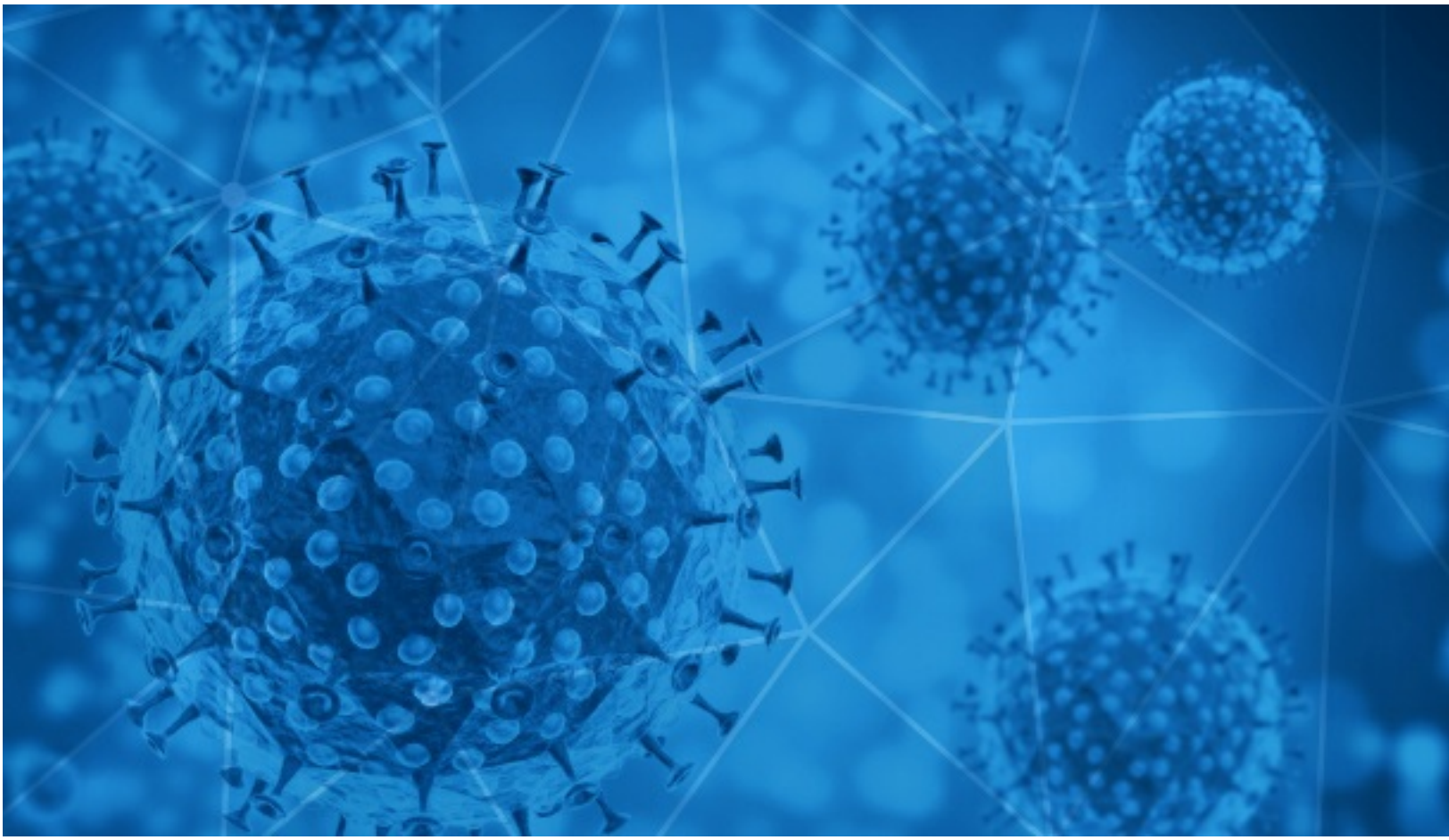
RiskIQ i3:

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

2020-07-02



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 2020-07-01 to 2020-07-02. During this period, RiskIQ analyzed 43,503 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,165 unique subject lines observed during the reporting period. The spam emails originated from 2,247 unique sending email domains and 4,280 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

