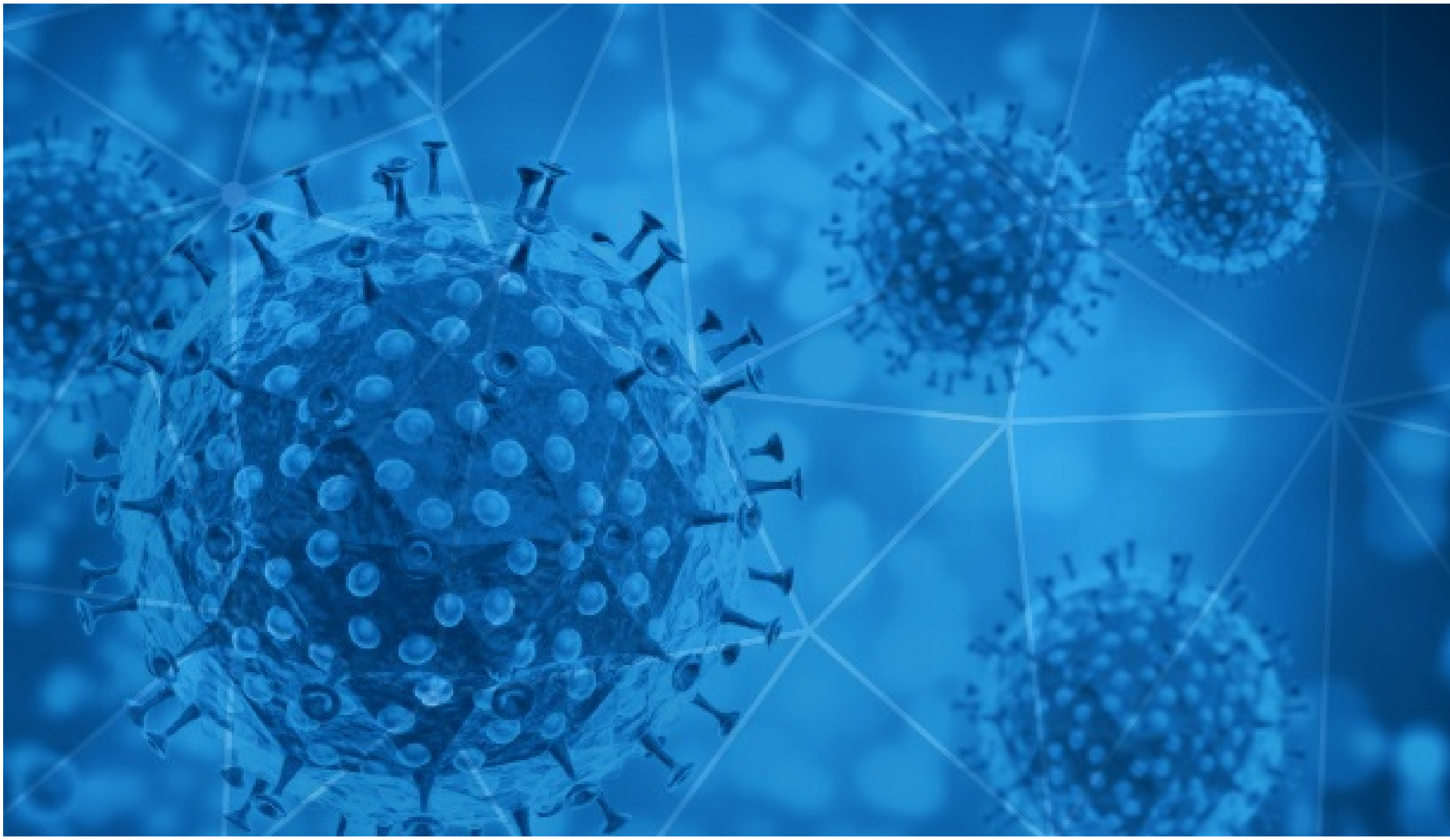
RiskIQ i3:

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

2021-03-29



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 2021-03-28 to 2021-03-29. During this period, RiskIQ analyzed 1,517 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 148 unique subject lines observed during the reporting period. The spam emails originated from 107 unique sending email domains and 178 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	923
- Covid Relief Donation	69
COVID-19 RELIEF FUND, SEND ALL REPLIES TO eacounc@aol.com	67
ATTN Beneficiary(COVID-19 pandemic Essential Worker Support Program (EWSP) WorldWide.	54
COVID-19	51
YOUR COVID-19 STIMULUS PACKAGE WORTH..	43
UNDP COVID19	22
COVID DRUG UPDATES 28/03/2021	17
Coronavirus : les vétérinaires et dentistes vont pouvoir administrer les vaccins | Des conseils d'expertes du bien-être pour bien vivre cette période anxiogène	15
Things to know about COVID-19 vaccination program	12
United Nation Covid .80	11
Morning Briefing: Woman left in agony waiting for knee surgery as waiting lists sky-rocket due to Covid	11
UAB COVID Vaccine Appointment	9
Is The Covid-19 Vaccine Controversy Completely Avoidable? Some say there is a 25 cent Antidote for COVID-19… They say “Rapid Virus Recovery is very, very simple…”	9
Donation For Covid Relief	8
COVID-19 update: Vaccine eligibility is expanding across the country	6
Arma tu kit para tus colaboradores y clientes contra el Covid	6
Covid19 Relief Fund	6
Chinese protective products of COVID-19	5
First locally acquired COVID-19 case in Australia in a week	5
$: Donation For Covid Relief	5
Let’s fight together to get through the COVID-19	4
403 CMAAO CORONA FACTS and MYTH 28th March Preventcovidutrial	4
[medical-voice-for-policy-change] 403 CMAAO CORONA FACTS and MYTH 28th March Preventcovidutrial	4
Dubai World Cup: Magical Mystic Guide wins; China to work with UAE for 'affordable' Covid vaccines; UAE driving licence: Flexible testing service launched in Sharjah	3

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

mail2royal.com	923
aiusm.com	82
aol.com	69
yandex.com	62
outlook.com	58
gmail.com	57
126.com	22
thumbaypharmacy.ae	17
passeportsante.net	15
163.com	13

Top-15 IPs Sending COVID Spam

176.9.34.47	923
202.22.143.47	69
82.137.245.120	54
134.122.91.202	51
96.86.106.193	43
194.94.124.8	36
194.94.124.9	31
192.145.237.249	22
84.38.130.173	17
113.160.166.122	13

Top-15 Countries Sending COVID Spam

DE	998
US	238
NC	69
SY	54
CN	25
NL	24
FR	23
GB	18
VN	13
TW	12

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

- CONFIDENTIAL -

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: 153,975
Domains with Potential Mail Servers: 2,551
Email-Capable Domains and Hosts: 51,735
Live Hosts and Domains Not Parked: 43,812

Mobile Apps

Apps in Official Stores: 519

by Store

Apple	257
Google	245
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,254

by Store Type:

Hybrid	1154
Secondary	1034
Affiliate	66

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1