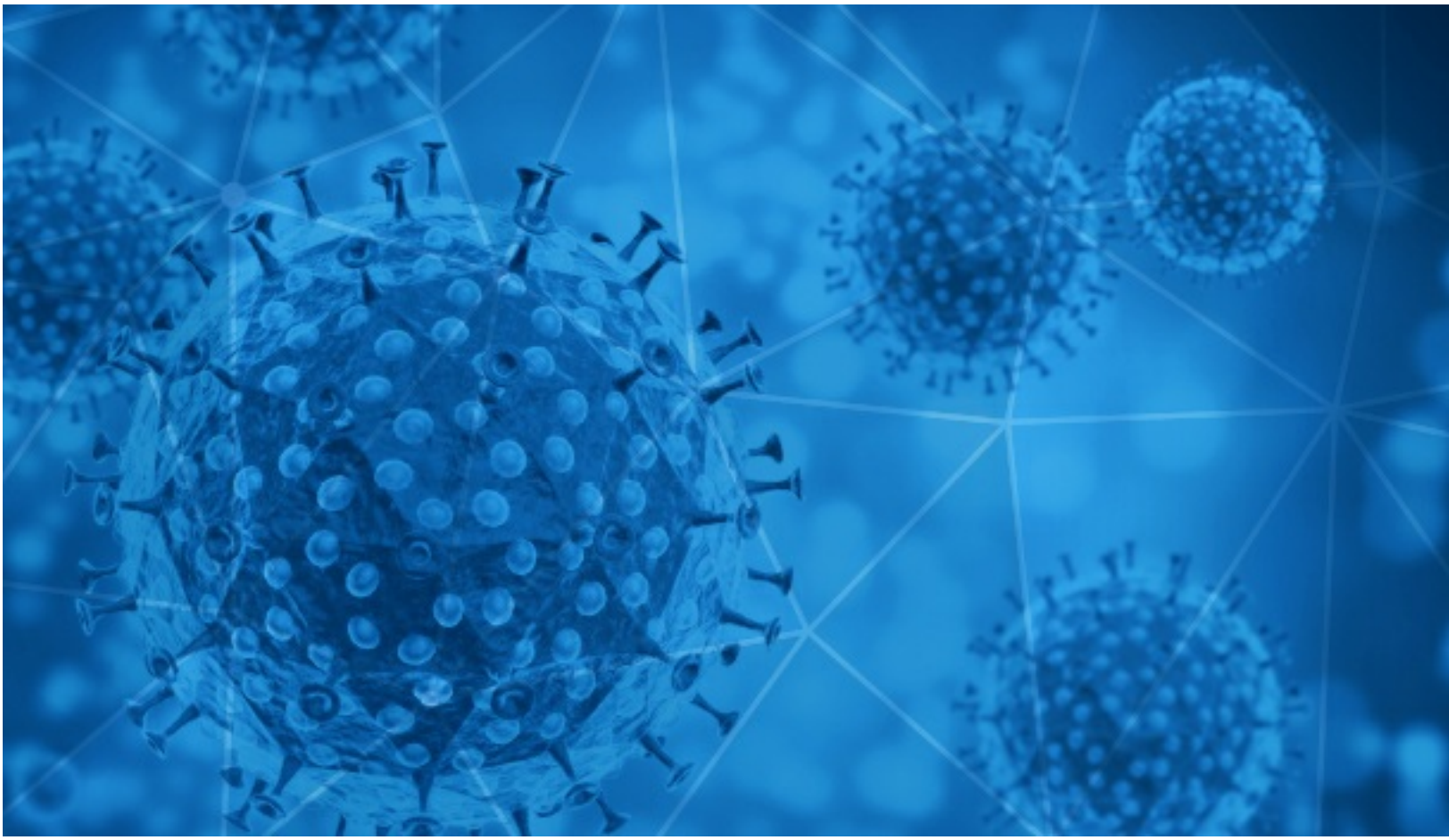
RISKIQ®

RiskIQ i3:

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

2020-12-08



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 2020-12-07 to 2020-12-08. During this period, RiskIQ analyzed 29,243 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,986 unique subject lines observed during the reporting period. The spam emails originated from 2,022 unique sending email domains and 5,018 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Serum Institute's ready as well	3755
Giuliani tests positive for COVID-19, what it feels like to get a coronavirus vaccine, and more from Apple News	3488
COVID-19 Update: We are open and now offering Free Virtual Consultations	2052
United Nations 2020 Covid-19 Compensation Payment.	1888
Corona Schnelltest	1131
Safety measures to stay protected against COVID-19	643
Прилагане на общия регламент за Защита на личните данни GDPR в условията на COVID- 19	601
UV-C-Sterilisationslampe als guter Weg zur Bekämpfung des Coronavirus (covid-19)	597
Re: Defeat Coronavirus, non contact fever alarm device	359
Contactless infrared body temperature thermometer defeat Coronavirus	354
Testy kasetkowe na COVID19 - chroń siebie lub firmę - 99% skutecznoci	349
Re: Corona virus Protection Pills.Order confirmation	327
Hope you are safe during this Covid-19 period.	324
Protégez-vous du Covid avec SOLUGERM France	287
Respuestas gerenciales para el post Covid19	232
Announcing my health care and COVID-19 team	229
COVID Cases Surge- CDC Urges Mask Usage, Get Your KN95 Masks Today Free Shipping	225
COVID-19 Relief Support.	213
Action required – submit your November Coronavirus Job Retention Scheme claims	208
RESTOCK: KN95 Masks Are Said To Be Our Best Protection From COVID, Get Your Mask Today	197
Re: covid-19 touch monitor	186
Global Pandemic Relief Fund 3 Million Pounds In 2020 Coca Cola Covid-19 Pandemic Relief Award	182
Re: Digital signage solution for Covid-19	171
COVID 19 Cases Spike Alarmingly But KN95 Masks Continue To Protect American Citizens	157
Covid-19 : un manque d’oxygène avec le masque ? | Combien coûte un enfant ? | Flexitarisme : quels bienfaits pour la santé ? |	157

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	3766
insideapple.apple.com	3488
yandex.com	1894
gmail.com	1212
covid-19-schnelltests-24.de	1131
keyable.net	713
ourvaluedcustomer2pjdrewardsrready.com	710
icicliprulife.com	643
abv.bg	602
uvclampen.ch	597

Top-15 IPs Sending COVID Spam

150.95.82.182	1894
113.89.43.81	713
77.55.217.43	597
194.146.26.41	420
46.242.244.139	355
67.219.150.138	327
212.4.42.16	324
194.146.26.51	307
219.65.85.23	231
219.65.85.35	215

Top-15 Countries Sending COVID Spam

US	10541
IN	4700
SG	2222
--	2067
CN	1662
PL	1054
GB	920
DE	656
BG	604
FR	428

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

Ocena ryzyka zawodowego (aktualizacja pod względem COVID -19)	12
NUEVA FORMACION COVID PARA EMPRESAS	5
14.12.-prawo pracy i czas pracy w podmiotach medycznych -Covid 19	3
COVID-19 Statement for 12/7/20	3
Hold the Date - Palisades Institute: The Impact of COVID-19 on Rockland County's Healthcare System	2
Cases needed for AHRQ ECHO National Nursing Home COVID-19 Action Network	2
CCS 10787 Acumula estado 40 mil 593 contagios y 3 mil 763 defunciones por COVID-19	2
RV: Relación casos Covid 19	2
RV: ESTIMACION DE PRUEBAS ANTIGENICAS PARA DIAGNOSTICO DE COVID-2021	2
COVID	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: 135,083
Domains with Potential Mail Servers: 2,612
Email-Capable Domains and Hosts: 51,520
Live Hosts and Domains Not Parked: 45,145

Mobile Apps

Apps in Official Stores: 481

by Store

Apple	243
Google	223
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,866

by Store Type:

Hybrid	967
Secondary	840
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1