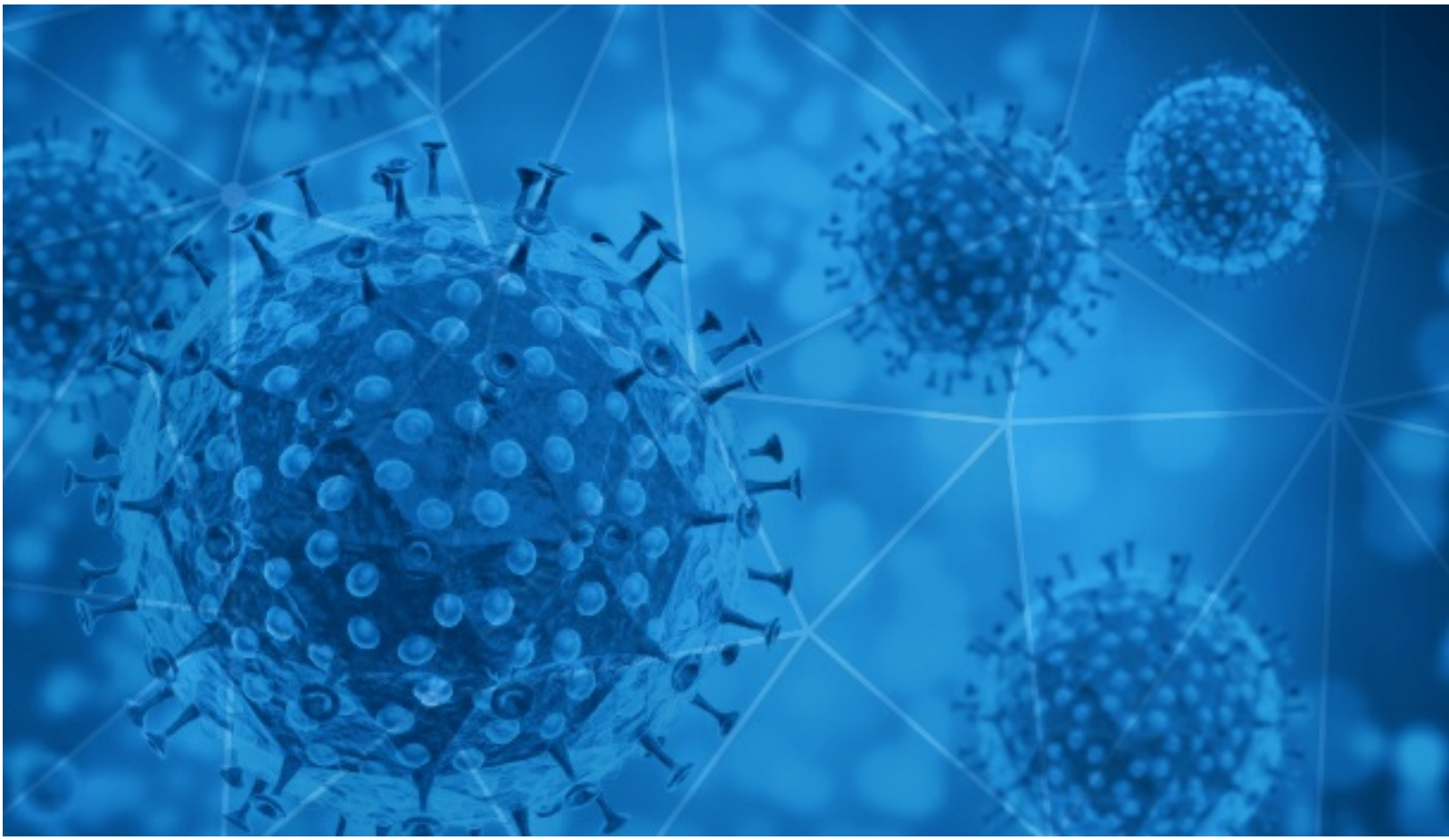
RiskIQ i3:

