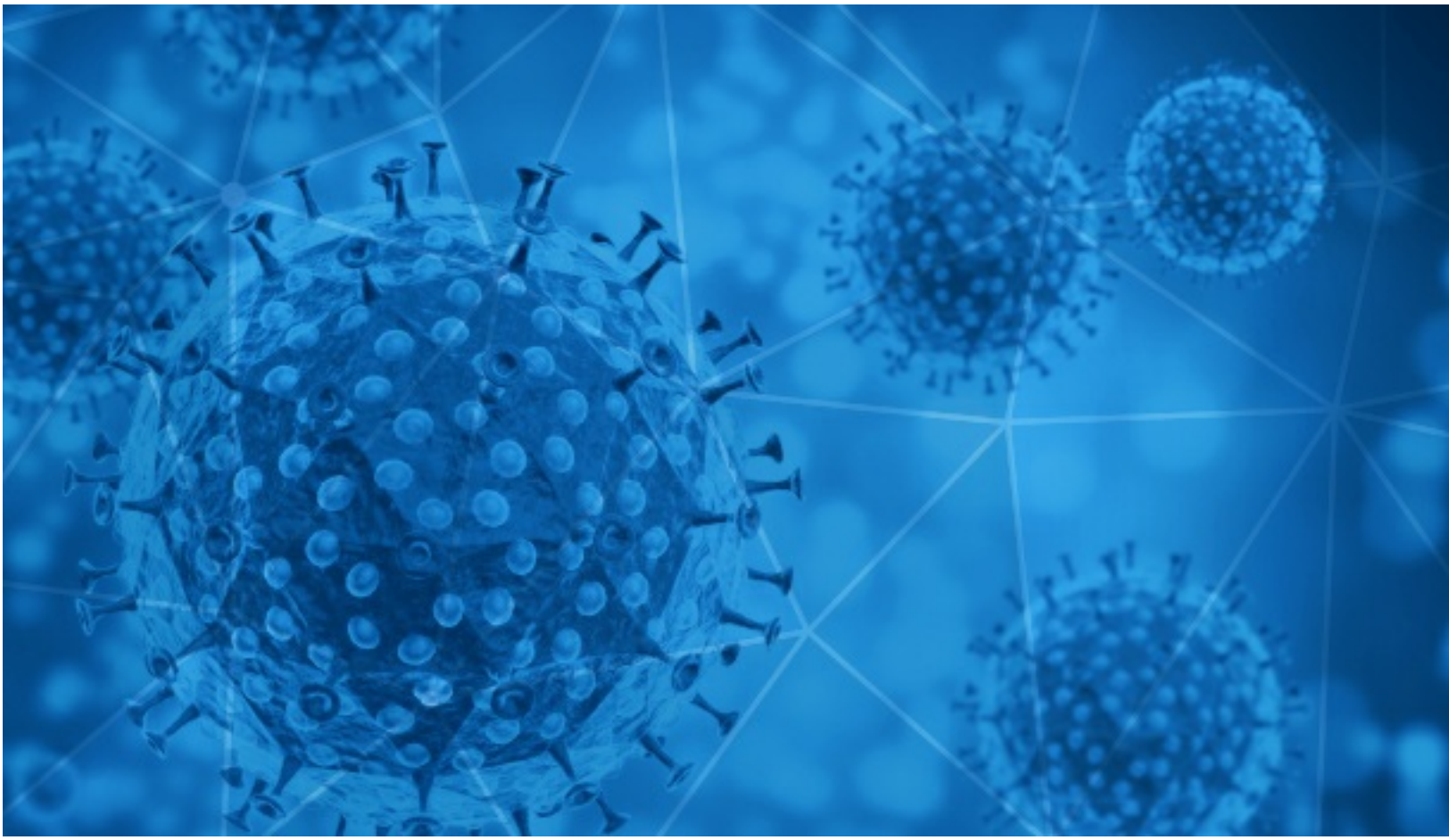
RiskIQ i3:

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

2020-06-17



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 2020-06-16 to 2020-06-17. During this period, RiskIQ analyzed 56,985 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,533 unique subject lines observed during the reporting period. The spam emails originated from 3,170 unique sending email domains and 5,637 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

