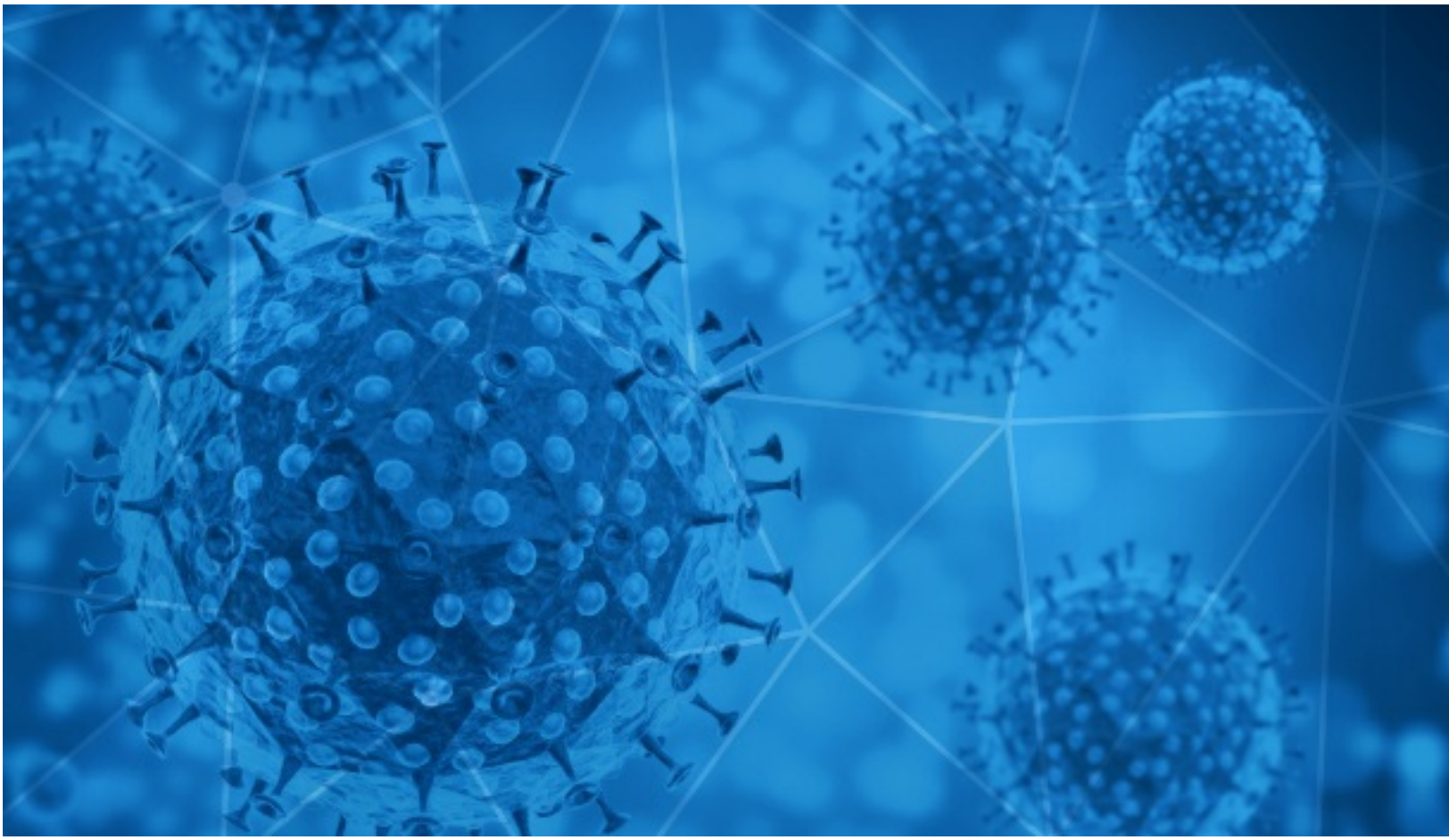
RiskIQ i3:

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

2021-02-02



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 2021-02-01 to 2021-02-02. During this period, RiskIQ analyzed 40,203 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,361 unique subject lines observed during the reporting period. The spam emails originated from 2,203 unique sending email domains and 4,099 unique SMTP IP Addresses. Analysts identified 11 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	9708
GOP senators counter Biden's COVID-relief plan, a powerful nor'easter is coming, and more from Apple News	5069
The Corona Letter: 'Vaccine poverty' can impact rich nations too	4072
Covid19- Fund Compensation Notice	3461
COVID TASTE RESULT	1944
YOU ARE COVID-19 REWARD BENEFICIARY	840
Re:Please Reply Fast To Claim Your Covid-19 Grant!!	669
Your Ultimate Protection against COVID-19. US FDA Registered	610
Public Relation Facebook Covid-19 Lottery	512
COVID-19 Pantallas Protectoras	475
Covid19 Relief Fund:Reply Asap No43	395
UN Covid-19 Winning Notificationw	252
UN Covid-19 Winning Notificationw	242
Help fight Covid-19: Support Nutrition for Children	242
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove...etc.	236
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW...	230
COVID-19	210
Re: Digital signage solution for Covid-19	203
CE FDA 510K GLOVES covid-19 Vaccine ,back to me	203
Destination Thailand News - News Alert - Thailand Ranked Among Top 5 Countries for COVID-19 Response	174
Covid-19: How to make money despite the pandemic.	160
Good Morning, SA | Rage attendees knew they had Covid-19, minister's lawyer was a spy, Winde defends beach protests	152
COVID-19 PANDEMIC COMPENSATION FUND	148
Pomóż nam przeprowadzić rzetelne badania. Weź udział w ankiecie „Polacy wobec szczepień przeciwko COVID-19”	119
Sr Smartsheet Developer__Reston, VA or Remote till COVID gets better is fine	114

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	9709
insideapple.apple.com	5075
timesofindia.com	4073
protonmail.com	3693
gmail.com	3620
163.com	767
teemanjay.net	737
webmail.co.za	532
vivaldi.net	517
mailinator.cl	475

Top-15 IPs Sending COVID Spam

153.19.70.33	3460
46.227.16.146	1690
115.238.247.228	967
128.210.126.200	669
79.175.173.238	497
163.172.151.186	494
103.225.54.72	398
103.225.54.64	342
59.152.229.114	336
103.225.54.58	329

Top-15 Countries Sending COVID Spam

US	11196
JP	10047
IN	4201
PL	3671
FR	3248
CN	2657
IR	497
GB	465
DE	390
HK	386

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

WEB OnLine COVID 19 Organizzazione lavoro PA e Spa pubbliche: remote working, contenuti POLA (entro 31/3), sicurezza 16/2/21	8
Frente común entre la Enfermería militar y civil para la lucha frente al COVID-19	4
Covid-19 compensation fund	3
EL COVID-19 IMPULSA LA FIRMA ELECTRÓNICA EN COLOMBIA	2
Fwd: FW: materiał informacyjny dotyczący szczepień COVID dla Seniorów	2
2nd Notice--COVID-19 Vaccination schedule/ Instructions	2
Fwd: CVASU COVID-19 TESTING LAB REPORT on 01/02/21	2
ECONOMIC AND SOCIAL COUNCIL (UN ECOSOC FIGHT FOR CORONA VIRUS PANDEMIC / 2020)	2
Covid19 Test Ecourier Kit Manifest (Home) Northern Ireland Mail Centre	2
COVID19	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: 141,069
Domains with Potential Mail Servers: 2,554
Email-Capable Domains and Hosts: 50,673
Live Hosts and Domains Not Parked: 44,345

Mobile Apps

Apps in Official Stores: 510

by Store

Apple	252
Google	241
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,068

by Store Type:

Hybrid	1058
Secondary	943
Affiliate	67

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1