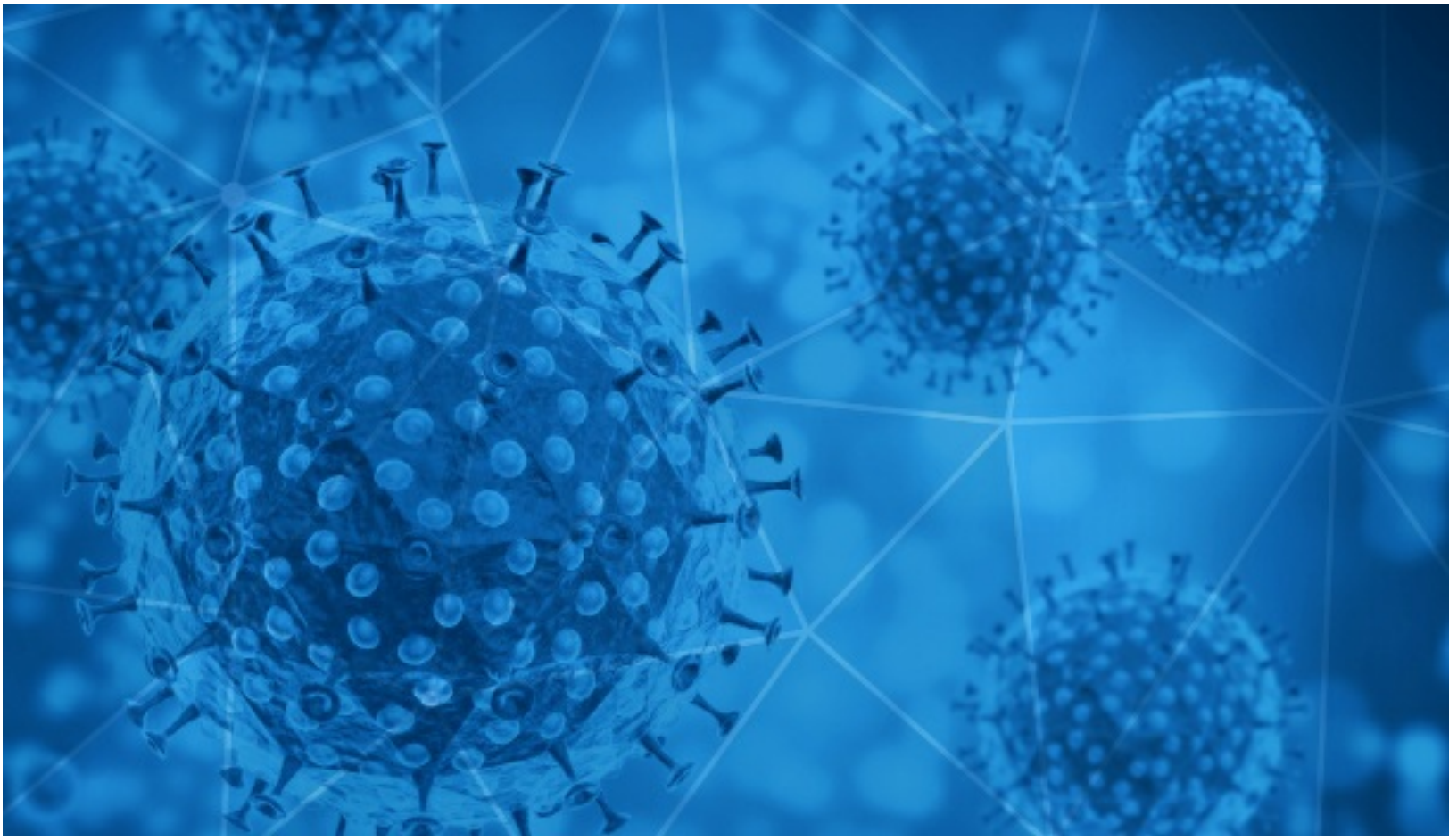
RiskIQ i3:

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

2021-04-23



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 2021-04-22 to 2021-04-23. During this period, RiskIQ analyzed 10,612 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,678 unique subject lines observed during the reporting period. The spam emails originated from 1,180 unique sending email domains and 2,225 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Breakthrough infections rare	1853
Covid passports 'from next month'	439
COVID-19 Update: We are open and now offering Free Virtual Consultations	353
Liquidación de Productos Covid -19	332
RELIEF FUND - COVID 19 INVESTMENT LOAN!	330
You could help advance COVID-19 VACCINE research	327
COVID-19 vaccine research survey	314
Important coronavirus vaccine research survey seeking healthy people 18+	314
COVID-19: PRONTA ATENCIÓN Y AISLAMIENTO	291
DC COVID-19 Community Corps Day of Action	187
Better than COVID Vaccine…	139
protective supplies for corona	128
Covid Relief Donation	117
Formati per la trasformazione digitale post Covid	116
TermoScanner e strumenti DPI Anti-Covid in pronta consegna con sconti oltre il 70% e prezzi a partire da Euro 39,00 + spedizione gratuita. Non Abbassiamo la guardia!!!	112
COVID-19 DONATION FOR YOU! GET BACK TO ME	109
Descarte de Covid-19. Pruebas moleculares, antígeno y anticuerpos. publicidad	99
Re: Your Order corona vaccine Free	97
Board Approved Lists of Staffs for Retrenchment! (Covid-19 Effects)	90
Toma de pruebas COVID19	78
Limpieza Preventiva COVID19	70
LJC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation.	68
Econet Express 501/2021 - COMÉRCIO EXTERIOR - IMPOSTO DE IMPORTAÇÃO - REDUÇÃO TEMPORÁRIA COVID-19 - Aplicação - LISTA DE EXCEÇÕES À TEC (LETEC) - Alteração	59
Chegou a hora de você se vacinar contra a Covid-19!	57
COVID-19 BENEFIT CASH GRANT!!!	54

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	1854
gadgetsology.us	955
gmail.com	923
email3.telegraph.co.uk	440
loanme.com	189
mlog3.cl	188
subscriptions.dc.gov	187
smartsirenx.us	139
itmcsystem.com	133
163.com	128

Top-15 IPs Sending COVID Spam

134.73.142.225	955
101.79.49.106	519
220.158.199.207	139
169.54.168.106	132
112.14.178.70	128
67.219.150.138	127
130.248.205.98	124
219.65.85.22	119
219.65.85.31	116
130.248.205.96	116

Top-15 Countries Sending COVID Spam

US	4016
IN	1990
DE	540
KR	523
FR	442
GB	357
--	309
CN	268
IT	244
AR	232

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

¿Cómo se celebran las juntas de vecinos en la era COVID?_NdP IESA	2
UN Covid 19 Relief fund.	2
Vaccinazioni COVID-19 in Azienda	2
Canceled: Croydon Primary Care Winter Resilience & COVID vaccination planning group	1
Scrum Masters during COVID?	1
HPH COVID-19 Bulletin #290 April 21	1
Sub : Claim Intimation : Mrs. Savitri Devi Mishra : Policy No: 171300/48/2021/ 155009 – Mediclaim Policy Policy No: 171300/48/2021/ 4673 – Corona Policy	1
Planillas Covid	1
COVID -19 VACCINE (SPM LIST)	1
MOUVEMENT U COVID DU 22/04/2021	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: 157,308
Domains with Potential Mail Servers: 2,499
Email-Capable Domains and Hosts: 48,513
Live Hosts and Domains Not Parked: 41,930

Mobile Apps

Apps in Official Stores: 529

by Store

Apple	262
Google	250
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,330

by Store Type:

Hybrid	1189
Secondary	1073
Affiliate	68

Blacklisted Mobile Apps: 32

by Store Type:

Secondary	29
Official	2
Hybrid	1