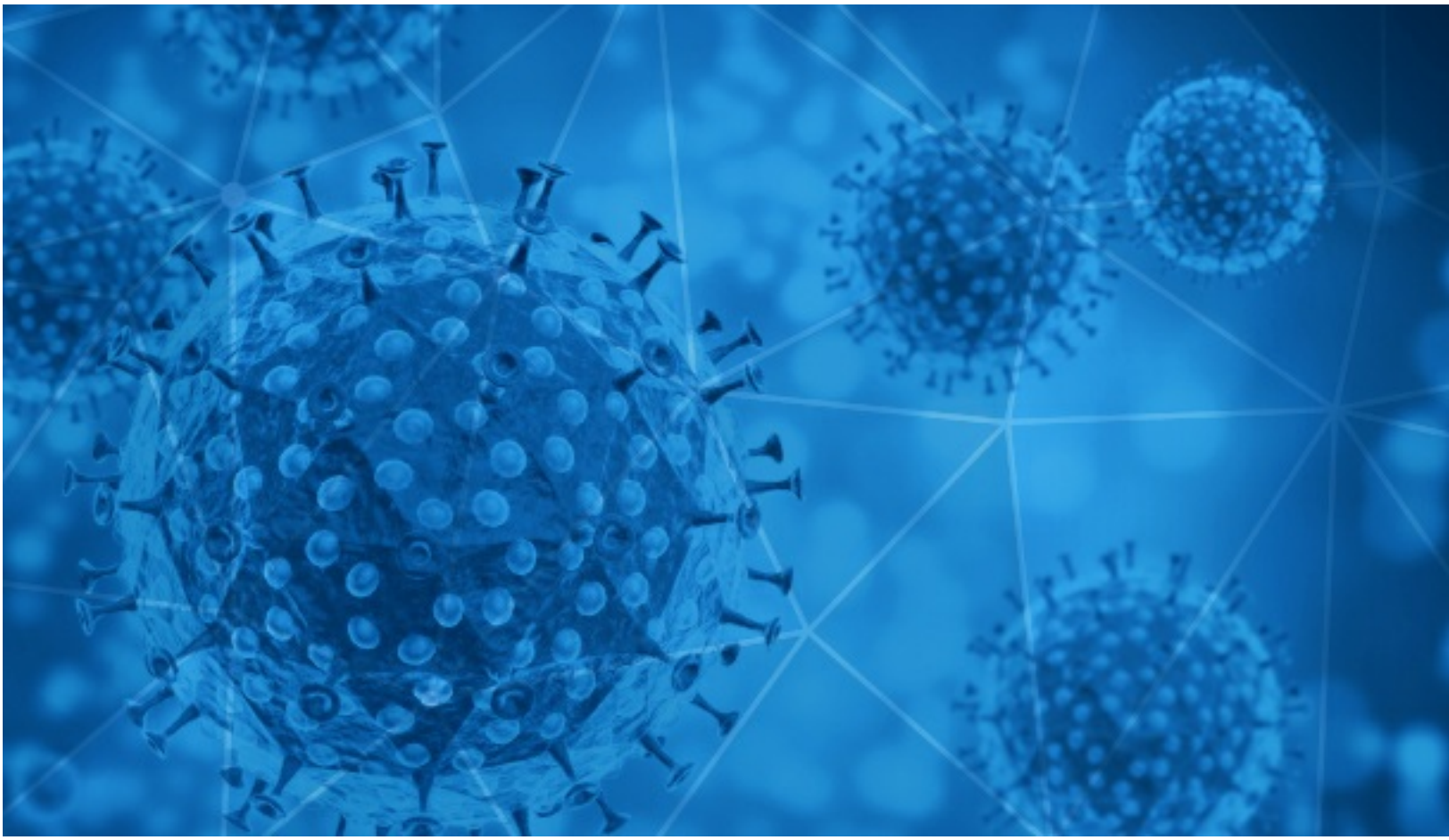
RiskIQ i3:

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

2020-08-11



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 2020-08-10 to 2020-08-11. During this period, RiskIQ analyzed 53,395 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,765 unique subject lines observed during the reporting period. The spam emails originated from 1,824 unique sending email domains and 4,519 unique SMTP IP Addresses. Analysts identified 218 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	18844
U.S. tops 5 million coronavirus cases, inside Trump's eternal reign at Mar-a-Lago, and more from Apple News	4340
TIMES TOP10: Covid's single day death toll crosses 1,000	1825
The Corona Letter: Pandemic and menstrual cycle	1779
Charter Air Service/Fast Air service/Mask /Covid-19 test/Medical equipment	1138
Covid-19 Face Mask	954
Iodine mouthwash protects against Covid-19 + Looting, Unrest Breaks Out in Chicago +Tekashi Attacked	547
Re: Estamos adaptados a la nueva situacion Covid-19	536
Re: Nos adaptamos a la nueva situacion Covid-19	523
Re: Tenemos que adaptarnos a la situacion Covid-19	510
Re: Estamos adaptados a la situacion Covid-19	505
Re: Hay que adaptarnos a la situacion Covid-19	485
Re: Adaptados a la nueva situacion Covid-19	481
Re: Nos tenemos que adaptar a la situacion Covid-19	477
I am glad you stayed safe from the Covid 19 pandemic	471
Re: Hay que adaptarse a la nueva situacion Covid-19	471
COVID 19 LOAN RELIEF	456
Seminario Procedimientos de Fiscalización Laboral, en Covid 19	449
Kit per Test Sierologici Covid -19	441
Seminario Taller Fiscalización de La Dirección del Trabajo en Covid 19	423
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	418
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	416
Especial Covid-19 - Arco Dual Detector de Temperatura y Metales	382
Prevención Covid 19	381
Gestion de Cobranzas y Riesgo Crediticio en Tiempos de COVID con Lineamientos Legales - PROMO 2X3.- Cupos Limitados	356

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

toyotacarrr.com	18848
insideapple.apple.com	4342
gmail.com	2202
bounce.indiatimes.com	1825
timesofindia.com	1780
126.com	1479
oceanbridgecargo.com	1138
hotmail.com	1112
countermail.com	969
seorazor.com	694

Top-15 IPs Sending COVID Spam

103.30.17.20	1138
106.75.37.217	954
113.89.41.239	686
201.231.58.134	565
45.143.222.149	471
38.143.99.76	456
103.225.54.223	426
181.46.136.168	416
103.225.53.183	409
103.225.54.170	387

Top-15 Countries Sending COVID Spam

JP	18914
US	11219
DE	5725
CN	3930
IN	3911
AR	1561
HK	1197
ES	1145
--	902
CL	864

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

QUOTATION FOR COVID 19 PREVENTIVE SUPPLIES, CHANYA ENTERPRISES	214
RV: Coronavirus 96	1

Top-15 Subjects Containing doc/xlsx Files

COVID-19 RELIEF FUNDING	5
covid alert	5
Press Release: IIT Guwahati and RR Animal Healthcare successfully manufactured and commercialised the indigenously developed COVID-19 diagnostic kits	4
Emergenza COVID-19 Appalti e Decreto Semplificazioni (D.L. 76/2020): verso la ripartenza del mercato? Roma 13/10/2020	4
Covid-19 compensation fund	4
Apply Covid-19 Recovery Loan!!!	3
[DIV15] Division 15 Research Grant Opportunity: Education Research in the Time of COVID-19 and Civil Rights and Social Justice Movements	3
Press Release: Country of Norway Relies on Everbridge Public Warning to Alert Citizens Traveling Internationally to Mitigate COVID-19 Risks - Order# 52264013	3
Press Release: IIT Mandi team elucidates and compares the disordered proteins in COVID-19 virus and other coronaviruses through computational studies	2
Line List Form COVID-19 (1)	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: 118,875
Domains with Potential Mail Servers: 2,893
Email-Capable Domains and Hosts: 43,326
Live Hosts and Domains Not Parked: 65,234

Mobile Apps

Apps in Official Stores: 383

by Store

Apple	201
Google	173
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,020

by Store Type:

Hybrid	645
Secondary	333
Affiliate	42

Blacklisted Mobile Apps: 24

by Store Type:

Secondary	21
Official	2
Hybrid	1