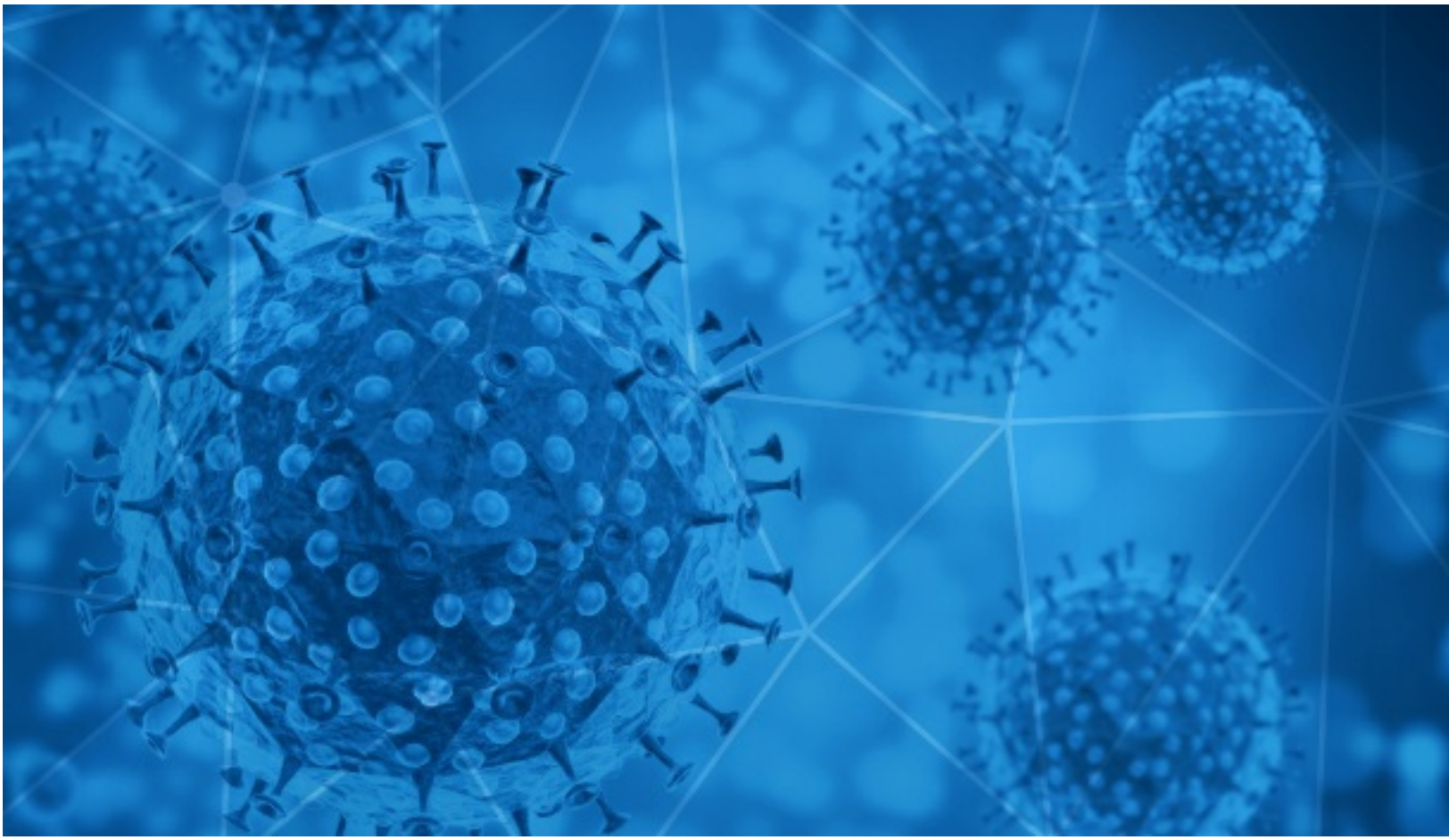
RiskIQ i3:

