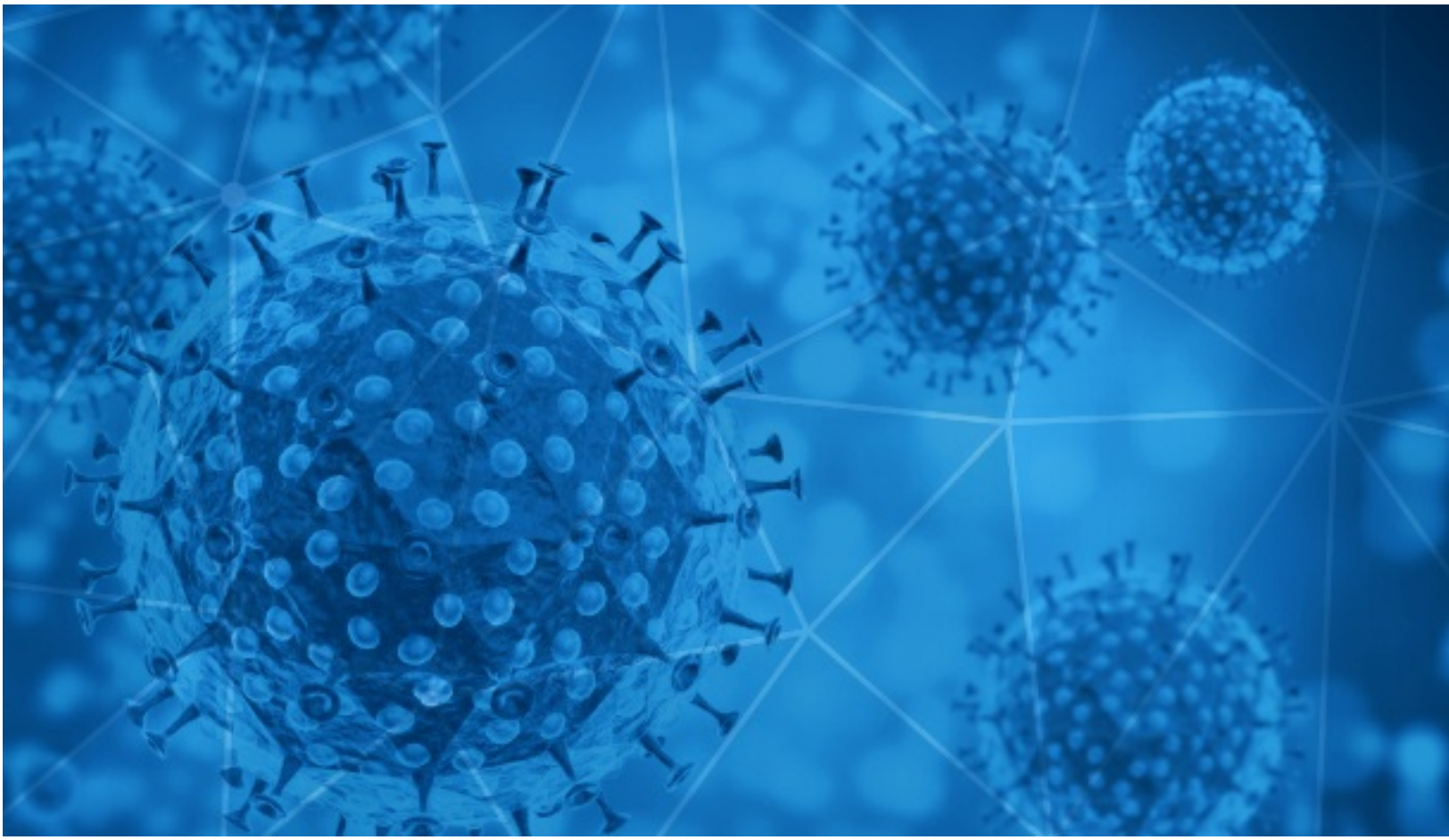
RiskIQ i3:

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

2020-12-09



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 2020-12-08 to 2020-12-09. During this period, RiskIQ analyzed 41,693 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,208 unique subject lines observed during the reporting period. The spam emails originated from 2,105 unique sending email domains and 3,877 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	12359
UK begins COVID-19 vaccinations, monoliths appear around the world, and more from Apple News	4428
The Corona Letter: An omnipresent coronavirus	3499
Safety measures to stay protected against COVID-19	907
Covid19_Relief (IRS) - You are eligible for a grant.	905
testy na covid-19	686
Contactless infrared body temperature thermometer defeat Coronavirus	678
Respuestas gerenciales para el post Covid19	603
Re: Defeat Coronavirus, non contact fever alarm device	594
File to claim your covid Business accredited fund	584
COVID-19 Relief Support.	565
antigen tests for COVID-19	408
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	376
Puricador y Sanitizador de Aire, Estirilizacion contra Coronavirus	365
Lampy sterylizujace UV-C jako dobry sposób walki z koronawirusem (covid-19)	357
No te descuides. Productos Covid a precios increíbles	356
COMING OUT OF COVID WITH SPASEEKERS	341
Re: Corona virus Protection Pills.Order confirmation	307
COVID-19 Impact on Banking and Financial Services	284
Test Rápido Covid-19 Segunda Generación	269
Hope you are safe during this Covid-19 period.	265
Announcing my health care and COVID-19 team	260
Join us for a fireside chat on "Adapting to the Accelerated Demand for Data & Cloud in a Post-COVID World" | 10th Dec | 3:00 PM	226
Protégez-vous du Covid avec SOLUGERM France	207
::: REG-#Season greetings [REDACTED_DOMAIN] #COVID-19*Relief Funds_From "WHO"::::	190

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	12359
insideapple.apple.com	4469
timesofindia.com	3503
keyable.net	1272
gmail.com	941
icicliprulife.com	907
securesuite.net	905
hotmail.com	623
outlook.com	616
walla.co.il	603

Top-15 IPs Sending COVID Spam

113.89.43.81	1272
197.81.195.127	905
199.192.16.207	584
82.85.174.28	552
109.196.164.106	408
103.225.54.136	405
77.55.217.43	394
162.13.135.56	340
103.225.52.250	319
103.225.54.121	315

Top-15 Countries Sending COVID Spam

JP	12423
US	12140
IN	4714
CN	2173
PL	1199
GB	1159
ZA	977
FR	883
IT	697
AR	685

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

Zasiłki ZUS-trudnosci w okresie covid 19	8
IMPORTANT - COVID-19 Partners Platform invited you to re-access applications within their organization	5
COVID-19 In Franklin County	5
WEBINAR ΜΕ ΘΕΜΑ ΣΥΝΟΛΙΚΗ ΦΡΟΝΤΙΔΑ ΤΟΥ ΑΣΘΕΝΟΥ�� ΜΕ COVID-19	2
Covid 19- Return to Work and Workplace Preparedness Course 2021	2
Real Time PCR Online Course (with special emphasis to COVID-19 testing)	2
Modify holiday plans & manage Covid stress this festive season – health experts	2
Covid Showdown At High Noon	1
Fwd: COVID-19 - December 8, 2020	1
Reg. Employee list for COVID Vaccine Demand	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: 135,457
Domains with Potential Mail Servers: 2,612
Email-Capable Domains and Hosts: 51,605
Live Hosts and Domains Not Parked: 44,959

Mobile Apps

Apps in Official Stores: 482

by Store

Apple	243
Google	224
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,868

by Store Type:

Hybrid	968
Secondary	841
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1