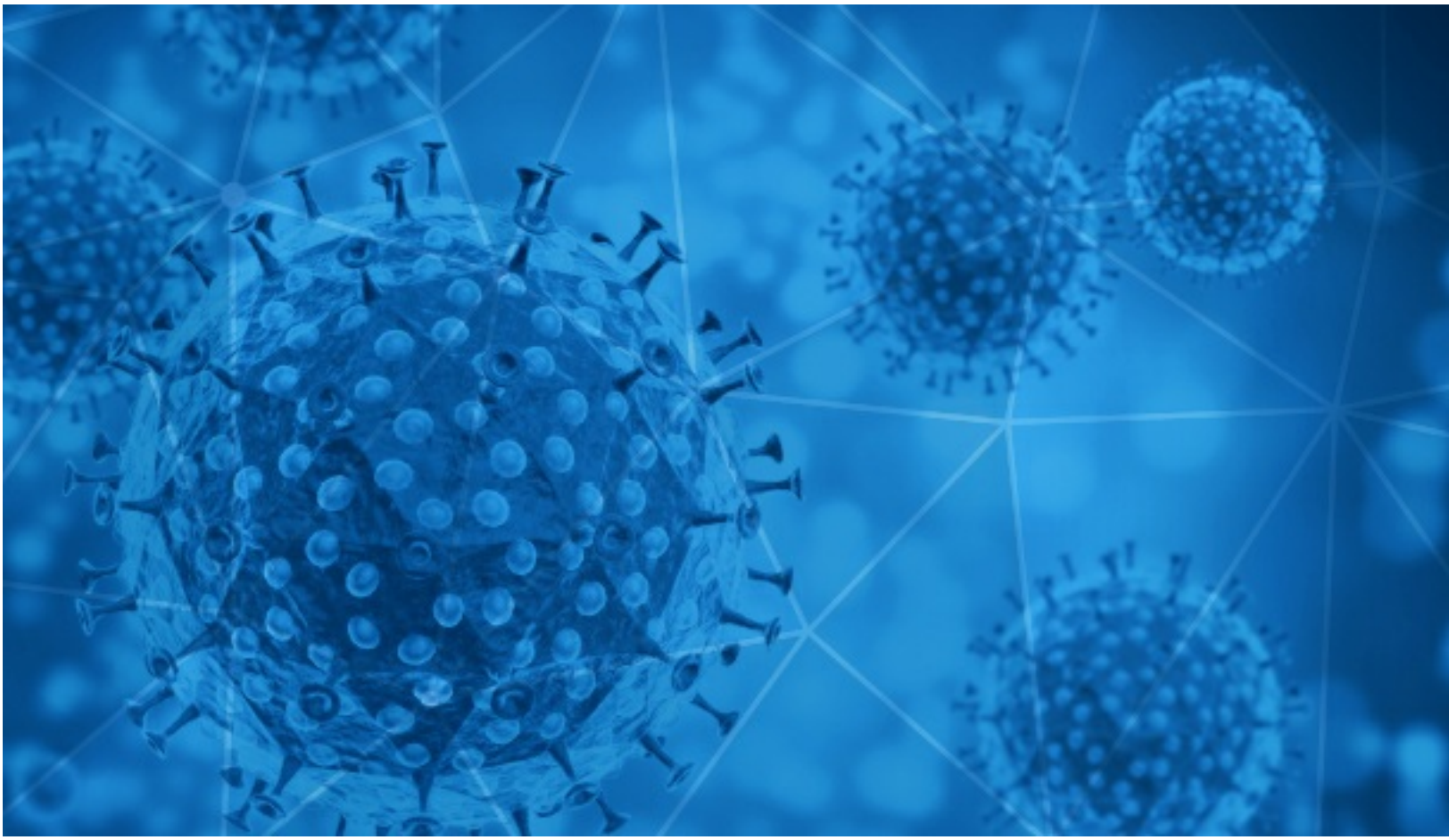
RiskIQ i3:

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

2021-03-09



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 2021-03-08 to 2021-03-09. During this period, RiskIQ analyzed 46,174 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,020 unique subject lines observed during the reporting period. The spam emails originated from 2,105 unique sending email domains and 4,398 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	18511
COVID-relief bill faces final hurdles, Prince Harry and Meghan Markle tell all, and more from Apple News	6998
The Corona Letter: A class divide in the vaccination drive	3690
covid 19 financial support.	1215
Retrogen is now performing diagnostic testing for COVID-19	819
The Morning: A Covid mystery	469
DisposableIsolation Gown-Your best COVID-19 solution	432
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove...etc.	376
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO ANTE EL COVID19	356
Re: Digital signage solution for Covid-19	344
Covid Risk Moving to US on Visa, Denied Re-Entry to US and Other Hot Topics This Week	301
Economic Fallout From COVID Continues □	276
[CND Español - 4352]. Mujer: el futuro post Covid lleva su toque particular	257
Ofertas Test Rapido Covid 19	186
NCJ Daily - Tell Us Your COVID Stories. Zero to Fierce. NCJ Preview. Food Trucks!	183
Coronavirus briefing: Back to school	179
Re: covid-19 touch monitor	178
Why are we not discussing killing Covid in indoor air and on Surfaces?	178
Senate Passes Amended $1.9 Trillion COVID-19 Stimulus Bill	175
covid 19 financial support.	164
COVID19 LOAN RELIEF OFFER / INVESTMENT	150
□Fiscalización Laboral ☝ últimos Cambios en Entorno Covid c	136
Aldi und Lidl vom Ansturm überrascht: Corona-Selbsttests im Einzelhandel nach kurzer Zeit ausverkauft	128
NEW ARTICLE: Vaccination and athletes - why it matters and it's NOT just about covid-19!	126
□Fiscalización Laboral ☝ últimos Cambios en Entorno Covid a	113

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	18513
insideapple.apple.com	7043
timesofindia.com	3690
aim.com	1379
gmail.com	1331
retrogenmail.com	819
nytimes.com	542
126.com	522
asiatic.com.tw	432
163.com	399

Top-15 IPs Sending COVID Spam

27.133.134.102	1379
50.30.46.201	819
103.225.54.15	575
103.225.54.114	567
157.245.42.150	547
103.225.52.115	519
103.225.54.70	425
103.225.52.132	422
103.225.55.214	406
103.225.54.215	401

Top-15 Countries Sending COVID Spam

JP	19963
US	15583
IN	3755
CN	1216
FR	610
DE	605
GB	581
AR	541
TW	438
CA	271

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Fwd: Attestation sur l'honneur COVID-19	1

Top-15 Subjects Containing doc/xlsx Files

Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	10
Prowadzenie postępowania administracyjnego w okresie koronawirusa (COVID-19)	3
Attendance Reminder: Financial Accounting Impact of COVID-19- An In-depth Look at IFRS	3
BLANK covid neg	3
El CGE y el INTA presentan una gran revisión documental sobre la relación de los aerosoles con la propagación del COVID-19 y los mecanismos de protección frente a la enfermedad	3
Buletin de presa 08.03.2021 + comunicat actiuni COVID	2
EDBA Statement on the COVID Impact on ED Operations	2
Clínica móvil vacunación Covid-19	2
IMSS FOTO NOTA.- Más de 180 mil trabajadoras del IMSS están en la primera línea de atención a pacientes COVID-19	2
UNICEF. Día de la Mujer. 10 millones más de niñas corren el riesgo de contraer matrimonio infantil debido a la COVID-19	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: 148,697
Domains with Potential Mail Servers: 2,350
Email-Capable Domains and Hosts: 52,269
Live Hosts and Domains Not Parked: 45,387

Mobile Apps

Apps in Official Stores: 514

by Store

Apple	254
Google	243
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,177

by Store Type:

Hybrid	1106
Secondary	1003
Affiliate	68

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1