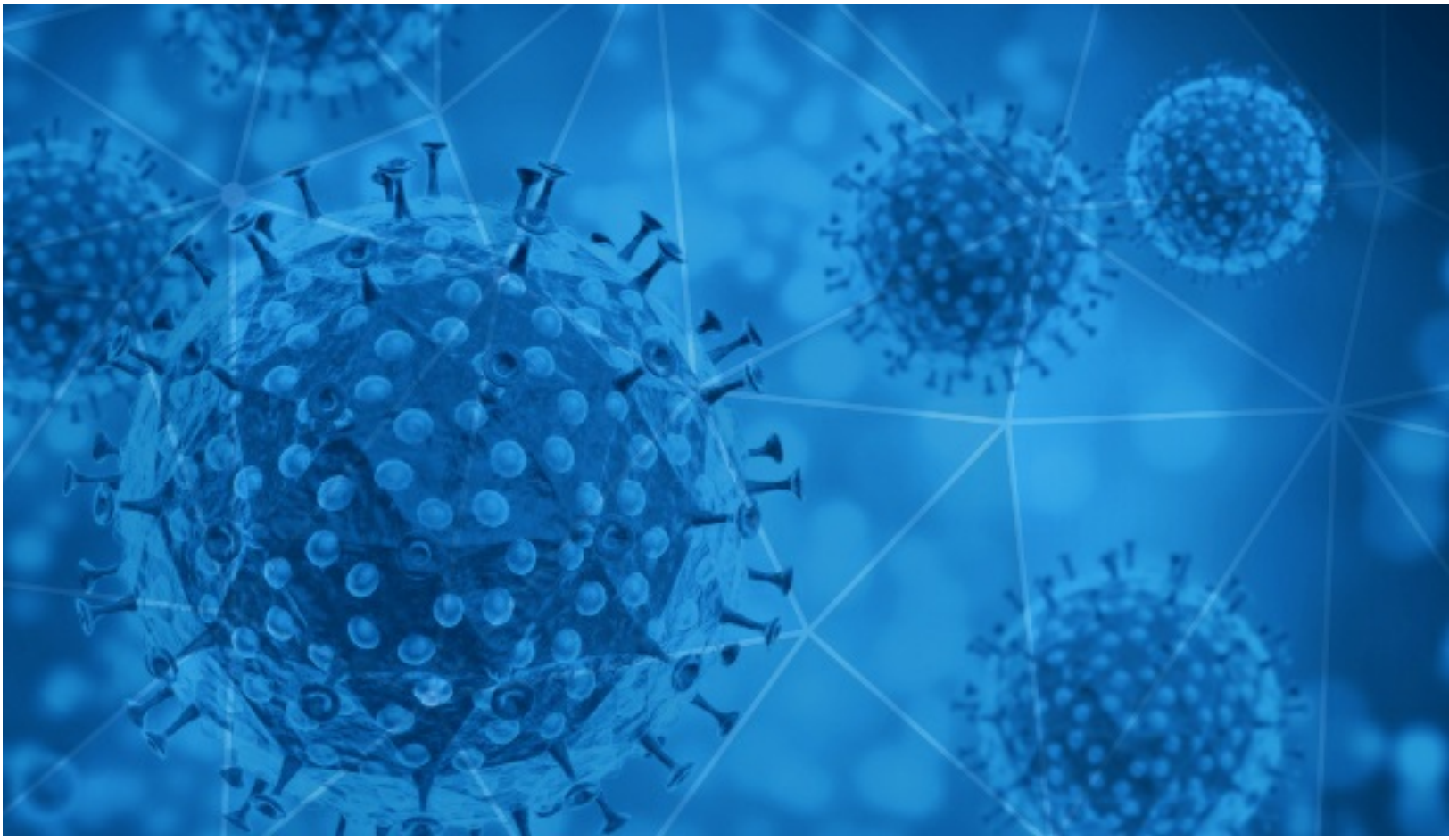
RISKIQ®

RiskIQ i3:

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

2020-09-28



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 2020-09-27 to 2020-09-28. During this period, RiskIQ analyzed 17,032 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,589 unique subject lines observed during the reporting period. The spam emails originated from 644 unique sending email domains and 1,850 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

US records highest number of COVID cases in a single day+Kentucky's AG Defend Cops Who Killed Taylor	1453
The Corona Letter: Why do some fall severely ill to Covid?	1270
My COVID-19 Donation	1210
Videos para la prevencion de Covid	826
Prevencion de covid19	814
Test de deteccion rapida COVID19	801
VENETO: operativo il Fondo Anticrisi attività produttive, per la concessione di finanziamenti agevolati alle imprese coinvolte nella crisi da COVID-19, per iniziative finalizzate alla realizzazione di investimenti e interventi di supporto finanziario	513
COVID-19 FUND	481
BEST way to manifest money in a post-corona world	361
COVID-19 KILLED ANTHONY	338
Secret Corona Cash Manifestation Formula	326
Mamparas de proteccion contra el coronavirus	283
Help to fight COVID-19 fever alarm security door	271
Mamparas de proteccion COVID19	270
Re:$500,000.00 Covid-19 Pandemic Relief	250
Incontri online in Italia (no corona)	226
Kasus Covid-19 Meningkat Lagi. Cek Tips Dokter Joy!	199
- Compensation / Grant For Everyone Affected By (COVID-19) Pandemic -	183
Re: Covid-19 acrylic protect shield	174
Re: Covid-19 acrylic protect shield	159
Re: Re: Covid-19 acrylic shield	158
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	152
Re: Your Covid-19 Relief Fund®	151
El turismo gastronómico después de la COVID-19	137
Fight COVID-19 / Cash Donation	137

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

countermail.com	2993
gmail.com	2164
caribbeanfever.com	1457
timesofindia.com	1270
126.com	771
manifmagicpro.com	687
yeah.net	604
hotmail.com	536
italiacontributi.it	513
executivemail.co.za	481

Top-15 IPs Sending COVID Spam

190.247.226.120	1545
43.239.110.184	1108
63.83.76.70	686
46.254.37.34	513
82.223.24.217	481
147.91.193.2	404
112.49.34.2	361
190.247.254.68	315
190.247.227.93	262
201.231.10.71	261

Top-15 Countries Sending COVID Spam

US	4100
AR	3010
CN	2622
IN	2530
ES	597
IT	539
DE	511
--	483
RS	404
CL	255

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

ANC Weekly COVID-19 Reports	17
CCS/10118: Suman1,377 fallecimientos y 15,090 los casos confirmados de COVID-19	2
Covid19 update and Price change	2
ARCOVID19 - Close Contact Packet	2
COVID -19 DUTY SCHEDULE OF DNB/CPS RESIDENTS	2
Fwd: PANGENOMICS_COVID 19_MEHSANA_27-9-2020	1
Confirmed Case of Covid 19	1
Ενημέρωση για COVID-19 από το Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών (27/9/2020)	1
Nota de Prensa: ADN realiza 8vo operativo de prevención y pruebas COVID19	1
Reminder: COVID Screening	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: 127,035
Domains with Potential Mail Servers: 2,898
Email-Capable Domains and Hosts: 48,028
Live Hosts and Domains Not Parked: 70,282

Mobile Apps

Apps in Official Stores: 435

by Store

Apple	220
Google	200
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,475

by Store Type:

Hybrid	813
Secondary	607
Affiliate	55

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1