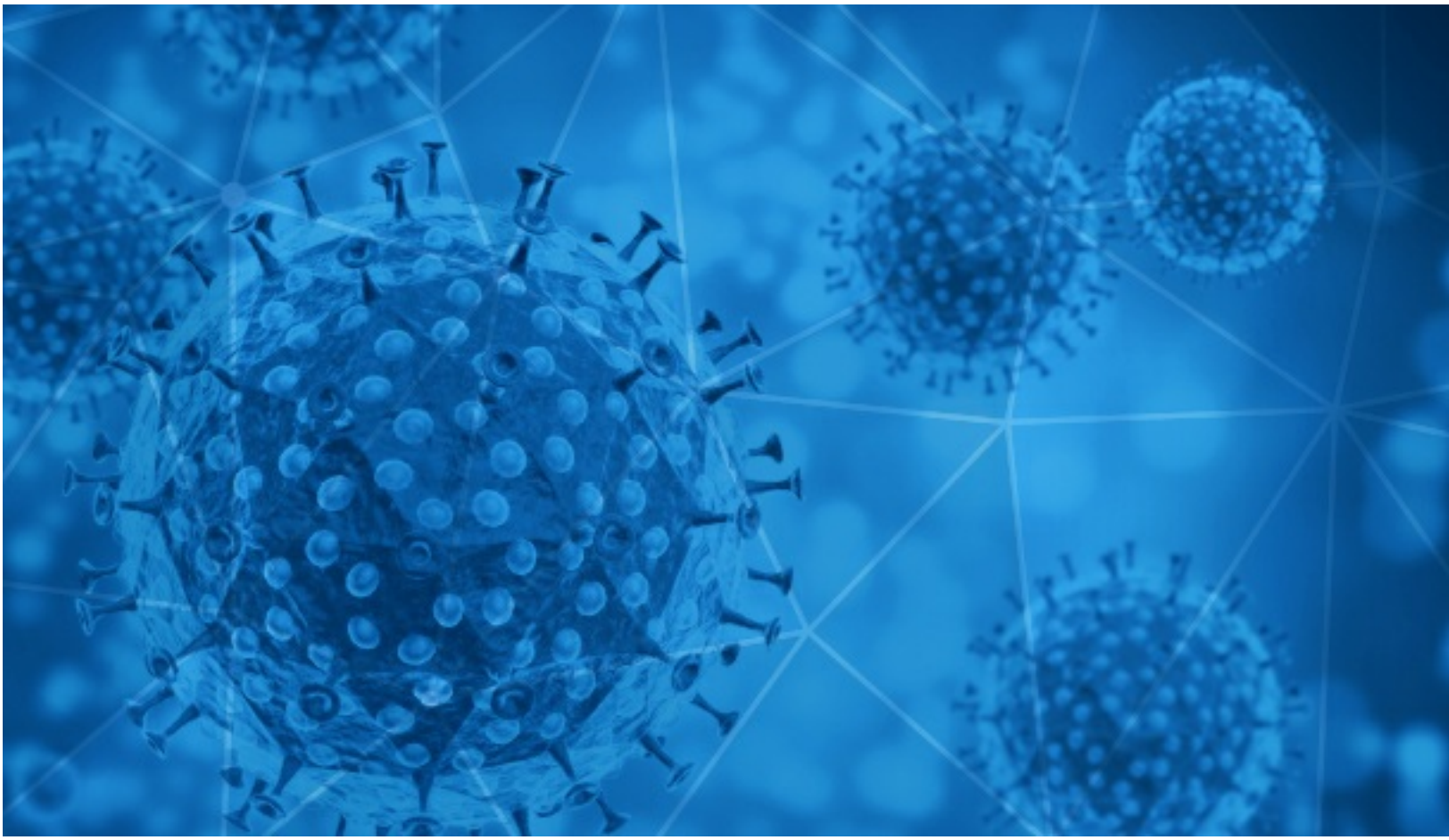
RiskIQ i3:

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

2020-12-25



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 2020-12-24 to 2020-12-25. During this period, RiskIQ analyzed 27,549 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,852 unique subject lines observed during the reporting period. The spam emails originated from 1,142 unique sending email domains and 3,102 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

