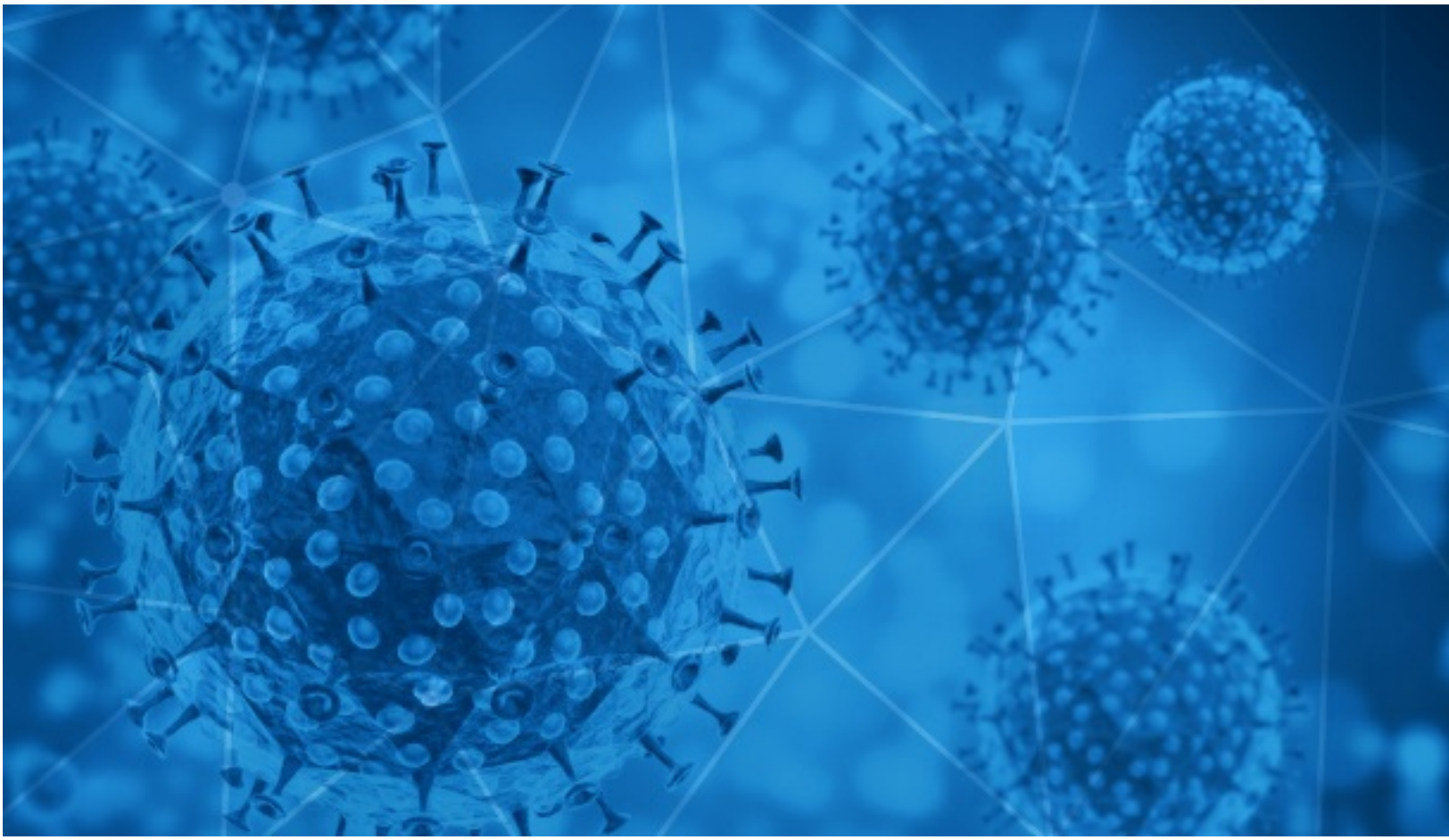
RISKIQ®

RiskIQ i3:

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

2020-06-22



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 2020-06-21 to 2020-06-22. During this period, RiskIQ analyzed 22,760 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,843 unique subject lines observed during the reporting period. The spam emails originated from 1,101 unique sending email domains and 2,646 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

FW: *IMPORTANT* Bulk Quote Request-Covid19	3267
COVID-19 / DONATION FOR YOU	1419
[POSSIBLE-SPAM] Re: COVID-19 (CORONA VIRUS 2020 COMPENSATION FUNDS	1080
The Corona Letter: A drug for mild patients comes to India	985
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	928
Implacable contra el COVID-19 AMONIOX	695
MICROSOFT COVID-19 RELIEF FUND	663
COVID-19 - Custom Projects | Mobile Application | SEO !! -etc [REDACTED_DOMAIN]	645
(COVID-19) - CLAIMS!	559
JUNE: CORONAVIRUS RELIEF FUND	509
COVID-19 Protection Products	424
Re: (COVID-19) - CLAIMS	394
Covid-19 Credit Facility Business Owners	342
Insumos de Protección COVID-19	241
Mamparas de proteccion COVID19	235
Re: Supply Protection products against COVID-19	223
Mamparas de proteccion contra el coronavirus	219
Redeem COVID-19 Financial Relief Funds Today	207
Como volver a la actividad post coronavirus?	203
Credito fiscal COVID para innovacion	201
Mantene tu lugar de trabajo libre de covid19	196
COVID-19 Claim Promo	191
Woensdag 30 graden, maar zwemmen in zee mag niet - Slechts 2 nieuwe corona-overlijdens - Huiszoeking bij weduwe Bende van Nijvel-slachtoffer	191
Evita el Covid19 en tu lugar de trabajo	189
Re: Surgical & Medical Mask for Coronaviruse / China white list Manufacturer	184

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	4312
mail.mil	3267
countermail.com	1581
126.com	1549
yahoo.com	1340
timesofindia.com	985
163.com	933
serviciosrentables.cl	695
websurfer.co.za	695
outlook.com	675

Top-15 IPs Sending COVID Spam

103.140.251.220	3266
212.227.254.175	1419
195.65.28.130	1080
119.122.90.119	807
163.172.75.16	695
159.89.80.159	694
177.23.28.38	508
152.67.129.137	424
201.231.19.121	416
190.247.226.73	386

Top-15 Countries Sending COVID Spam

US	4095
--	3643
CN	3044
IN	1906
DE	1700
AR	1637
CH	1083
TR	966
FR	953
BR	541

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Annexe reglement interieur Covid 19 Camping Clos du hym ***	1

Top-15 Subjects Containing doc/xlsx Files

ANC Weekly COVID-19 Reports	24
COVID-19 RELIEF FUNDING	6
PHHS 6 19 2020 End of Day Report for COVID 19	2
COVID-19 Joint Panel Information - Faith Community Town Hall Materials	2
Webinar: Peripheral Nervous System complication of COVID-19 and Management principles	2
COVID-19	1
DECESO POR COVID-19	1
Admitted covid 19 patient details of 20/06/2020 08am to 21/06/2020 08am	1
Press Release: Viafet, one of the leading Genomics Laboratories, is offering Covid-19 testing	1
planilhas covid att 21-06	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: 108,499
Domains with Potential Mail Servers: 2,736
Email-Capable Domains and Hosts: 41,559
Live Hosts and Domains Not Parked: 45,061

Mobile Apps

Apps in Official Stores: 300

by Store

Apple	170
Google	122
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 738

by Store Type:

Hybrid	452
Secondary	252
Affiliate	34

Blacklisted Mobile Apps: 20

by Store Type:

Secondary	19
Official	1