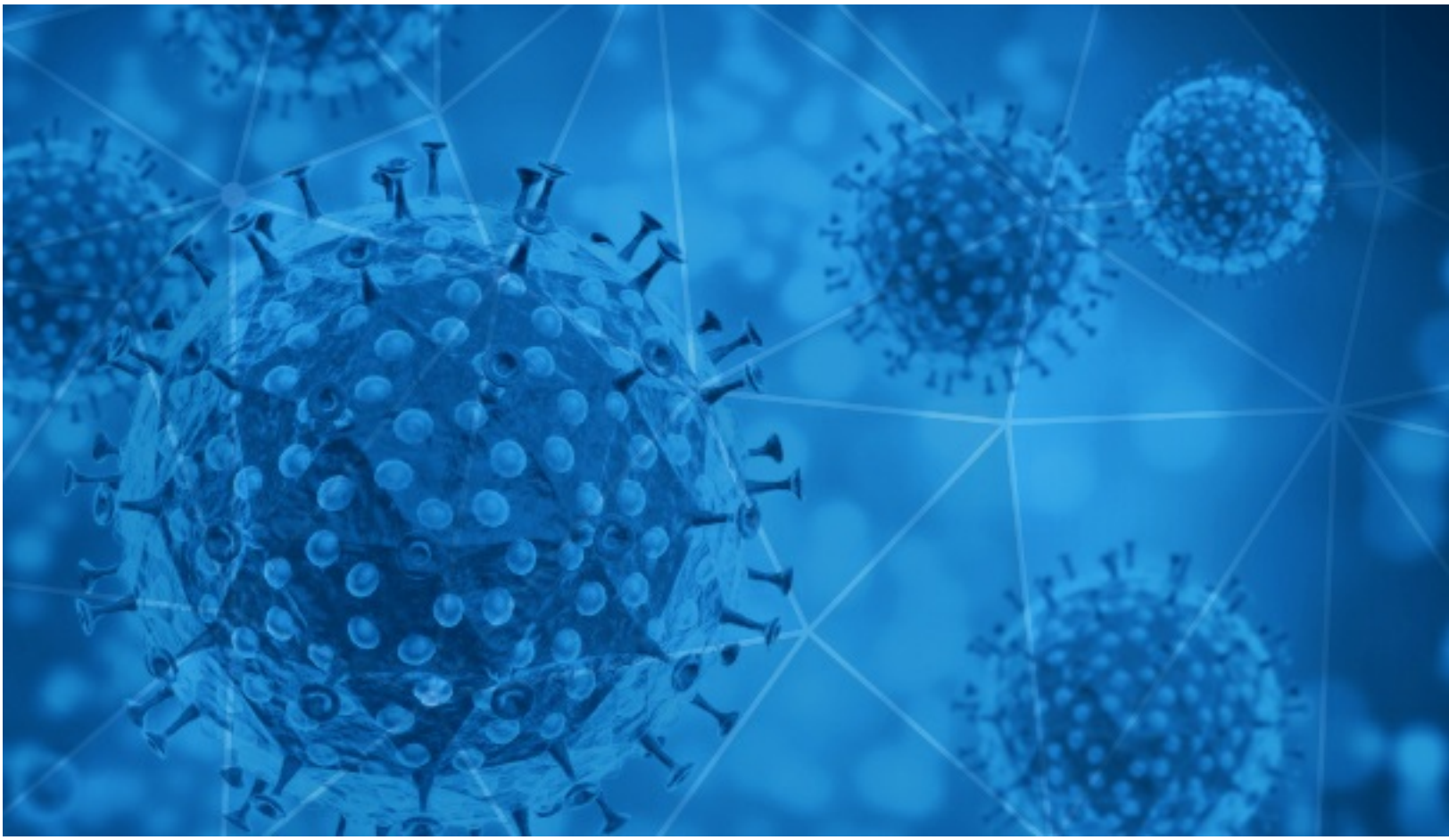
RiskIQ i3:

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

2021-03-15



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 2021-03-14 to 2021-03-15. During this period, RiskIQ analyzed 30,711 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,581 unique subject lines observed during the reporting period. The spam emails originated from 954 unique sending email domains and 2,253 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□	17771
The Corona Letter: The mental toll on healthcare workers	4303
ATTN Beneficiary(COVID-19 pandemic Essential Worker Support Program (EWSP) WorldWide.	496
Re: Digital signage solution for Covid-19	426
Do you have Covid Antibodies ?	316
[L07] The world is recovering from covid-19 it is time to TRAIN your best people!	298
[OL01] The world is recovering from covid-19 it is time to TRAIN your best people!	236
Demeyer: ‘Plots stonden er 200 casseurs’ - Coronablog | Politie schrijft 65 pv’s uit na samenscholing parkings Kinepolis en Kortrijk Xpo - ‘Zal nooit vergeten hoe Assad zijn volk oorlog verklaarde’ - Historica Annelien De Dijn: ‘Belgen missen een…	228
[OL02] The world is recovering from covid-19 it is time to TRAIN your best people!	226
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	205
Re: covid-19 touch monitor	175
Doctors Issue Dire Warnings About COVID-19 Vaccine Dangers	174
covid 19 financial support.	158
□Fiscalización Laboral ☝ últimos Cambios en Entorno Covid	121
Safety measures to stay protected against COVID-19	111
Re: Donation For Covid Relief	111
Killing COVID in Indoor Air and on Surfaces	110
Unite Against COVID - Weekly Update	101
*****We fight against Covid19*****	100
Covid19 Relief Fund $2.5M USD	97
Donation For Covid Relief	97
formation COVID	94
COVID-19	82
New EEOC Guidance for Employers Mandating COVID Vaccines at Work	67
COVID-19 VICTIMS COMPENSATION PAYMENT	67

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

giant-pw.com	17773
timesofindia.com	4303
1treebridge.com	760
126.com	601
outlook.com	601
storytellersgroup.in	315
mail.standaard.be	228
aiusm.com	208
mail2royal.com	205
aim.com	203

Top-15 IPs Sending COVID Spam

65.175.68.7	760
103.225.52.221	559
103.225.55.136	492
77.246.51.158	482
103.225.52.111	482
103.225.53.55	474
103.225.53.97	460
103.225.55.81	427
103.225.52.147	423
103.225.53.222	421

Top-15 Countries Sending COVID Spam

JP	17807
IN	4534
US	3515
CN	804
DE	492
ZW	485
FR	485
GB	412
BE	358
DJ	201

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

ANC Weekly COVID-19 Reports	18
djb-Veranstaltung: Corona und Frauen	2
Cập nhật về thuốc chủng ngừa dịch Covid-19 (Vaccine Covid-19)	2
Formulas for Nursing Hours in the midst of COVID Responses	2
COVID 19 Natore(14.03.2021)	1
Fw: Cập nhật về thuốc chủng ngừa dịch Covid-19 (Vaccine Covid-19)	1
*****SPAM*** Registered Nurse - Covid-19 testing/BRIXTON/COVIDRGN/15 | From: Volcanic Notification(no-reply@volcanic.jobs)**	1
COVID-19 restrictions help understand human impacts on marine life- Flinders Uni	1
RGD NO COVID 13/3/21	1
COVID 19 Vaccination Daily Report Natore (14.03.2021)	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: 149,485
Domains with Potential Mail Servers: 2,564
Email-Capable Domains and Hosts: 51,739
Live Hosts and Domains Not Parked: 46,412

Mobile Apps

Apps in Official Stores: 515

by Store

Apple	253
Google	245
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,192

by Store Type:

Hybrid	1116
Secondary	1008
Affiliate	68

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1