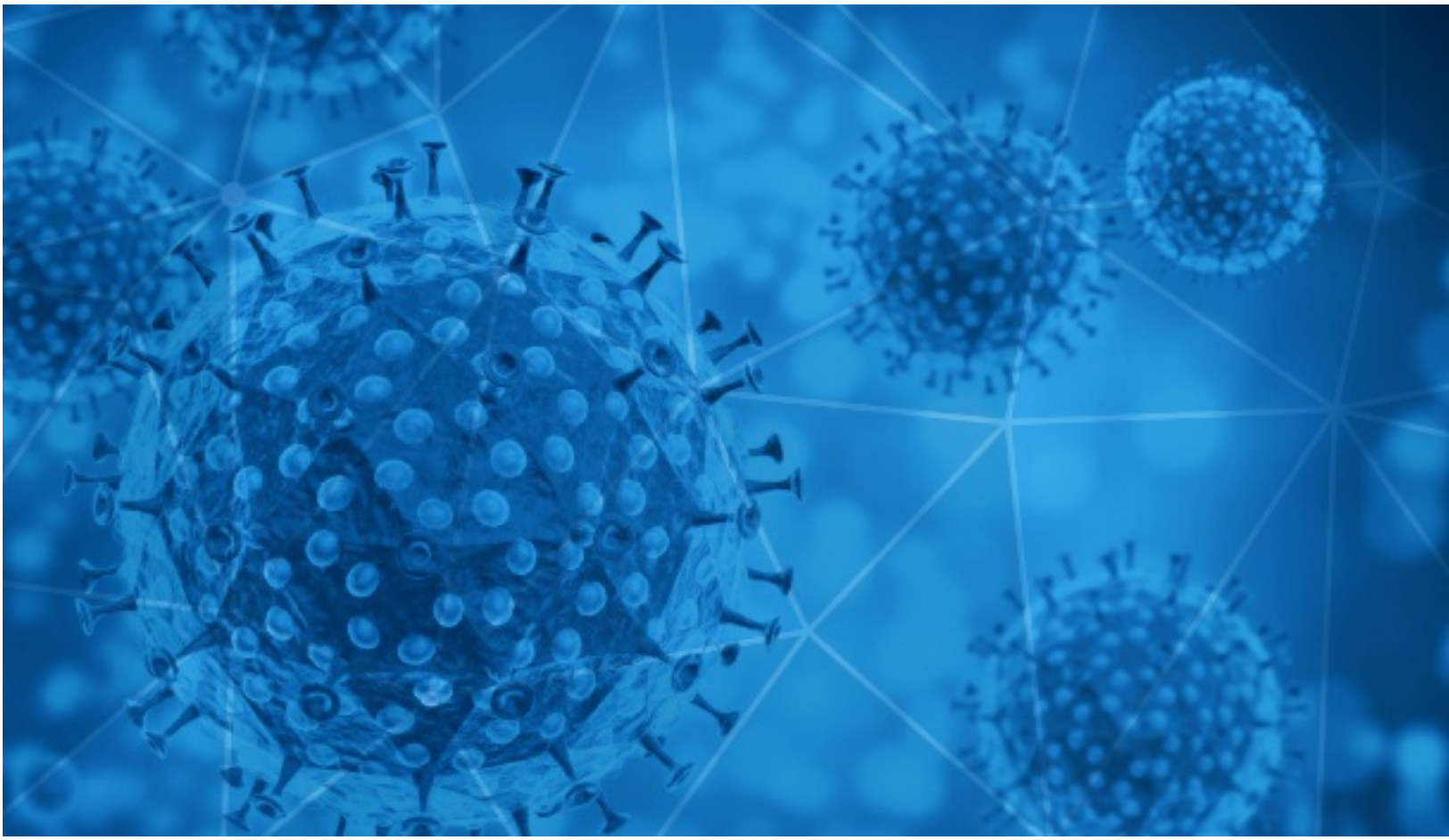
RiskIQ i3:

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

2021-01-28



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 2021-01-27 to 2021-01-28. During this period, RiskIQ analyzed 59,692 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 6,695 unique subject lines observed during the reporting period. The spam emails originated from 2,303 unique sending email domains and 4,395 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	12690
Anti-Corona-Masken von Markenfabrikant 3M FFP2	9416
Anti-Corona-Masken von Markenfabrikant 3M	6033
Help the world's response to Covid-19 with the most protective mask on the market.	3721
The Corona Letter: Vaccination lessons from Israel	3439
Public Relation Facebook Covid-19 Lottery Department	1160
Coronavirus COVID-19 and the impact on car and auto auctions	1129
COVID-19 Pantallas Protectoras	977
Public Relation Facebook Covid-19 Lottery Department!	959
Totem Sanitizador COVID-19 unico con indiador de temperatura	772
Línea de prendas médicas anti covid, especialmente fabricadas para sentirse cómodo todo el día	756
SecVA Nominee Talks Priorities, Caregivers Covid Testing, Vaccines	693
_Step_Closer_To_FDA_ Approval_ 20 People_Take COVID19_ PILL!	457
Equipamentos de Proteção Individual (EPI's COVID 19)	326
COVID TASTE RESULT	275
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove...etc.	255
Re: Digital signage solution for Covid-19	228
NCJ Daily - 28 New COVID-19 Cases. Storm Brings Snowfall, Wind, Power Outages. Fortuna School Closes Due to COVID.	211
YOU ARE COVID-19 REWARD BENEFICIARY.	209
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW...	195
Mi seguro insumos covid 19 protege a tu familia	192
_Step_Closer_To_ FDA_ Approval_ 20_ people_ Take_ COVID19_PILL !	188
Flu/Covid-19 Weekly questionnaire - Reminder week 4	187
COVID-19: Employer support – live webinars	184
COVID-19 What youâre not being told!	178

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

outlook.com	15701
epc-store.com	12690
newhack.buzz	3721
timesofindia.com	3447
hospiramedical.co.uk	3050
rediffmail.com	2115
gmail.com	2046
prostate.buzz	1129
messages.va.gov	820
grupocorreomasivo.com	672

Top-15 IPs Sending COVID Spam

107.167.2.130	8711
45.11.0.73	4308
23.228.101.31	3721
107.174.142.107	1559
172.245.93.102	1376
59.152.229.114	1216
23.228.115.19	1129
5.180.79.11	877
200.28.49.88	772
110.186.72.61	650

Top-15 Countries Sending COVID Spam

US	24616
JP	12907
--	6023
IN	3637
CN	1957
FR	1893
HK	1247
PE	941
CL	794
GB	629

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

WEBINAR COVID 19 bilancio IAS/IFRS: equilibrio finanziario, aspetti contabili rilevanti e novità fiscali - 4 CFP Odcec - 25/2/21	28
AOTS Webinar on The Leadership for the Post COVID-19 Era	14
COVID 19 WEB ON LINE ANTICORRUZIONE E TRASPARENZA: proroga al 31/03/2021 del PTPCT – 24/02/2021	8
Disinformazione e crisi economica da Covid-19 alla base dell'ortodonzia fai-da-te e low-quality. ASIO lancia l'allarme	4
UVC Air & Surface Sanitization for Dentist Offices for Coronavirus & other pathogens	3
Документалната поредица на HBO с реални COVID-19 случаи "Жизнени показатели" е с премиера на 7 февруари	3
Covid19 Test Ecourier Kit Manifest (Home) Northern Ireland Mail Centre	2
COVID - Biojam estabelece acordo para colocar no mercado 2 milhões de testes de saliva	2
COMUNICATO STAMPA // Covid, sanità in prima linea: Finanziaria “premia” i Medici ma dimentica gli Ospedali Religiosi Classificati	2
PRUEBAS DETECCION DE COVID19 SEROLOGICAS Y DE ANTIGENOS	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: 140,877
Domains with Potential Mail Servers: 2,563
Email-Capable Domains and Hosts: 50,861
Live Hosts and Domains Not Parked: 43,939

Mobile Apps

Apps in Official Stores: 506

by Store

Apple	249
Google	240
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,054

by Store Type:

Hybrid	1054
Secondary	933
Affiliate	67

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1