My COVID-19 Donation.	8685
TIMES TOP10: How bad did the Covid situation get in June?	3518
The Corona Letter: Making sense of an oversupply of research	2791
Fauci gives grim COVID-19 estimate, the coronavirus mutation taking over the world, and more from Apple News	1628
Ya disponible TEST COVID19 en fábrica	1562
Oferta Test Rápidos COVID-19, Mascarillas, Alcohol Gel y Amonio Cuaternario.	1434
Implacable contra el COVID-19 AMONIOX	1156
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	836
MICROSOFT CORONAVIRUS RELIEF FUND	641
Cómo Administrar un Almacén con el Impacto del Covid19	598
COVID-19 - Mobile App Development/ PHP, Magento, Drupal, E-Commerce -etc texelglobal.com	545
BEST way to manifest money in a post-corona world	541
APLICACIÃN PRUEBAS RÃPIDAS COVID-19: CÃ³mo funcionan y cÃ³mo se aplican	533
Secret Corona Cash Manifestation Formula	512
Minimice el Riesgo de contagio del Coronavirus - Validacion Biometrica	502
Webinar on Lay-offs & Salary-cuts due to COVID-19 - Register now!	463
Korea Trend News-COVID19(4)	404
COVID-19 RELIF FUNDS OF £5,950 million	374
Productos Covid 19 - Entrega Gratis RM	314
Extra editie: Richtlijnen voor gebruik airco in coronatijden	301
Notification regarding Alternative Evaluation Scheme during COVID-19	296
Re: Supply Protection products against COVID-19	264
Usted ha sido citado para una prueba obligatoria de (COVID-19) .	262
Re: keep away from Covid-19	249
Extra édition: La climatisation en temps de corona	242

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmail.com	10824
bounce.indiatimes.com	3518
timesofindia.com	2791
insideapple.apple.com	1647
brandmed.cl	1562
correosmasivos.cl	1433
126.com	1368
outlook.com	1167
serviciosrentables.cl	1156
halkiredmysdiebtes.us	1053

Top-15 IPs Sending COVID Spam

187.174.101.179	8684
159.89.80.159	1153
194.29.67.14	1052
119.122.91.11	830
5.56.22.141	793
5.56.22.142	767
81.95.112.26	711
51.38.133.70	655
45.237.96.13	641
51.77.33.44	531

Top-15 Countries Sending COVID Spam

US	10714
MX	8745
IN	7873
CN	2753
DE	2513
--	1934
FR	1894
CA	1094
BE	836
GB	610

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

PHHS 6 30 2020 End of Day COVID 19 Response Report	7
BHP – obowiązki pracodawcy i pracownika w dobie Covid 19	6
RV: CUMPLIMIENTO DE PROTOCOLOS DE BIOSEGURIDAD PARA MANEJO DE PANDEMIA CORONAVIRUS - COVID19	6
PROTEGE A TU EMPRESA FRENTE AL COVID	4
CII Online Programme on 'Workplace Precautions during COVID 19' 9 July 2020 : 11.00 am to 1.00 pm	4
NP Aj Sitges - El Sitgestiu Cultural 2020 canvia la fórmula amb propostes de música, cultura i experiències com a fil conductor, adaptades a les mesures de seguretat pel coronavirus	3
Signages # Covid 19- for your Office Space and work place ||	3
El uso de la zona azul de Barcelona crece tras el estado de alarma en ratios superiores a las preCOVID	2
Przypomnienie o szkoleniu online : Dwa lata RODO - podsumowanie najważniejszych regulacji oraz praktyczne zagadnienia dotyczące ochrony danych osobowych w związku z COVID-19	2
Fwd: Información COVID	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: 111,278
Domains with Potential Mail Servers: 2,813
Email-Capable Domains and Hosts: 42,140
Live Hosts and Domains Not Parked: 53,397

Mobile Apps

Apps in Official Stores: 311

by Store

Apple	174
Google	129
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 818

by Store Type:

Hybrid	507
Secondary	275
Affiliate	36

Blacklisted Mobile Apps: 20

by Store Type:

Secondary	19
Official	1