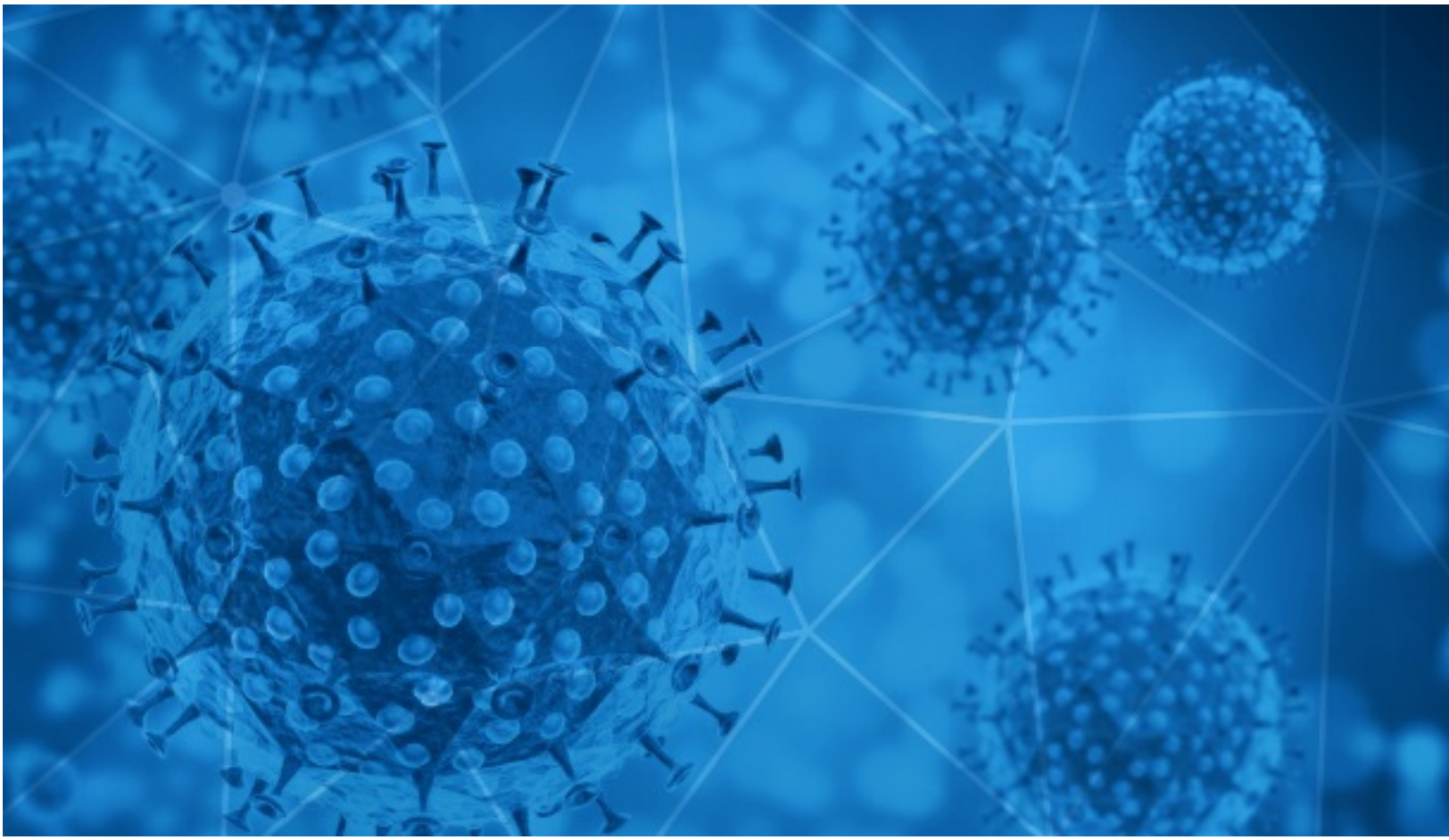
RISKIQ®

RiskIQ i3:

