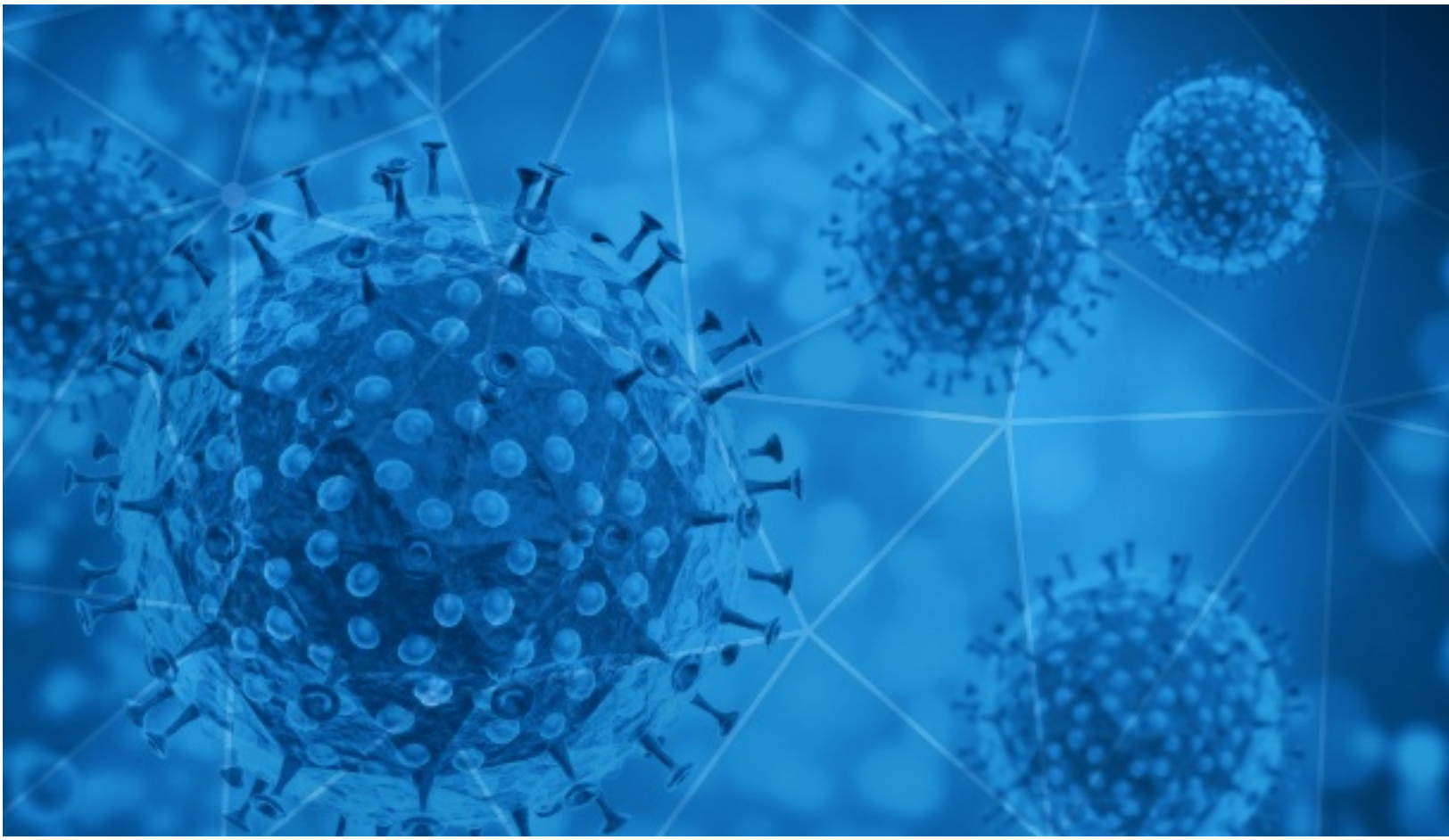
RiskIQ i3:

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

2021-03-25



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 2021-03-24 to 2021-03-25. During this period, RiskIQ analyzed 12,425 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,929 unique subject lines observed during the reporting period. The spam emails originated from 1,307 unique sending email domains and 2,374 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Bless you, common cold	2000
Children in line for Covid jabs	547
LJC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation	482
United Nation Covid .39	416
YOUR COVID-19 STIMULUS PACKAGE WORTH..	375
United Nation Covid .22	332
Seguro COVID19 para la construccion	331
Liquidación de Productos Covid -19	269
RE: COVID-19 RELIEF FUNDS	251
Recuperacion Efectiva de los Subsidios Laborales ante Essalud Post Covid19	246
Retrogen is now performing diagnostic testing for COVID-19	242
Staats Loterij Covid19 Global Fund Relief!	183
Pruebas para Detección de Covid-19 | Clinica Sanens	151
Hello redacted@threatwave.com, Test Covid al mejor precio del mercado. Desde 4,95 euros. Envio inmediato.	148
SARS-COVID-19 Antigen Schnelltest	141
UNDP COVID19	127
Flu/Covid 19 Weekly questionnaire - Reminder week 12	122
Re: Corona virus Protection Pills.Order confirmation	110
Arma tu kit para tus colaboradores y clientes contra el Covid	96
Hi, Just Confirm your Covid Antibody IgG test appointment at Rs 449/- only and get relaxed.	96
Ofertas Test Rapido Covid 19	95
Spolehlivé rychlotesty na COVID-19 a nově zlevněné respirátory	89
Covid19 Relief Fund	77
protective supplies for corona	73
[Earn Credits] Live Longer & Healthier Life w/ 'COVID-19 Diabetes Wellness'!	72

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	2000
yandex.com	771
email3.telegraph.co.uk	610
gmail.com	506
leonenzolawfirm.com	482
aol.com	343
walla.co.il	331
fulda.de	251
euroavisos.com	246
retrogenmail.com	242

Top-15 IPs Sending COVID Spam

51.79.146.45	482
194.76.227.39	416
96.86.106.193	375
213.154.3.45	332
199.217.112.130	242
18.218.79.206	183
190.247.241.5	183
130.248.205.95	183
130.248.205.97	162
130.248.205.96	154

Top-15 Countries Sending COVID Spam

US	4401
IN	2079
FR	925
DE	765
--	639
AR	396
CN	344
AZ	332
IT	270
CA	257

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

UN Covid 19 Relief fund.	7
ACTUALIZACIÓN DERECHOS ADICIONALES PASAJEROS CON RESULTADOS POSITIVO A COVID/ RESTRICIÓN INGRESO	4
(■■■■■■■■■■) ■■■■■■■■■■■ ■■■■■■■■■■■■■■■■■■■■■ ■■■■■■■■■■■■■■■■■■ COVID-19	3
Reminder - COVID Testing on Campus Today	2
REGISTER NOW! Living in an Anxious World: COVID-19, Substance Misuse, and the Impact on Families	2
Fwd: COVID-19	2
Information for your upcoming COVID 19 Vaccination this week	2
planillas covid	1
BCIS Covid19 Case	1
CCS 11734 Se suman 16 decesos por COVID-19 para llegar a 5 mil 600 casos en la entidad	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: 151,092
Domains with Potential Mail Servers: 2,556
Email-Capable Domains and Hosts: 51,261
Live Hosts and Domains Not Parked: 44,724

Mobile Apps

Apps in Official Stores: 519

by Store

Apple	257
Google	245
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,237

by Store Type:

Hybrid	1142
Secondary	1029
Affiliate	66

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1