descarte de Covid-19.	178
Re: covid-19 touch monitor	174
Retrogen is now performing diagnostic testing for COVID-19	172
Coronavirus briefing: Europe vaccine warning	167

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	18212
standardbank.co.za	8446
insideapple.apple.com	6061
timesofindia.com	3109
gmail.com	2236
undisbursementcentre.org	1061
vivaldi.net	951
keyable.net	855
unremittanceoffice.us	819
sabaziusv.com	668

Top-15 IPs Sending COVID Spam

109.199.69.21	4185
178.22.234.45	3711
149.56.110.130	1061
161.47.81.122	951
45.117.210.137	819
113.116.204.169	683
103.225.52.165	670
103.225.54.231	587
103.225.54.159	559
88.202.186.250	550

Top-15 Countries Sending COVID Spam

JP	18281
US	15748
IN	4479
PL	4298
NL	3898
CN	1780
CA	1319
GB	1164
ES	920
FR	777

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Aktualności PC World: Kalkulator szczepień na Covid-19 - sprawdź kiedy twoja kolejka [Aktualizacja 03.03.2021r]	5
Re: □□: New order... ventas.corona	1

Top-15 Subjects Containing doc/xlsx Files

WEBINAR COVID 19 Sicurezza Lavoro: adempimenti anti-contagio, protocolli, ispezioni e responsabilità-29/3/21	6
NP_Día Internacional del Linfedema - El Coronavirus dificulta el tratamiento y seguimiento de los pacientes con linfedema en España	2
CORONA-ROOSTER vanaf 3 maart	2
IWD_Accenture presenta lo studio "IF NOT NOW, WHEN" su Covid e parità di genere	2
[ODP-MASTER-PROVIDER-LIST] ODP SURVEY - Direct Service Professional (DSP) COVID-19 Vaccination Need and Access Survey	2
Boletim Epidemiológico Covid-19 - 310	1
Kinderstunde Corona 03.03.21.docx	1
Atresmedia y Banco Santander impulsan la tecnología como motor de cambio y recuperación en la era Covid-19 a través de LEVANTA LA CABEZA (NP + Fotos)	1
RV: MATERIALES ASESORÍA EVIDENCIAS COVID 19/21 Y ELABORACIÓN DE AUDIOVISUALES	1
Covid-19 Vaccination Info.	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: 148,202
Domains with Potential Mail Servers: 2,534
Email-Capable Domains and Hosts: 52,877
Live Hosts and Domains Not Parked: 45,322

Mobile Apps

Apps in Official Stores: 513

by Store

Apple	253
Google	243
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,151

by Store Type:

Hybrid	1091
Secondary	992
Affiliate	68

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1