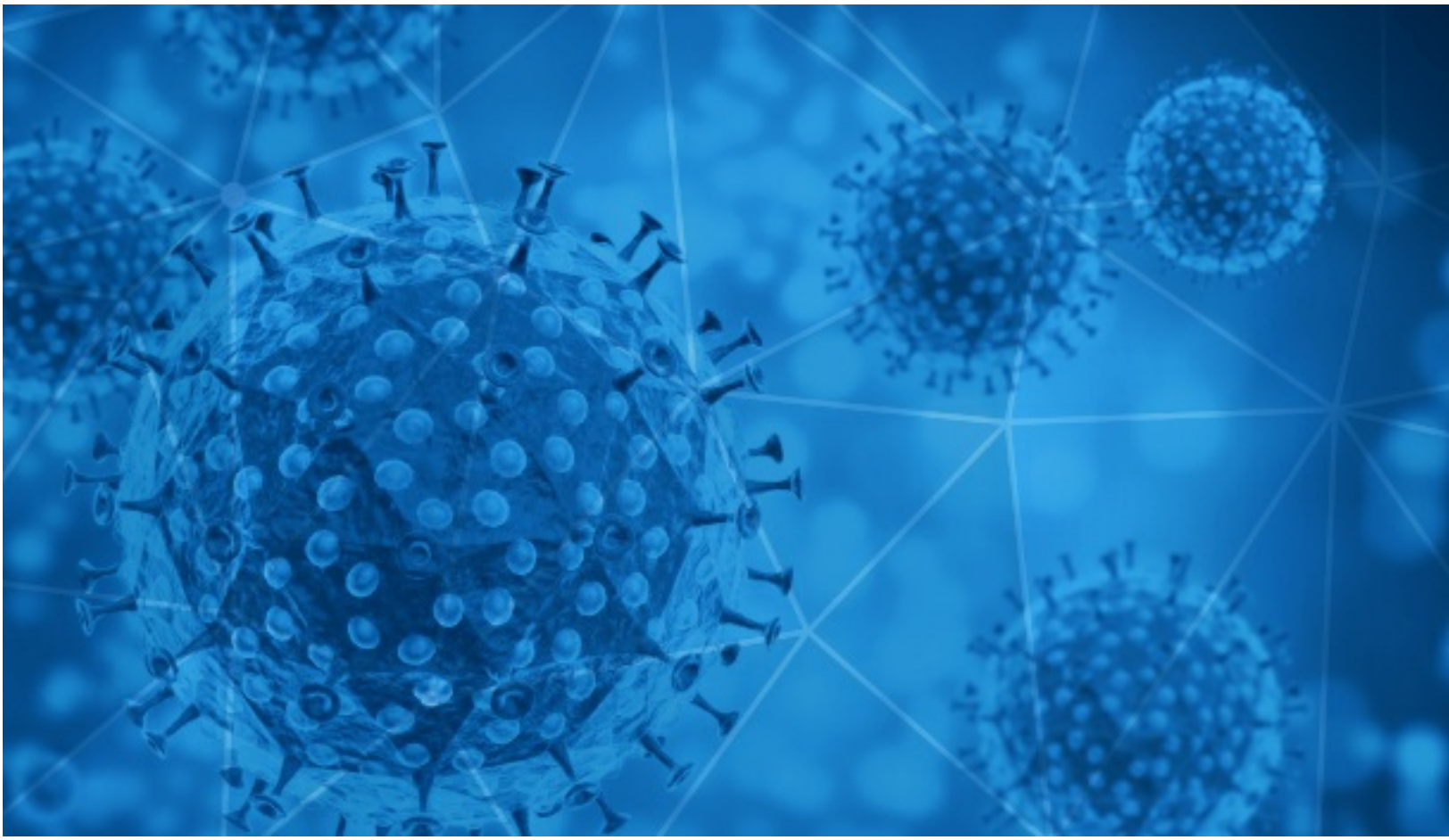
RISKIQ®

RiskIQ i3:

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

2020-12-30



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 2020-12-29 to 2020-12-30. During this period, RiskIQ analyzed 27,141 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 5,031 unique subject lines observed during the reporting period. The spam emails originated from 1,641 unique sending email domains and 3,280 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	6402
The Corona Letter: Will vaccines overcome the trust deficit?	4599
SARDEGNA, SOSPESO IL FONDO RESISTO: nuovo avviso dopo il 18 gennaio 2021. Contributi a fondo perduto alle PMI e Grandi imprese per sostenere imprese e lavoratori in conseguenza della sospensione o ridotta attività dovuta alCovid-19. Scadenza 22 febb	722
Let’s fight together to get through the COVID-19	457
Fake news about COVID-19 is spreading faster than virus	405
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	349
COVID19 Pandemic Grows, Stock Up On KN95 Masks Urgently- Shipping Waived Today	345
Re: Personal, SME & Business Relief [COVID-19]	322
COVID ALLEVIATION STIMULUS PROGRAM [IMF]	271
Offering N95 FACE MASK (3M 1860,1860S, Makrite 9500 N95,N95S,HARLEY, SAMPLING SWAB AND TUBE KITS,Novel Coronavirus (COVID-19) Test ,quick delivery in a couple days	243
Una razón más para tener cuidado con el azúcar: empeora el diagnóstico por covid-19	221
Beanspruchen Sie Ihr Operation Covid-Paket	221
NCJ Daily - Two Deaths and 64 New COVID Cases. Last Full Moon of 2020. Fixing Broadway.	198
Economic effects of Covid-19 l Tips to charge down your electricity bill	162
Re: Digital signage solution for Covid-19	159
Apply for your COVID-19 Relief Loan	155
Re: covid-19 touch monitor	153
Medicamentele folosite pentru tratarea lui Trump de Covid-19 ar putea fi folosite pentru a reduce spitalizarea la jumatate	152
Hospitalizations due to COVID-19 reach new record high in Arkansas	151
Oferta de préstamo Covid-19	144
COVID19s Biggest Defense- Authentic KN95 Certified Masks, Free Shipping Today Only	138
COVID-19 Vaccine Update	131
BOOM! Woman Says What Americans Are Thinking “I’m Done” With this COVID Insanity!	122
XAT 2021: COVID-19 Guidelines and Safety Measures	107
Biden Covid Adviser Says He’ll Invoke Defense Production Act For Coronavirus Vaccine	105

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

epc-store.com	6403
timesofindia.com	4599
stargoldmedics.com	2535
gmail.com	1203
italiacontributi.it	722
163.com	526
bearsonlinesportsstore.com	345
cmbmutualfunds.com	322
126.com	312
outlook.com	310

Top-15 IPs Sending COVID Spam

172.245.93.73	2534
103.225.53.177	916
46.254.37.34	722
103.225.52.111	423
103.225.53.211	406
103.225.53.57	367
175.44.33.22	352
180.165.115.217	349
194.146.36.190	344
103.225.52.64	339

Top-15 Countries Sending COVID Spam

US	8529
JP	6431
IN	4917
CN	1430
IT	966
FR	553
--	549
GB	447
DE	334
PH	322

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

NdP_Logista, preparada para la distribución de la vacuna del COVID-19	4
COVID-19 Office Update	2
IMSS Boletín 867.- Inicia aplicación de vacuna COVID-19 a personal de salud del IMSS en municipios de Coahuila y Nuevo León (FOTOS)	2
IMSS FOTO NOTA.- Personal de salud del IMSS de Chiapas, Guanajuato y Puebla llega a la Ciudad de México para reforzar Equipos de Respuesta COVID	2
LIST OF BRANCHES ATTACHED FOR COVID 19 RESOLUTION.	2
AISLAMIENTO DE PERSONAL POLICIAL POR COVID-19.	2
Pressemitteilung: Corona-Pandemie verschärft drastisch wirtschaftliche Probleme der Krankenhäuser	2
Información para ESPECIAL COVID	1
COVID Testing Counts 28-12-20	1
Re: MCPH Press Release — COVID Cluster	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: 137,855
Domains with Potential Mail Servers: 2,581
Email-Capable Domains and Hosts: 52,511
Live Hosts and Domains Not Parked: 48,951

Mobile Apps

Apps in Official Stores: 499

by Store

Apple	244
Google	239
WindowsPhone	15
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,962

by Store Type:

Hybrid	1006
Secondary	896
Affiliate	60

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1