Trump's pardoning spree continues, COVID-19 reaches Antarctica, and more from Apple News	4334
The Corona Letter: Single dose for many or double dose for some?	3335
Black Doctor Dies from COVID After BEGGING 4 Treatment @ RACIST Hospital+Whites Only Church get PER-	1526
Contactless infrared body temperature thermometer defeat Coronavirus	991
LJC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation.	908
Re: Defeat Coronavirus, non contact fever alarm device	893
Get your Corona-virus Mask while supplies last!	831
Reduce your risk of Corona-virus with this Mask	822
New Corona-virus Mask!	815
Trump correctly tells the RINO's and Commies in Congress to shove the COVID Relief they penned, right up their asses…	815
Traveling soon, wear this mask to fight chances of getting Corona-virus	774
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	734
Opportunity Knocks: How You Can Make Money From VideoTours 360 During Covid-19	635
COVID-19 Vaccine	460
Offering N95 FACE MASK (3M 1860,1860S, Makrite 9500 N95,N95S,HARLEY, SAMPLING SWAB AND TUBE KITS,Novel Coronavirus (COVID-19) Test ,quick delivery in a couple days	282
COVID-19 Vaccine Update	261
Let’s fight together to get through the COVID-19	253
Covid-19 Donation	218
Women scientists vs corona virus	192
Remote-Work: Schöne neue Arbeitswelt? | Corona-Update: Alle Infos zum Impfstoff | Digitaler Vertrieb: So funktioniert Sales heute	170
How are Gym Franchises Coping with COVID-19?	160
Covid-19 Relief Fund	157
Re:covid-19 touch monitor	147
□□□□□□□□□COVID-19□□□□□□□□□ □COVID-19□□□□□□□□□□□□□□□ .....□□□□□□□□ □□□□□□□□	142
NCJ Daily - 27 Confirmed COVID Cases. AG Looks to Take County Back to Court. COVID Closes Toni's Until Dec. 27. Eureka Man Killed in Crash. Pedestrian Killed on 101 Identified.	139

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

insideapple.apple.com	4339
timesofindia.com	3341
clervisor.com	3242
keyable.net	1884
caribbeanfever.com	1526
aol.com	1183
gmail.com	923
frontsight.com	815
ecaptcdhorijumaontfourth.com	583
163.com	554

Top-15 IPs Sending COVID Spam

69.94.130.184	3242
113.89.42.210	1788
131.0.103.220	908
209.123.15.146	815
216.87.190.231	425
46.233.16.77	337
120.229.72.228	229
175.44.33.22	212
216.87.190.229	208
104.237.196.5	199

Top-15 Countries Sending COVID Spam

US	15936
IN	3592
CN	3257
BR	987
GB	346
JP	339
BG	339
DE	284
FR	279
AU	263

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

Precizări de presă privind procedura de testare pentru infecția cu COVID -19 în contextul reluării circulației dinspre Regatul Unit al Marii Britanii și Irlandei de Nord spre Republica Franceză	4
Two Positive Cases of COVID-19: Wide Hollow	3
Buletin de presa 24.12.2020 + comunicat actiuni COVID19 + update comunicat santaj	2
[editors--peacevoice] submission: op-ed: essential workers, hazard pay, safety measures, record profits, covid	2
Organizaciones sociales trabajan por una “Navidad sin Covid-19 en SDN	2
RE: [redacted] ([redacted]) [redacted] COVID 19-M3	2
TR : Vaccination COVID	1
Bekannt aus den Medien - Livinguard Pro Mask - antivirale Gesichtsmaske mit 95% Filter - FFP2-Masken, Covid-19 Schnelltests etc.	1
□□□□12□□□□COVID-19□□□	1
Re: RE: KTM-DOH reissuance due to Covid-19 for 27 DEC travel	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: 137,434
Domains with Potential Mail Servers: 2,596
Email-Capable Domains and Hosts: 52,352
Live Hosts and Domains Not Parked: 47,623

Mobile Apps

Apps in Official Stores: 494

by Store

Apple	245
Google	234
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,939

by Store Type:

Hybrid	993
Secondary	886
Affiliate	60

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1