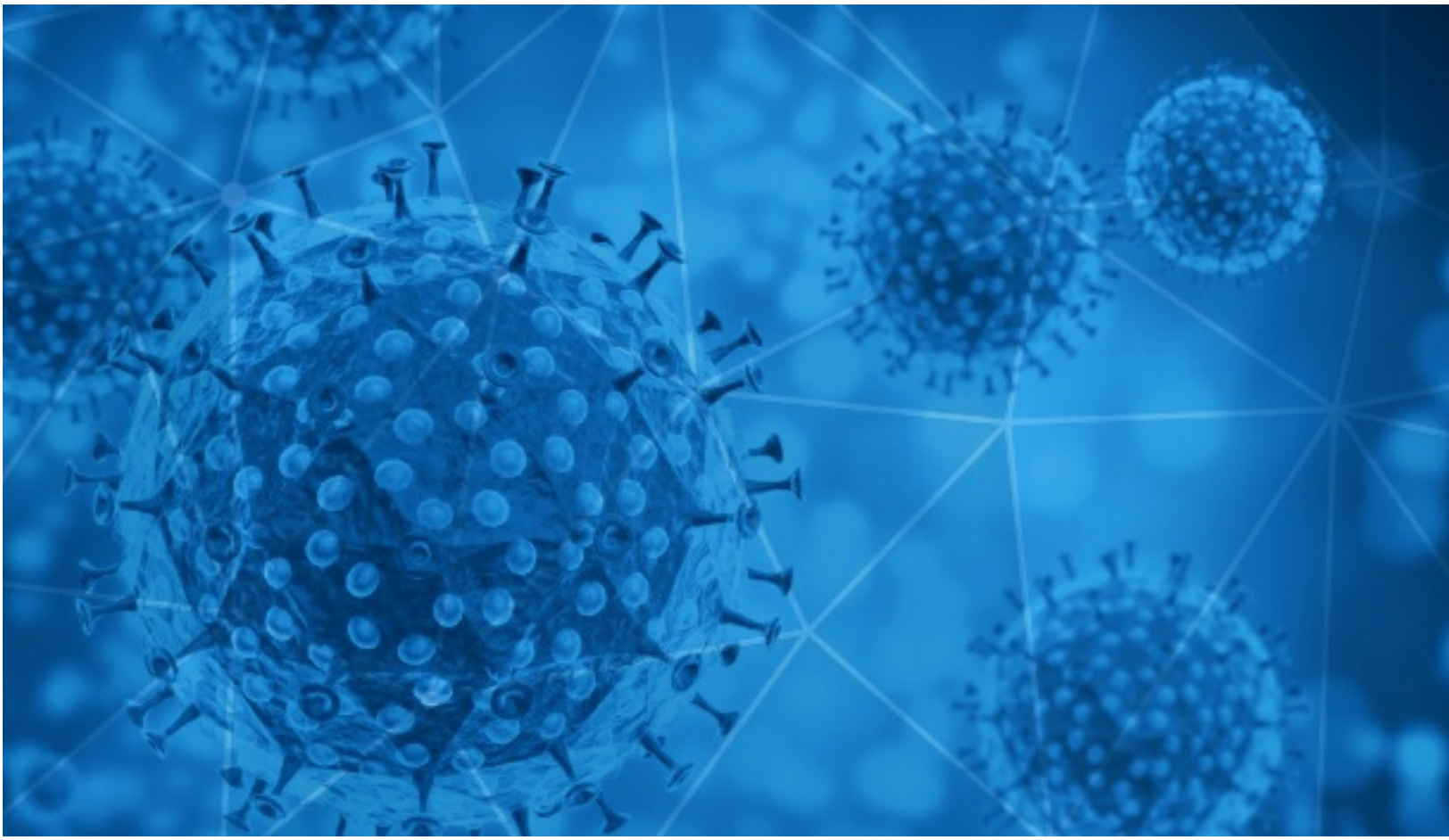
RiskIQ i3:

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

2020-09-23



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 2020-09-22 to 2020-09-23. During this period, RiskIQ analyzed 25,505 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,393 unique subject lines observed during the reporting period. The spam emails originated from 1,709 unique sending email domains and 3,621 unique SMTP IP Addresses. Analysts identified 42 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: What 'recoveries' don't say about Covid-19's spread	4062
How Investment Guru Ray Dalio Recommends Protecting Against COVID-19	1388
Help to fight COVID-19 fever alarm security door	1142
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	976
Reife Frauen zu Corona-Zeiten treffen	832
Insumos protección covid	719
My COVID-19 Donation	711
Test de deteccion rapida COVID19	648
face mask against COVID-19	521
Videos para la prevencion de Covid	498
Про що роботодавець може просити в часи COVID-19, а про що — ні, 3 правила суперечок на співбесіді	474
Prevencion de covid19	435
IMPORTANT Bulk Quote Request-Covid19	350
Re: COVID-19 - E-Commerce Website | SEO (Results Guaranteed) - [REDACTED_DOMAIN]	310
Register Now | Most in-demand jobs and skills amid COVID - 19	305
Fix your Covid Antibody IgG + IgM appointment at Rs 750 only and get report within 24Hrs.	286
Attn: Covid19 Economic Assistance Program	234
Covid-19 Rapid Test Kits	213
Mamparas de proteccion contra el coronavirus	212
Mamparas de proteccion COVID19	193
О чем работодатель может просить во времена COVID-19, а о чем — нет, 3 правила споров на собеседовании	187
HKTDC Export Index 3Q20: Exporter Confidence Rallies Moderately While Spectre of Covid-19 Still Looms Large	187
Re: COVID-19 - Website Maintenance | SEO (Results Guaranteed) [REDACTED_DOMAIN]	186
Covid 19 Relief Fund Promo.	168
Re: Covid-19 acrylic protect shield	153

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	4062
gmail.com	2193
countermail.com	1986
lioei.cam	1388
126.com	1345
keyable.net	1142
data2web.de	832
tie.cl	719
yeah.net	688
work.ua	661

Top-15 IPs Sending COVID Spam

95.141.25.165	1388
190.247.223.11	1212
113.116.205.95	1069
46.20.37.30	832
190.22.144.113	719
43.239.110.184	711
190.247.240.114	528
119.122.90.244	515
103.153.78.33	349
219.65.85.27	245

Top-15 Countries Sending COVID Spam

IN	5972
CN	4364
US	3972
AR	2026
GT	1388
DE	1204
UA	901
CL	807
BE	533
FR	531

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

***IMPORTANT* Bulk Quote Request-Covid19**	40
*****UNCHECKED*** *IMPORTANT* Bulk Quote Request-Covid19**	1

Top-15 Subjects Containing doc/xlsx Files

covid 19 pay out	5
CII Virtual Session on "How to Reboot Manufacturing Post Covid-19 Impact? Using the AI/ Digital Technology" : 30 September 2020	3
LA CRISIS DEL CORONAVIRUS OBLIGA A POSTERGAR DE NUEVO LA XVI EDICIÓN DE FISAHARA	3
Οι ψηφιακά ώριμες μικρομεσαίες επιχειρήσεις σε καλύτερη θέση να αντιμετωπίσουν τις επιπτώσεις του COVID-19	3
Profesjonalny sekretariat w dobie pracy zdalnej / BHP w dobie Covid19	3
Анализ на COVID-19 + антитела за 2 суток (КП во вложении)	3
DECLARACION JURADA CORONAVIRUS	2
Parent Memo 20200922 COVID update	2
RE: Covid Travel Restrictions - update	2
KOMUNIKATË PËR SHTYP: 20,000 Euro donacion për kompletimin e sallës së lindjes për gratë me Covid-19	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: 126,505
Domains with Potential Mail Servers: 2,939
Email-Capable Domains and Hosts: 47,829
Live Hosts and Domains Not Parked: 71,197

Mobile Apps

Apps in Official Stores: 422

by Store

Apple	213
Google	194
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,428

by Store Type:

Hybrid	798
Secondary	575
Affiliate	55

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	25
Hybrid	2
Official	2