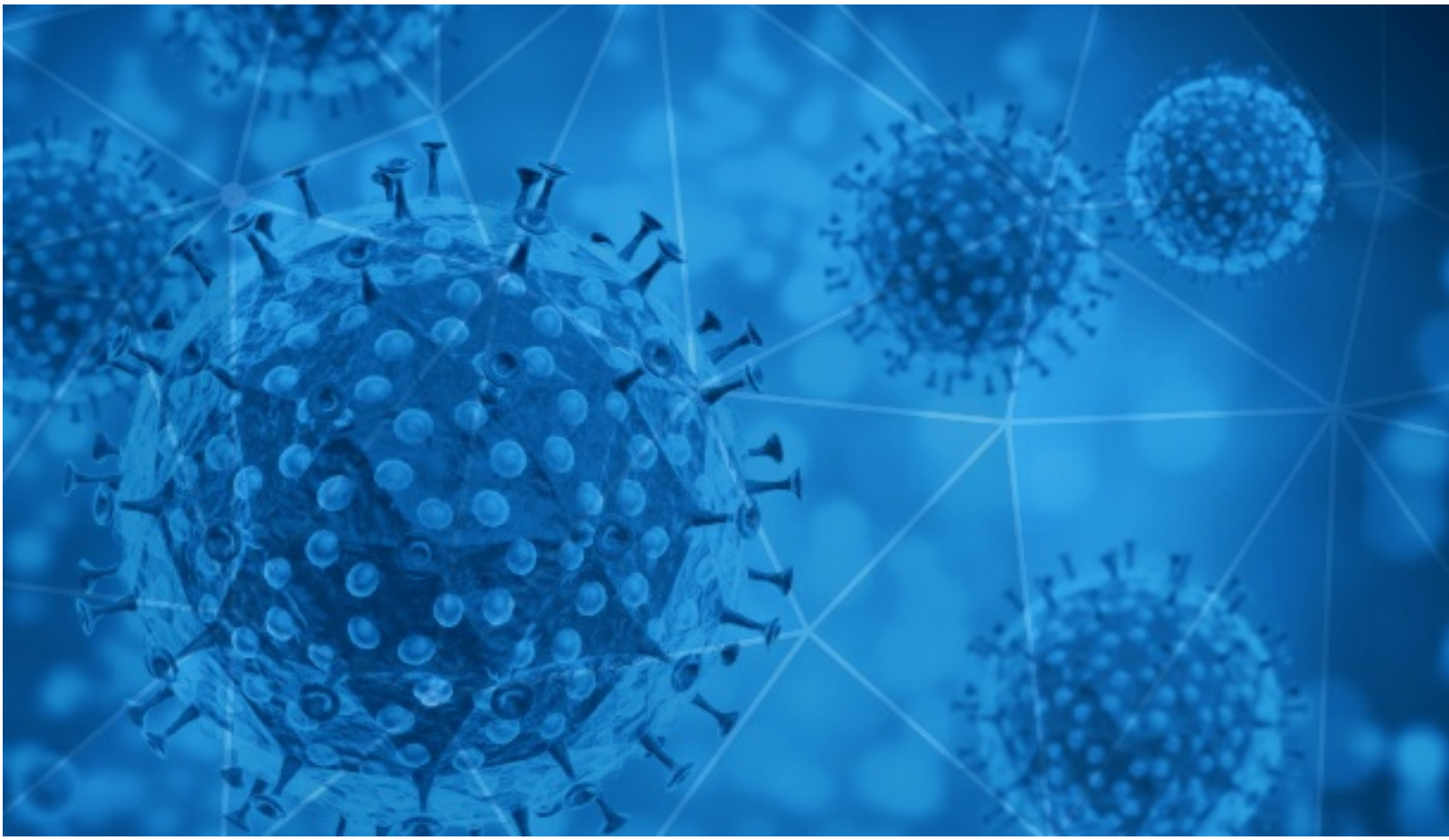
RiskIQ i3:

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

2020-07-13



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 2020-07-12 to 2020-07-13. During this period, RiskIQ analyzed 21,483 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,854 unique subject lines observed during the reporting period. The spam emails originated from 882 unique sending email domains and 2,097 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	5050
Test Rapido Covid 10.000 CLP	3588
COVID-19 Update: We are open and now offering Free Virtual Consultations	1984
PyMEs contra el COVID19	814
Covid 19 Wohltätigkeitsfonds	486
Super Promociones Julio - Proteccion COVID-19	401
The world's worst job? +Man, 30, DIES after catching coronaVirus at a COVID party +Roger Stone FREE	394
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO ANTE EL COVID19	320
COVID-19 - Mobile App Development/ PHP, Magento, Drupal, E-Commerce -etc [REDACTED_DOMAIN]	290
Test Rapido COVID 19	290
Oferta Test Rápidos COVID-19, Mascarillas, Alcohol Gel y Amonio Cuaternario.	287
The Corona Letter: Lockdowns are back but will they help?	274
Evita el Covid19 en tu lugar de trabajo	268
Mantene tu lugar de trabajo libre de covid19	262
Korea Trend News-COVID19(4)	248
Re: covid-19 protect products we can provide	179
Covid-19 relief payments	166
My COVID-19 Donation	145
Update coronacijfers. Daggemiddelde aantal besmettingen neemt opnieuw licht toe	141
Re: N95 face mask and Corona Virus Detection Reagen supplier	129
(Ams-149)....COVID-19 Personal Protective Equipments(PPE)/Medical Items bulk Supply.	120
Re: Surgical & Medical Mask for Coronaviruse / China Qualified	116
Re: keep away from Covid-19	113
COVID protective gear in stock!	105
santizing for COVID19 keep your clients safe	104

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

toyotacarrr.com	5050
trendingtopic.cl	4279
wikimedia.org	1984
gmail.com	1822
countermail.com	1344
126.com	479
163.com	422
caribbeanfever.com	395
correosmasivos.cl	287
timesjobs.com	282

Top-15 IPs Sending COVID Spam

51.77.33.39	1581
51.38.159.218	963
51.38.157.47	799
51.77.33.44	688
103.225.55.107	542
51.77.33.43	534
201.248.69.230	485
181.46.136.165	320
103.225.53.54	301
103.225.55.118	295

Top-15 Countries Sending COVID Spam

JP	5385
FR	5145
US	3305
AR	1683
CN	1116
IN	955
BR	619
VE	485
AU	345
KR	255

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	9
AOSIS Statement for virtual townhall on COVID-19 Omnibus	2
JBS BROOKLYN - IMPORTANT ANNOUNCEMENT Re Covid	1
PLANILHAS DO COVID 19	1
MANTA 27 JULIO ACTUALIZACIÓN TRIBUTARIA 2020 Y REFORMAS TRIBUTARIAS EN LA LEY ORGANICA DE APOYO HUMANITARIO (COVID-19) CURSO ON LINE 100 % PRACTICO	1
July 11 [redacted] COVID -19 [redacted]	1
AN011F-20 Due Date Extension for COVID-19 Ticketing Handling Guidelines	1
NOTIFICATION OF COVID POSITIVE REPORT	1
INSN SAN BORJA ELABORA Y PONE A DISPOSICIÓN GUÍA TÉCNICA PARA EL DIAGNÓSTICO Y TRATAMIENTO DE COVID-19 EN NIÑOS	1
CONCEJALA GRACE ARCOS PRESENTA QUERELLA CONTRA PIÃERA Y MAÃALICH POR PRESUNTA RESPONSABILIDAD EN MUERTES A CAUSA DE 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: 114,266
Domains with Potential Mail Servers: 2,803
Email-Capable Domains and Hosts: 43,105
Live Hosts and Domains Not Parked: 65,646

Mobile Apps

Apps in Official Stores: 331

by Store

Apple	178
Google	144
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 880

by Store Type:

Hybrid	556
Secondary	286
Affiliate	38

Blacklisted Mobile Apps: 21

by Store Type:

Secondary	19
Hybrid	1
Official	1