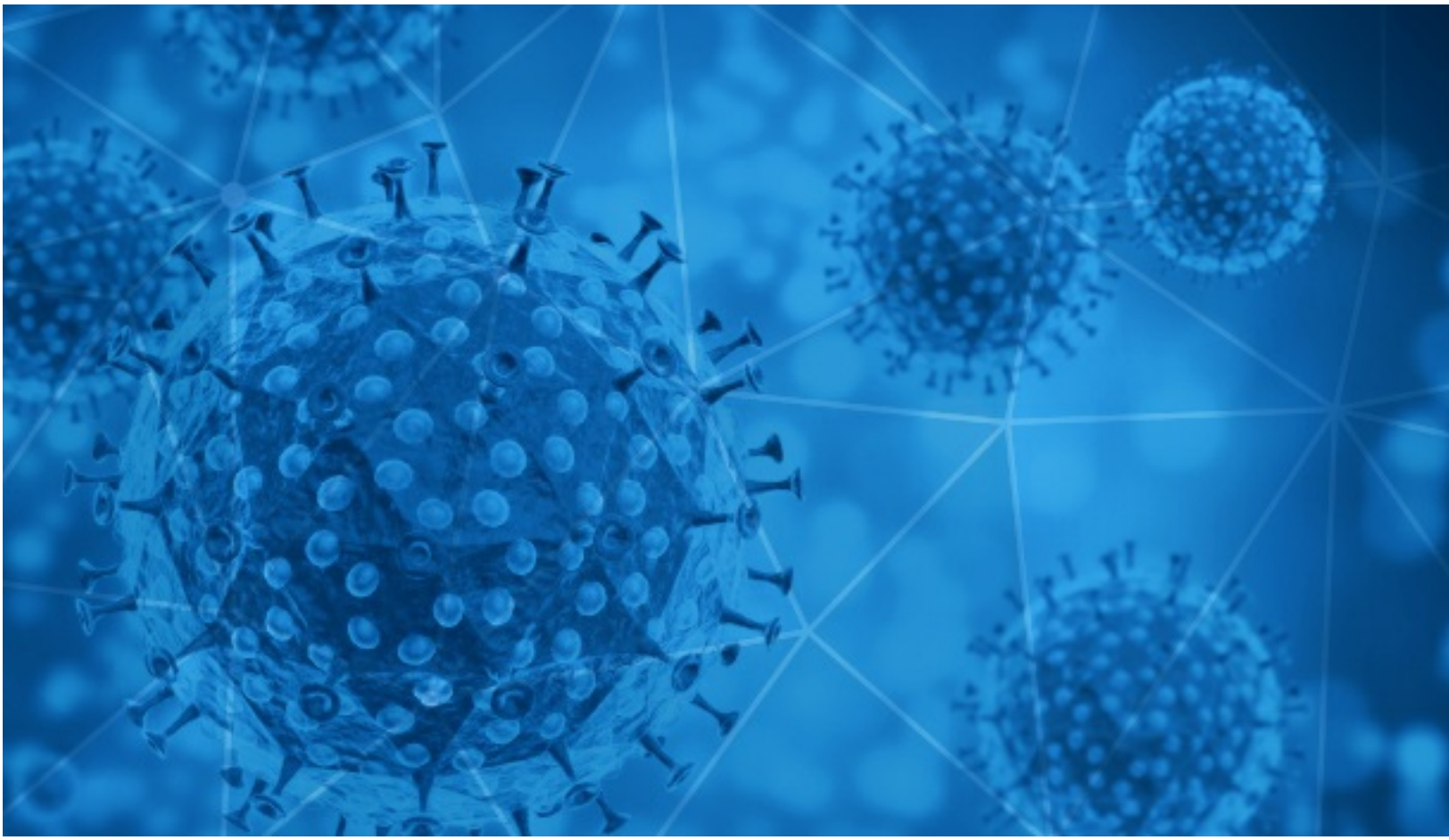
RiskIQ i3:

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

2020-09-11



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 2020-09-10 to 2020-09-11. During this period, RiskIQ analyzed 28,053 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,857 unique subject lines observed during the reporting period. The spam emails originated from 1,954 unique sending email domains and 3,926 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Plasma therapy is no silver bullet	3411
Covid-19 Rapid Test Kits	1716
Nechcete do karantény? Potřebujete anti-covid 19 respirátor!	1362
Coronavirus (covid 19).Relief Bailout	1237
Cuidate del COVID19 con nuestros productos	1133
REQUIRED COVID19 MEDICAL SAFETY PPE	876
4 teachers DEAD from COVID since start of school + White Professor Who Pretended to Be Black Resigns	864
My COVID-19 Donation	472
Re: Defeat Coronavirus, non contact fever alarm device	464
Contactless infrared body temperature thermometer defeat Coronavirus	461
Traitors: Democrats Nuke COVID Relief Bill...Again	416
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	330
Ante el elevado riesgo de contagio por Coronavirus en Perú.	322
COVID-19 LATEST NEWS	307
Bryo Contra Covid19	254
Nuevo catálogo de productos anti-COVID 2020	252
Fix your Covid Antibody IgG + IgM appointment at Rs 750 only and get report within 24Hrs.	218
Precios Imbatibles / Productos COVID 19	198
Let’s fight together to get through the COVID-19	196
Direct client is actively hiring for Data Scientists -Remote till Covid-19 subsides - 3 openings	185
Covid 19: Versicherungsleistung	185
Productos Covid-19	183
Employment opportunity amid covid-19 pandemic	170
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	169
Preparing for CAT 2020 Amid COVID-19 Pandemic	165

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	3412
gmail.com	2335
sinosa.co.za	1716
donatela.site	1362
126.com	1349
hbbcustomercenter.com	1240
countermail.com	1133
keyable.net	925
medicproduction.com	876
caribbeanfever.com	864

Top-15 IPs Sending COVID Spam

194.8.253.148	1362
177.136.47.226	1217
139.99.133.125	876
113.116.204.179	859
190.247.227.41	722
43.239.110.184	471
192.52.167.213	347
192.169.7.168	340
96.44.135.92	336
181.46.136.168	330

Top-15 Countries Sending COVID Spam

US	7216
IN	4399
CN	3054
AR	1505
CZ	1378
BR	1326
AU	913
DE	909
FR	851
GB	796

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

PHHS 9 9 2020 End of Day COVID 19 Summary	7
Dokumentacja pracownicza w dobie COVID 19 - szkolenie on-line	7
NP Crece la venta online de carne en España pese al COVID-19	4
Precizări de presă privind actualizarea listei „zonelor de risc“ stabilită de autoritățile germane în contextul pandemiei de COVID-19 - 10 septembrie	4
NdP FAMMA denuncia que bajo la excusa del COVID-19 los alumnos con discapacidad son excluidos	3
CCS / 9944: Suman 1,252 fallecimientos y 13,071 casos confirmados de COVID-19 en el estado	2
Este 29 de Setiembre!: Contratos laborales y cláusulas contractuales para el sector construcción en tiempos de COVID-19 .	2
Índice EcoVadis: Las empresas españolas mejoran sus resultados en sostenibilidad a pesar de la crisis de la COVID-19	2
RV: ACTUALIZACION INFORMACION COVID-19	2
COVID 19 Notification Letter 9/9/20	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: 123,702
Domains with Potential Mail Servers: 2,970
Email-Capable Domains and Hosts: 45,887
Live Hosts and Domains Not Parked: 68,892

Mobile Apps

Apps in Official Stores: 412

by Store

Apple	211
Google	186
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,303

by Store Type:

Hybrid	759
Secondary	491
Affiliate	53

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	25
Hybrid	2
Official	2