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

2021-01-07



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 2021-01-06 to 2021-01-07. During this period, RiskIQ analyzed 44,105 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,679 unique subject lines observed during the reporting period. The spam emails originated from 2,158 unique sending email domains and 4,179 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	17362
The Corona Letter: India yet to finalise details of vaccine purchase	4481
Covid-19 Relief F und	1485
Re: Defeat Coronavirus, non contact fever alarm device	998
Contactless infrared body temperature thermometer defeat Coronavirus	952
Covid-19 Pandemic Relief Program	764
Gran Venta Outlet - Productos Covid 19	679
Community Leader Telephone Townhall on Coronavirus Cancelled	562
Re: Covid-19 relief fund!	427
Let’s fight together to get through the COVID-19	417
COVID-19 Update: We are open and now offering Free Virtual Consultations	392
Todo En Insumos Covid 19	387
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	362
Know the Facts About COVID-19	341
Join the Bowser Administration for a Community Leader Telephone Townhall on Coronavirus	337
COVID-19 PANDEMIC COMPENSATION FUND	330
Flu/Covid-19 Weekly questionnaire - Reminder 1	309
COVID-19 Financial Support/Loan Program.	300
Action required – submit your Coronavirus Job Retention Scheme December claims	286
.Net Solutions Architect 100%!r(MISSING)emote until Covid subsides @ Columbus OH - 24+ monthÃÂ¢ÃÂ¿ÃÂ¿s contract - Interviews started…	211
.Net Solutions Architect 100% remote until Covid subsides @ Columbus OH - 24+ monthÃÂ¢ÃÂ¿ÃÂ¿s contract - Interviews started…	181
Help prevent the spread of respiratory diseases like COVID-19 in your workplace	172
Test Covid Per Farmacie - Sierologici e Antigenici	171
Re:covid-19 touch monitor	167
Good Morning, SA | SA government delay on Covid vaccines exposed, Motsoaledi plans printing works expansion	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

epc-store.com	17365
timesofindia.com	4481
gmail.com	2290
keyable.net	1950
xcontrol.it	1485
subscriptions.dc.gov	899
163.com	558
representative.com	426
126.com	407
accionlabs.com	392

Top-15 IPs Sending COVID Spam

113.116.204.166	1833
159.203.20.65	812
157.245.42.150	666
103.225.55.189	530
103.225.53.174	466
103.225.53.181	455
103.225.53.136	441
103.225.55.59	430
45.82.71.10	426
103.225.54.199	410

Top-15 Countries Sending COVID Spam

JP	17407
US	8540
IN	4638
CN	3533
FR	1365
CA	1201
GB	1056
JO	760
--	756
DE	701

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

Re: Actualización de Directorio para vacuna COVID-19	4
Comunicat de presă - România s-a alăturat demersului comun al unor state membre UE privind dezvoltarea unui mecanism european pentru accesul statelor PaE la vaccinul anti-COVID-19	4
STILL TIME TO REGISTER - Palisades Institute: The Impact of COVID-19 on Rockland County's Healthcare System	3
COVID	2
Positive Cases of COVID-19: 01/05/21	2
IMSS Boletín 011.- Primera dosis de la vacuna contra COVID-19 la han recibido 21 mil 634 trabajadores de la salud del IMSS	2
Mason's Travel - Seychelles Covid 19 update / Mise a jour 2021 # 2	2
Viguatur Portafolio de Servicios 2021 y Protocolo de Salud y Seguridad ante el Covid 19	2
Per E-Mail senden: Öffnungszeiten Corona.docx	2
Comunicato AIFA n. 622 - COVID-19: il 7 gennaio riunione della CTS AIFA per vaccino Moderna	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: 138,654
Domains with Potential Mail Servers: 2,578
Email-Capable Domains and Hosts: 52,813
Live Hosts and Domains Not Parked: 53,662

Mobile Apps

Apps in Official Stores: 499

by Store

Apple	244
Google	239
WindowsPhone	15
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,994

by Store Type:

Hybrid	1026
Secondary	907
Affiliate	61

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1