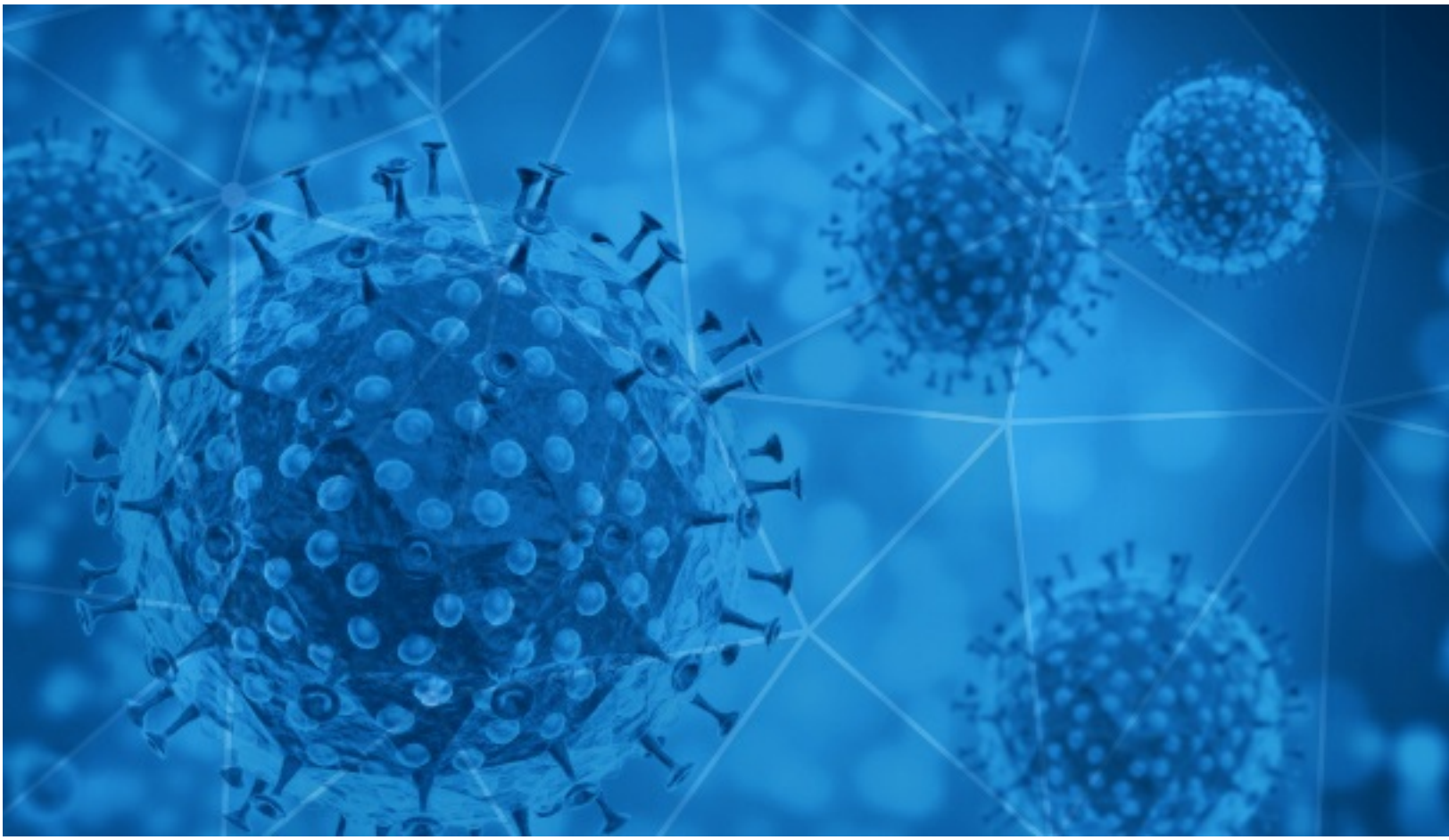
RiskIQ i3:

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

2021-04-01



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 2021-03-31 to 2021-04-01. During this period, RiskIQ analyzed 35,812 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,429 unique subject lines observed during the reporting period. The spam emails originated from 1,233 unique sending email domains and 2,378 unique SMTP IP Addresses. Analysts identified 5 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	9041
These 3 Corona-Virus Lies Put Your Family in Danger	4945
25er Pakete Covid Schnelltest lieferbar (Speicheltest)	4461
Covid Test sofort lieferbar. (SARS-Cov-2-Test)	2536
Aktuell wieder lieferbar. SARS-Cov-2-Test Corona (SARS-Cov-2-Test)	2019
The Corona Letter: Rare immune response may explain blood clots	1703
UNITED NATIONS COVID-19 RESPONSE AND RECOVERY FUND	1053
COVID 19 RELIEF FUND / LOAN (INVESTMENT) FOR redacted@threatwave.com	575
COVID19 LOAN / BOND INVESTMENT OFFER	492
Public Relation Facebook Covid-19 Lottery Department	439
Fino allï¿½ultimo paziente Covid-19	253
Hello redacted@threatwave.com, Test Covid al mejor precio del mercado. Desde 4,95 euros. Envio inmediato.	244
Congratulations! You are a Covid 19 Benefit Winner !!	226
Recuperacion Efectiva de los Subsidios Laborales ante Essalud Post Covid19 -8 y 9 de Abril	210
Re:Your Covid vaccine is approved for vacination	208
COVID-19 GRANT CUM MEGA MILLIONS LOTTERY	191
Covid Relief Donation -$	165
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	146
COVID-19 Update: We are open and now offering Free Virtual Consultations	146
protective supplies for corona	139
Liquidación de Productos Covid -19	129
BENEFITS PAYMENT SUPPORT FOR COVID-19	126
Seguro COVID19 para la construccion	121
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	103
Ofertas Test Rapido Covid 19	96

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	9043
gmx.net	9018
thusian.click	4945
gmail.com	2410
timesofindia.com	1710
protonmail.ch	1053
rediffmail.com	439
163.com	380
ediscomspa.com	253
app.mailstudio.in	244

Top-15 IPs Sending COVID Spam

195.62.46.95	4945
188.72.187.70	2859
160.202.164.163	2692
157.245.42.150	1749
178.251.230.138	1494
160.202.164.164	1284
83.12.212.149	1053
46.17.95.105	516
103.225.54.197	453
103.225.53.115	405

Top-15 Countries Sending COVID Spam

JP	9122
US	8589
--	5040
AZ	2859
DE	1966
IN	1794
PL	1077
CN	765
GB	700
CA	467

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Mandatory Covid-19 vaccination/Form is attached.	5

Top-15 Subjects Containing doc/xlsx Files

03.31.2021 TeamAmerica ACCOR Press Release COVID 19 Testing and the Environment	4
Comunicato Stampa TEXA | CONFERMATA L'EFFICACIA DEL SANIFICATORE AD OZONO TEXA CONTRO IL COVID-19	4
WG: Durchführung von Antigen-Selbsttests zum Nachweis des Coronavirus SARS-CoV-2 in Schulen ab dem 19.04.2021	2
La Parroquia de La Inmaculada de Alcorcón (Madrid) se protege frente a la Covid 19 con medidores de CO2 para esta Semana Santa	2
External Announcement: DHL Global Forwarding Customer Advisory – COVID-19 ECRS Update 7	1
ho so covid	1
NeuroBo Therapeutics MODERATE & SEVERE COVID-19 INPATIENT STUDY AWARDED	1
Planilla por aislamiento de Covid 19 - Dpto. Ctro. de Análisis de Seguridad (DIP)	1
covid -19 Vaccination Report	1
FW: COVID Fleet & Fuel Exp	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: 154,255
Domains with Potential Mail Servers: 2,552
Email-Capable Domains and Hosts: 50,808
Live Hosts and Domains Not Parked: 43,286

Mobile Apps

Apps in Official Stores: 520

by Store

Apple	257
Google	246
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,266

by Store Type:

Hybrid	1159
Secondary	1040
Affiliate	67

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1