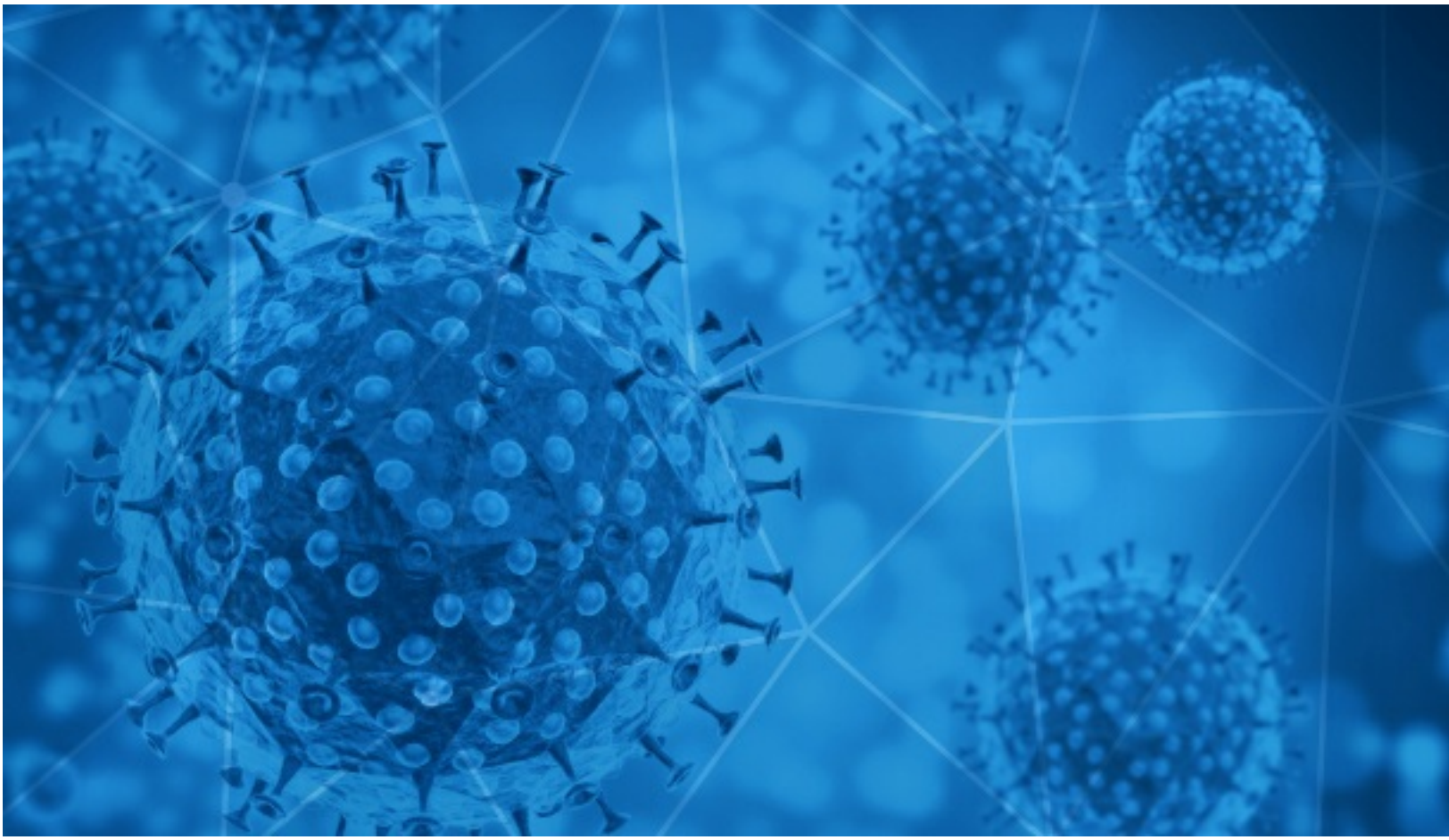
RiskIQ i3:

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

2021-01-06



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 2021-01-05 to 2021-01-06. During this period, RiskIQ analyzed 55,498 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,541 unique subject lines observed during the reporting period. The spam emails originated from 2,170 unique sending email domains and 4,876 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	15318
What to know about today's elections in Georgia, four states identify new coronavirus variant, and more from Apple News	5574
Covid-19 Relief F und	3393
KN95 face mask anti covid19	3391
Anti Corona masks	3060
The Corona Letter: The good side of Bharat Biotech's vaccine	2307
TEST COVID 2021	1512
COVID-19 Update: We are open and now offering Free Virtual Consultations	1172
Contactless infrared body temperature thermometer defeat Coronavirus	827
Re: Defeat Coronavirus, non contact fever alarm device	788
ATTN: KN95 Certified Masks Are Being Recommended For Daily Usage To Combat COVID19	719
CDC Urges Americans To Stock Up On KN95 Certified Mask To Help Curve COVID19 Virus	701
URGENT: Health Officials Urge Use Of KN95 Certified Mask To Curve COVID19 Virus	700
Todo En Insumos Covid 19	552
Know the Facts About COVID-19	432
COVID-19 PANDEMIC COMPENSATION FUND	396
Let’s fight together to get through the COVID-19	375
How tech at India's national data repository meets extraordinary demands from GoI projects |This is how Oyo converted COVID challenge into opportunity	318
Welcome Back Esquire-Back to School Stationery Products and Covid-19 PPE Products, Notebooks, Monitors, Printers and Much More	279
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	265
Direct Client State Req: Need Sr. Java Lead Developer, Tallahassee ,FL & SharePoint Online Developer Remote until COVID-19!!	262
COVID-19 Financial Support/Loan Program.	204
Free COVID-19 course	197
Good Morning, SA | Experts weigh government's Covid vaccination plans, Free State asbestos roofing danger lurks	192
COVID LOANS FROM UNITED NATIONS	171

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	15322
outlook.com	6679
insideapple.apple.com	5574
xcontrol.it	3393
timesofindia.com	2307
plazalamas.com	2120
gmail.com	1885
keyable.net	1615
covid19.com	1511
akhirawahdnshaamolananjibobih.com	670

Top-15 IPs Sending COVID Spam

213.108.199.125	6040
150.136.130.23	2948
72.19.15.130	2112
113.116.207.1	1615
134.255.232.165	1511
103.225.52.178	458
159.203.20.65	445
103.225.53.86	437
103.225.53.231	437
103.225.52.27	436

Top-15 Countries Sending COVID Spam

JP	15393
US	15360
--	8519
CN	3189
IN	2891
DE	2122
GB	1285
CA	985
FR	928
IT	553

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

Organizzazione e gestione lavoro PA e Spa pubbliche nell'Emergenza COVID: POLA e lavoro da remoto 16/2/21	12
COMUNICATO STAMPA - VACCINAZIONE ANTI-COVID19: AL MONTECATONE R.I. ADESIONE VICINA AL 70%	3
Positive Cases of COVID-19: 01/04/21	2
Fwd: «Профилактика инфекционных заболеваний. Актуальные вопросы профилактики новой коронавирусной инфекции COVID – 19»	2
Confirmed COVID Case	2
Buletin de presa 05.01.2021 + comunicat actiuni COVID	2
Itchen College COVID 19 Update	2
COVID-19 Supplier Risk Management & Part Supply Impact [2nd Phase outbreak]	2
postive covid	1
Alerta: surgen engaños relacionados a la vacuna contra el COVID-19	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: 138,522
Domains with Potential Mail Servers: 2,580
Email-Capable Domains and Hosts: 52,758
Live Hosts and Domains Not Parked: 52,763

Mobile Apps

Apps in Official Stores: 496

by Store

Apple	241
Google	239
WindowsPhone	15
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,992

by Store Type:

Hybrid	1025
Secondary	906
Affiliate	61

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1