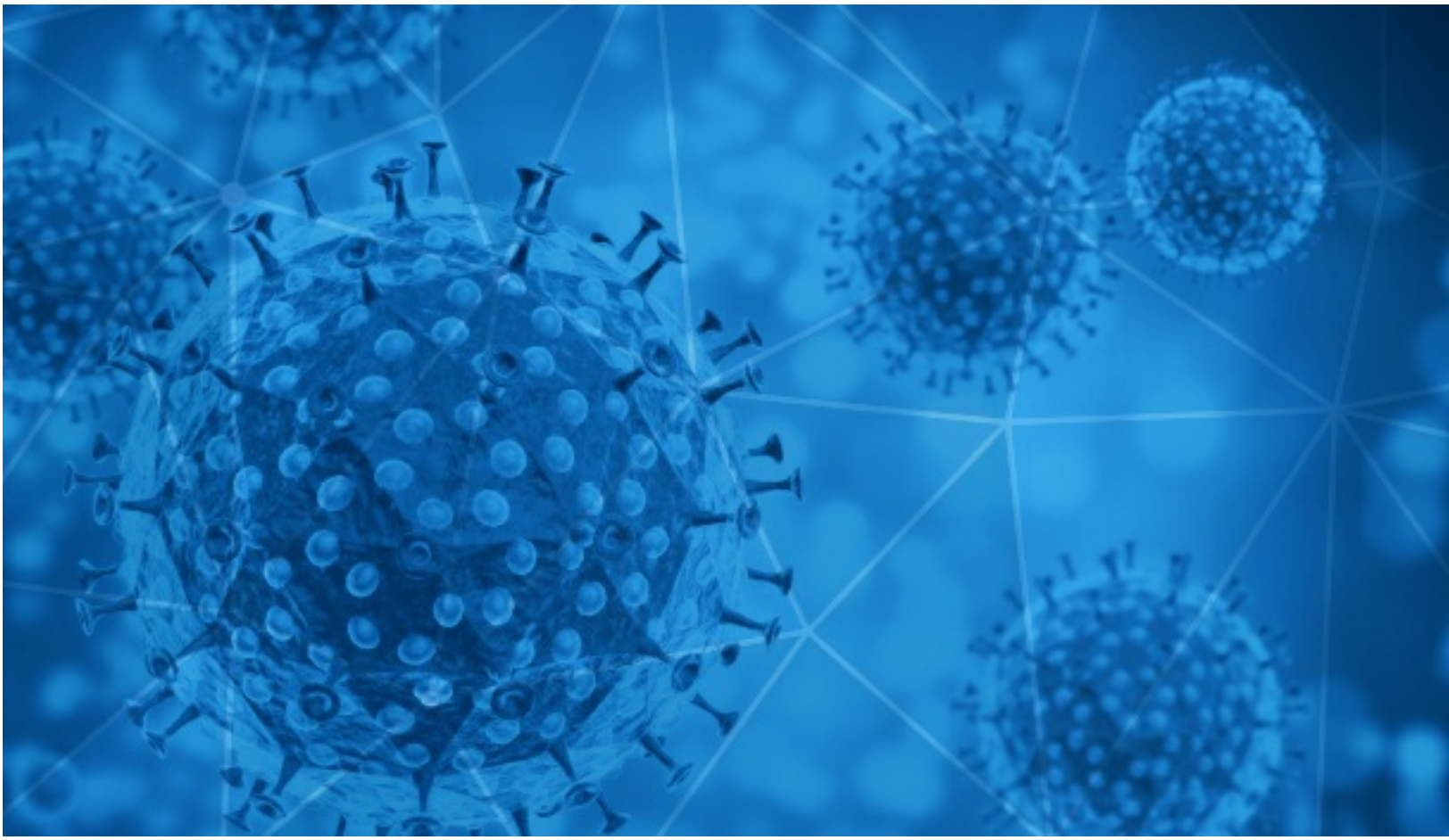
RiskIQ i3:

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

2020-10-14



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 2020-10-13 to 2020-10-14. During this period, RiskIQ analyzed 33,433 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,276 unique subject lines observed during the reporting period. The spam emails originated from 2,112 unique sending email domains and 4,344 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Another vaccine trial paused	3846
Trump and Biden head to battleground states, the first COVID-19 reinfection in the U.S., and more from Apple News	3165
Mamparas de proteccion COVID19	1326
Mamparas de proteccion contra el coronavirus	1292
COVID 19 Donation	1281
Mental Illness, COVID, ADAAA, and the Workplace: Taking Responsibility as an Employer | Presenter-Dr. Susan Strauss	1015
Test de deteccion rapida COVID19	841
Mascarillas y Otros Covid	783
Test rapido para la deteccion del Coronavirus	782
Limpieza y desinfeccion COVID 19	660
COVID-19 Robbing Your Retirement? Get #1 Retirement Playbook [FREE]	603
Equipos de Protección y Prevención del COVID-19	564
Form 941 and 941X with COVID changes	503
Sanitización y Limpieza contra el Covid-19	390
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	386
Protection from Coronavirus and other diseases	354
Evite el coronavirus en su negocio	327
¡Llegaron! Equipos de desinfección UV-C de alta calidad disponibles en Perú | Elimina el Covid-19	312
Re:Corona virus Protection Pills and sex pills.	282
Para Desinfectar y Matar el CoronaVirus con UVC	279
Re: Your Order Corona virus Protection Pills and sex pills.	273
Help to fight COVID-19 fever alarm security door	257
3 days to go | Webinar - Form 941 and 941X with COVID changes	242
Contactless infrared body temperature thermometer defeat Coronavirus	239
Re: Defeat Coronavirus, non contact fever alarm device	215

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

tutanota.com	5213
timesofindia.com	3847
insideapple.apple.com	3166
gmail.com	2060
yeah.net	877
isap.enviador.cl	783
keyable.net	711
126.com	681
e.viewvariant.co	603
focazen.com	564

Top-15 IPs Sending COVID Spam

181.239.232.96	3174
43.239.110.184	1281
201.231.6.62	1176
165.22.32.231	783
113.116.206.208	666
190.247.255.158	624
107.173.152.127	601
67.219.150.138	282
67.219.147.50	273
210.51.26.142	250

Top-15 Countries Sending COVID Spam

US	11091
IN	5372
AR	5361
CN	3218
GB	2137
FR	837
DE	802
ES	444
BE	435
CA	376

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

CUMPLIMIENTO DE PROTOCOLOS DE BIOSEGURIDAD PARA MANEJO DE PANDEMIA CORONAVIRUS - COVID19	8
El CÁNCER DE MAMA: Una amenaza constante que no se detiene ante el COVID-19 - LIGA COLOMBIANA CONTRA EL CÁNCER.	7
PHHS 10 13 2020 End of Day COVID 19 Summary	7
COVID-19 - 3 milhões de testes COVID no mercado Português em menos de 24 horas	5
NP_El Índice de Interconexión Global de Equinix revela el ritmo al que el COVID-19 está acelerando la transformación digital en el mundo	3
COVID-19 e PMA: pubblicato il primo studio che attesta l'assenza del virus in ovociti di donatrici positive - Eugin	3
Fwd: SAVE THE DATE Corso gratuito: CORSO GRATUITO: “IL WEB MARKETING TURISTICO IN EPOCA (POST) COVID E PIANIFICAZIONE AZIENDALE - BUSINESS PLAN”	3
RE: REPORTE COVID PEDREGAL	2
Kopia Załacznik - informacje ws. COVID.xlsx	2
La Covid19 no afecta a la fertilidad femenina ni se transmite a la descendencia	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: 129,239
Domains with Potential Mail Servers: 2,786
Email-Capable Domains and Hosts: 48,287
Live Hosts and Domains Not Parked: 57,453

Mobile Apps

Apps in Official Stores: 460

by Store

Apple	234
Google	211
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,573

by Store Type:

Hybrid	852
Secondary	664
Affiliate	57

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1