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

2021-02-23



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 2021-02-22 to 2021-02-23. During this period, RiskIQ analyzed 53,144 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,266 unique subject lines observed during the reporting period. The spam emails originated from 2,111 unique sending email domains and 4,037 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	12225
Coronaschutzmasken 0,06 Euro (Schwarz, Pink, Blau)	7798
Hygiensche Einwegmasken: Coronaschutzmasken 6 Cent (Schwarz, Pink, Blau)	5624
What Fauci says about the drop in COVID-19 cases, why the Texas power grid failed, and more from Apple News	5586
The Corona Letter: A faster execution or a flexible vaccine strategy?	3624
COVID19 LOAN RELIEF OFFER / INVESTMENT	1194
Re: Personal, SME & Business Relief [COVID-19].	1081
COVID19 Diferencia entre certificado de aislamiento e incapacidad	1078
COVID-19 Relief Fund"	973
my COVID-19 support loan at 3%	609
Updates for Multi-State Taxation during COVID Pandemic	294
my COVID-19 support loan at 3%!	291
New Corona-virus Mask!	268
Traveling soon, wear this mask to fight chances of getting Corona-virus	263
Get your Corona-virus Mask while supplies last!	261
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove...etc.	256
Reduce your risk of Corona-virus with this Mask	236
Re: Supply Medical supplies for Coronavirus	225
[SPAM] RE:COVID-19 Compensation Claim....	225
Get your own restaurant app at no cost during COVID restrictions.	210
Coronavirus y viajar: ¿podré irme de viaje en la Semana Santa de 2021?	189
Schond Dries Van Langenhove de coronaregels wel? - Agenda Overlegcomité op vrijdag bekend - Vlaanderen verzet zich tegen Europese CO2-plannen - Texas houdt VS pijnlijke spiegel voor - Naomi Osaka biedt antwoord op nivellering vrouwentennis	185
Accords vins - fromages : comment les goûts sont-ils modifiés ? | Covid-19 : que nous disent les dessins d'enfants ? | Cœur et cerveau : pourquoi il faut limiter les aliments frits |	179
Dufferin-Peel CDSB - Announcements: Daily Covid-19 Screening Tool Reminder:	142
Benefício Liberado - COVID 19	141

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmx.de	13421
giant-pw.com	12225
insideapple.apple.com	5586
timesofindia.com	3637
gmail.com	3430
cmbmutualfunds.com	1223
saludtotal.com.co	1102
clervisor.net	1028
163.com	496
outlook.com	295

Top-15 IPs Sending COVID Spam

94.176.238.197	7622
107.167.2.247	3256
172.81.131.102	2537
200.31.17.85	1100
63.81.84.11	1028
51.68.136.26	973
181.210.29.152	680
198.38.84.190	595
101.79.49.106	591
120.89.46.222	588

Top-15 Countries Sending COVID Spam

US	17560
JP	12311
LT	7623
IN	3772
FR	1526
AR	1239
PH	1223
GB	1058
HN	684
CN	678

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

RE: Sr. Network Engineer - Location: Morrisville, NC (Remote till Covid) - $50 on C2C(Please share 10+yrs of experience)	33
Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	10
Ocena ryzyka zawodowego (aktualizacja pod względem COVID -19) / ZUS w praktyce	7
Hospitais referência para Covid-19 da Grande João Pessoa estão com 90% de ocupação de leitos de UTI	3
Deloitte launches its Doing Business Guide for the United Arab Emirates: Business agility in a COVID environment	2
Câmara de Grândola distribui Kit de proteção contra a COVID-19 à população	2
FUNDACION CAPACITAR, SEMINARIO DE REFORMAS TRIBUTARIAS 2021 CIERRE FISCAL CONSIDERANDO EFECTOS DEL COVID 19 E IMPUESTOS DIFERIDOS	2
Statement on Covid Vaccine from UKLDCNN	2
Seminar zum Thema Corona und Steuern und weitere Seminarangebote	2
Fwd: CVASU COVID-19 Testing Lab report on 21/02/21	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: 147,002
Domains with Potential Mail Servers: 2,566
Email-Capable Domains and Hosts: 53,635
Live Hosts and Domains Not Parked: 44,926

Mobile Apps

Apps in Official Stores: 515

by Store

Apple	255
Google	243
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,120

by Store Type:

Hybrid	1075
Secondary	977
Affiliate	68

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	26
Official	2
Hybrid	1