COVID-19 And Your Credit Health	4836
Standard Bank COVID-19 Payment Relief Funds Approved	4305
Covid-19 Credit Facility Business Owners	4129
Paneles anti Covid-19 para atención de Público.	3850
The Corona Letter: India's elderly caught between a virus and a lockdown	3242
COVID-19 / DONATION FOR YOU	2164
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	1379
COVID-19 - Custom Projects | Mobile Application | SEO !! -etc [REDACTED_DOMAIN]	1125
Calificacion De Origen Laboral Enfermedad Covid-19	1050
STAY SAFE CORONA-VIRUS (COVID 19) IS REAL!!!	971
Test Rapido COVID 19	799
Please stay safe Corona-Virus (Covid 19) is real !!!	743
Productos para la Proteccion del Covid-19	668
Mamparas de proteccion contra el coronavirus	595
Mamparas de proteccion COVID19	580
Fuera Covid 19 - Kit Piso desinfectante + Piso Secante y Amonio Cuaternario	565
Bioseguridad Covid Prevención para su Empresa. [þµ β li c i dAd]	548
Covid 19 urgent Update	514
¿Estás buscando VINIL DE ALTO TRÁNSITO para el distanciamiento social? - Productos ANTICOVID	456
sei sicuro da il COVID19... nell'ambito lavorativo.	423
Navigating Covid-19: Human Resources Enablers	382
Estimado Cliente (COVID-19)	327
Blame the Left for Any New COVID Spikes	313
Soluciones para la prevencion del covid19	304
Hurry! Register for a Free Webinar on 'Learn to Live with COVID-19' on 16th June at 05:00pm by SMC Global & BLK Hospital	302

- CONFIDENTIAL -

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	9871
eservices-laposte.fr	4836
upobps.in	4305
publica20.club	3851
timesofindia.com	3242
countermail.com	2902
y28mail.com	2003
126.com	1951
163.com	1120
ccapacitaonline.com	1050

Top-15 IPs Sending COVID Spam

149.255.35.152	4242
187.174.101.179	4128
160.20.147.106	3850
212.227.254.175	2164
52.49.5.166	1530
207.154.221.139	1050
201.231.6.119	1024
201.231.5.68	979
157.119.122.139	809
119.122.91.33	736

Top-15 Countries Sending COVID Spam

US	17468
DE	5036
IN	4891
--	4452
MX	4272
CN	3857
AR	3101
FR	1681
IE	1578
JP	1387

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

Competency-Based Training Needs Analysis Post Covid-19 I 22-23 July 2020	8
COVID-19 PALLIATIVES BONUS ON PAGA	4
LA COVID-19 DISPARA LA DEMANDA DE SERVICIOS DE FACTURA ELECTRÓNICA Y FIRMA DIGITAL	4
ACTION ALERT: Roanoke Electric Co-op Member-owners need COVID-19 Relief!	3
[EPP3] questionnaire COVID-19 INSERM-Etude EPP3	3
Covid-19 Related Products Price List	3
Αναρτήθηκε στο Διαδίκτυο η απόφαση για τα τουριστικά καταλύματα φιλοξενίας κρουσμάτων covid-19 και δυνατότητας αναστολής συμβάσεων εργαζομένων σε εποχικές τουριστικές επιχειρήσεις.	3
Perú / Covid-19: un Estudio de Abogados avanza en demandas colectivas contra China y la OMS.	2
Updated Covid-19 Protocols and Procedures	2
Kpi Ultrasound Inventory - Covid (itude) or attitude?	2

- CONFIDENTIAL -

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: 107,524
Domains with Potential Mail Servers: 2,714
Email-Capable Domains and Hosts: 41,341
Live Hosts and Domains Not Parked: 41,987

Mobile Apps

Apps in Official Stores: 297

by Store

Apple	167
Google	122
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 690

by Store Type:

Hybrid	417
Secondary	240
Affiliate	33

Blacklisted Mobile Apps: 20

by Store Type:

Secondary	19
Official	1