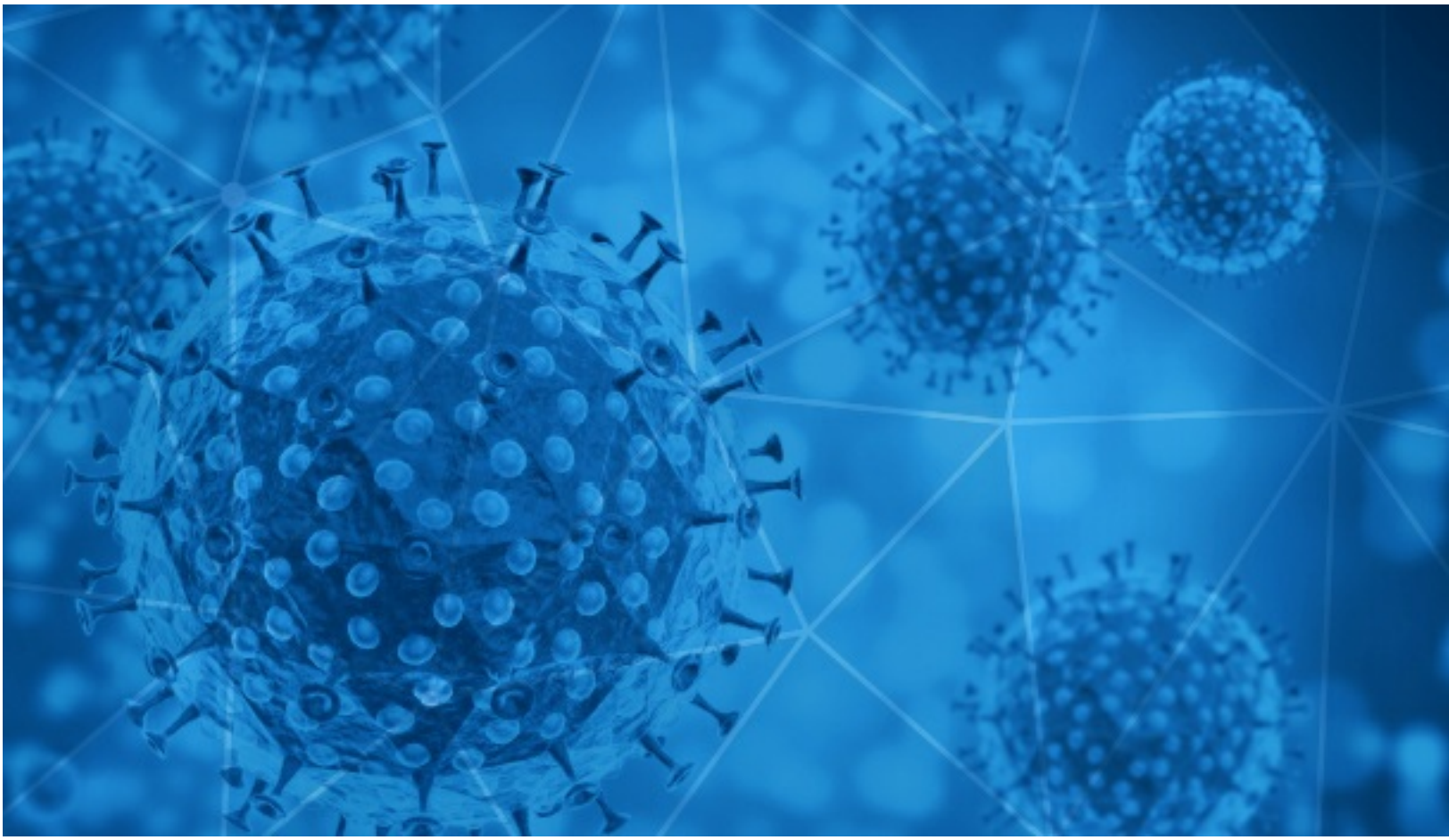
RiskIQ i3:

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

2020-10-13



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 2020-10-12 to 2020-10-13. During this period, RiskIQ analyzed 62,680 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 13,406 unique subject lines observed during the reporting period. The spam emails originated from 1,986 unique sending email domains and 4,447 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	18075
COVID-19 Update: We are open and now offering Free Virtual Consultations	5158
The Corona Letter: How Covid causes brain fog	3864
COVID 19 Donation	1538
COVID-19 Protection Products	947
Pretty Ricky Member Arrested for COVID Loan Scam {VIDEO}Drunk Cardi B twerks on Offset @ B-Day party	842
Nara Deer Possibly Face Starvation & Addiction as Tourists Dwindle Due to Coronavirus - Sankaku News	687
TermoScanner Anti-Covid in pronta consegna. Prezzi dimezzati e modelli a partire da soli Euro 499,00. Non Abbassiamo la guardia!!!	633
Test de deteccion rapida COVID19	628
Test rapido para la deteccion del Coronavirus	627
Mamparas de proteccion contra el coronavirus	469
Test Rápido Covid-19 Segunda Generación - 10.000 Un Entrega Inmediata	452
Mamparas de proteccion COVID19	431
Limpieza y desinfeccion COVID 19	420
Re:Corona virus Protection Pills and sex pills.	361
Re: Your Order Corona virus Protection Pills and sex pills.	320
Hi, Reminder call for your Covid antibody test at Rs 750 only | Confirm soon.	285
Let's fight COVID with 5x Immunity Booster	284
Re: Defeat Coronavirus, non contact fever alarm device	268
Help to fight COVID-19 fever alarm security door	265
Corona virus (Covid19) Bailout Fund	262
Contactless infrared body temperature thermometer defeat Coronavirus	261
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	227
Re: sales,The nasty outbreak caused by covid-19	204
RE: IMPORTANT INFORMATION ,CORONA VIRUS DEATH ...	193

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

epc-store.com	18078
tizgharan.org.uk	6667
campaignhub.xyz	5158
sampark.gov.in	4955
timesofindia.com	3864
tutanota.com	2570
gmail.com	2277
stargoldmedics.com	947
caribbeanfever.com	842
keyable.net	794

Top-15 IPs Sending COVID Spam

159.89.48.131	5154
43.239.110.184	1538
181.239.232.123	1514
181.239.232.96	1054
51.83.130.184	947
113.116.204.205	771
208.100.24.254	687
185.221.173.42	632
103.225.53.84	569
103.225.53.34	522

Top-15 Countries Sending COVID Spam

JP	18244
US	16316
IN	10530
CA	3434
CN	3019
AR	2603
FR	1977
IT	1045
DE	569
GB	493

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

covid 19 fund Payment	13
REMINDER: Covid 19 Wage Subsidy for affected Tourism/Manufacturing businesses	6
Covid-Autum	4
ULima | Taller Gestión de las Relaciones Laborales en Tiempos Post Covid-19 online | 21 de octubre	4
Mời tham dự khóa đào tạo "Nâng cao năng lực quản lý cấp trung hậu COVID-19" ngày 22-23/10/2020	4
про випадок COVID-19	2
Trump's Corona: Allzeithoch bei der Suche	2
Биотек - Барање за р��зервација на COVID 19	2
[Università di Verona] Economia e cultura per sconfiggere il Covid-19 - ciclo videoconferenze	2
RE: FOR IMMEDIATE RELEASE COVID-19 Cases Now More Evenly Spread Across Grant County and Among Age Ranges	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: 129,054
Domains with Potential Mail Servers: 2,801
Email-Capable Domains and Hosts: 48,234
Live Hosts and Domains Not Parked: 68,414

Mobile Apps

Apps in Official Stores: 460

by Store

Apple	234
Google	211
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,569

by Store Type:

Hybrid	850
Secondary	662
Affiliate	57

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1