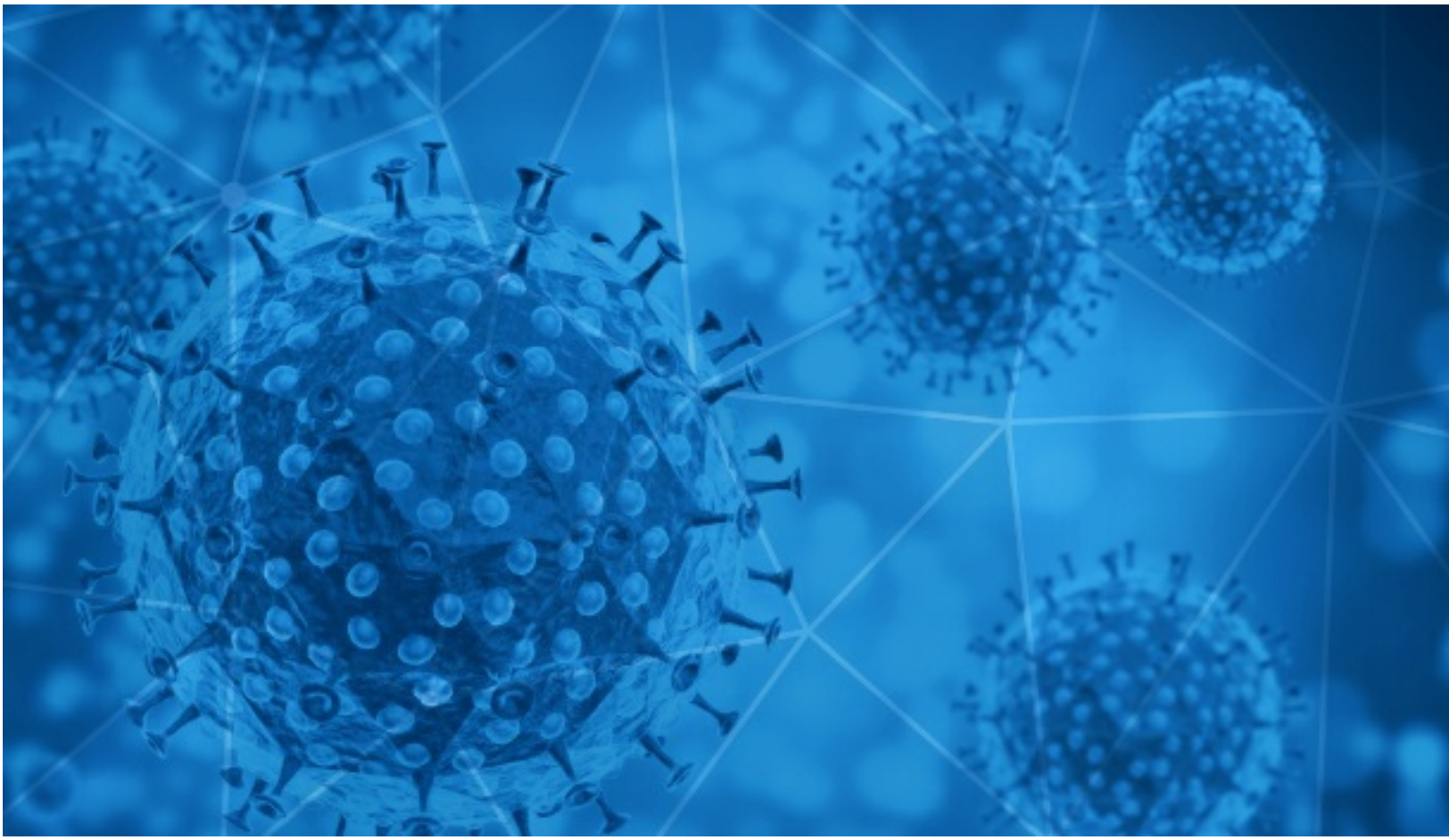
RiskIQ i3:

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

2020-09-22



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 2020-09-21 to 2020-09-22. During this period, RiskIQ analyzed 29,048 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,913 unique subject lines observed during the reporting period. The spam emails originated from 1,412 unique sending email domains and 2,949 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

Hay que adaptarnos a la situacion Covid-19	1768
Nos adaptamos a la nueva situacion Covid-19	1747
Hay que adaptarse a la nueva situacion Covid-19	1743
Tenemos que adaptarnos a la situacion Covid-19	1737
Nos tenemos que adaptar a la situacion Covid-19	1720
Estamos adaptados a la situacion Covid-19	1702
Adaptados a la nueva situacion Covid-19	1683
Estamos adaptados a la nueva situacion Covid-19	1655
The Corona Letter: How Covid-19 both decreased and increased pollution	931
Test de deteccion rapida COVID19	724
Evite el acto involuntario de tocarse el rostro, faciales para protegernos del coronavirus.	634
Products of COVID19	627
Help to fight COVID-19 fever alarm security door	605
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	589
Coronavirus (Covid19) Relief Bailout	346
Corona minimaliseert uw orderboek	291
Videos para la prevencion de Covid	272
Prevencion de covid19	257
Mamparas de proteccion contra el coronavirus	235
face mask against COVID-19	234
Re:Corona virus Protection Pills and sex pills.	232
Aprovecha productos de protección Covid en Oferta!!!	218
Le corona minimise votre livre de commandes	217
Join the Bowser Administration for a Community Leader Telephone Townhall on Coronavirus	216
Mamparas de proteccion COVID19	215

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

fibpad.com	4805
seorazor.com	4484
tidair.com	4466
countermail.com	1703
gmail.com	954
timesofindia.com	931
126.com	816
medicproduction.com	627
keyable.net	514
expobase.be	508

Top-15 IPs Sending COVID Spam

201.231.5.227	1049
139.99.133.125	627
113.116.204.28	592
81.95.112.26	508
190.247.226.206	435
119.122.90.61	404
177.11.0.13	346
164.90.181.158	244
67.219.150.138	232
201.231.115.229	219

Top-15 Countries Sending COVID Spam

DE	14169
US	4043
CN	2731
AR	1728
IN	1707
BE	718
PE	641
AU	641
BR	457
GB	264

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

CII Virtual Session on "How to Reboot Manufacturing Post Covid-19 Impact? Using the AI/ Digital Technology" : 30 September 2020	5
PHHS 9 21 2020 End of Day COVID 19 Summary	5
COVID-19 Anticorruzione-Trasparenza P.A. e società pubbliche: PNA 2019-2021 e recenti provvedimenti Roma 26/11/20	3
RE: Urgent Job Opening :: Sr. Java Developer// Secaucus, NJ or Philly Area (West Norristown/ Collegeville) (remote to start then onsite post-covid – candidate's choice of site post-covid) // Long term Contract	2
PROMO ANTI-COVID	2
COVID-19 TESTING	2
Covid-19 Related Products Price List	2
COVID-19 Green economy e sviluppo sostenibile: modelli di business, ecobonus, cessione credito Roma 22/10/20	2
REPORTE DIARIO COVID 19	1
Coronavirus - advice for the Third Sector across Lancaster District. Updated Monday 21st September 2020	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: 126,223
Domains with Potential Mail Servers: 2,945
Email-Capable Domains and Hosts: 47,724
Live Hosts and Domains Not Parked: 71,752

Mobile Apps

Apps in Official Stores: 422

by Store

Apple	213
Google	194
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,412

by Store Type:

Hybrid	798
Secondary	559
Affiliate	55

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	25
Hybrid	2
Official	2