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

2020-07-30



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 2020-07-29 to 2020-07-30. During this period, RiskIQ analyzed 47,545 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 5,152 unique subject lines observed during the reporting period. The spam emails originated from 2,051 unique sending email domains and 4,299 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: How to equitably distribute a vaccine?	2310
YOU ARE LUCKY WINNER OFPALLIATIVE PROMO OF COVID19	1113
PyMEs contra el COVID19	963
(Webinar) Lay-offs & Salary-cuts due to COVID-19 - Register now!	796
Due to Covid 19 Pandemic , you and your family have been selected to receive (£1,000,000.00 British Pound) charity donation/grant.	745
Wearing a KN95 mask is your best defense against coronavirus	624
31 de studii despre Criza COVID-19, din perspectivă legală	592
Covid 19 Wohltätigkeitsfonds	543
Super Promociones Julio - Proteccion COVID-19	494
IMFC Covid 19-Zuschuss!	365
Soluciones para la prevencion del covid19	357
Como volver a la actividad post coronavirus?	342
Cabinas para la prevencion del coronavirus?	341
2020 COVID-19 Scholarships at University of Minnesota + Fordham University – USA + Others	315
RE: Assess your employees, Conduct Online skill tests to engage them on healthy competetion during covid times	308
Protección contra el Covid19	302
Eliminar Covid-19	281
MICROSOFT COVID-19 RELIEF FUND - GLOBALGIVING	265
Let’s fight together to get through the COVID-19	261
Proteção do COVID-19	257
Test Rapido COVID 19	240
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	227
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	224
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	211
□ - SII- Emergencia de salud Covid-19 81765	211

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

cl.jooble.org	18612
gmail.com	2981
timesofindia.com	2310
countermail.com	2003
stone.com.br	1592
dpt-awardprize.com	1113
126.com	1065
naukri.com	847
trendingtopic.cl	739
hotmail.com	710

Top-15 IPs Sending COVID Spam

150.109.54.114	1113
201.231.6.193	1054
200.89.73.38	880
45.127.62.47	877
45.118.134.118	704
142.11.218.87	623
85.204.79.10	592
201.134.139.73	576
201.231.6.201	502
119.122.88.223	438

Top-15 Countries Sending COVID Spam

CA	17552
US	8860
IN	3636
CN	3286
AR	2270
FR	1339
CL	969
TH	895
SG	894
MX	793

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

Safety, Security at Work Training(Post Covid 19 Preparedness Course)	10
IMSS FOTO NOTA. Personal del HGR No. 46 del IMSS en Jalisco celebra cumpleaños a paciente con COVID-19	3
CUMPLIMIENTO DE PROTOCOLOS DE BIOSEGURIDAD PARA MANEJO DE PANDEMIA CORONAVIRUS - COVID19	3
[ogp] FW: Call for EOI: The Covid 19 Fund.	2
Corona maatregelen	2
BHP – obowiązki pracodawcy i pracownika w dobie Covid 19	2
FW: COVID Regulations Updated information for NSW Businesses	2
CARLOMARIA | oggi alle 19.30 in diretta streaming per RISING WAR\tCHILD UK,\tuna raccolta fondi in aiuto dei bambini che vivono nelle zone di\tguerra e con il Coronavirus	2
Data Covid 19 PT. DRP Periode 29 Juli 2020	1
covid-19 protocols	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: 116,777
Domains with Potential Mail Servers: 2,857
Email-Capable Domains and Hosts: 44,105
Live Hosts and Domains Not Parked: 65,100

Mobile Apps

Apps in Official Stores: 361

by Store

Apple	190
Google	162
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 931

by Store Type:

Hybrid	598
Secondary	294
Affiliate	39

Blacklisted Mobile Apps: 23

by Store Type:

Secondary	20
Official	2
Hybrid	1