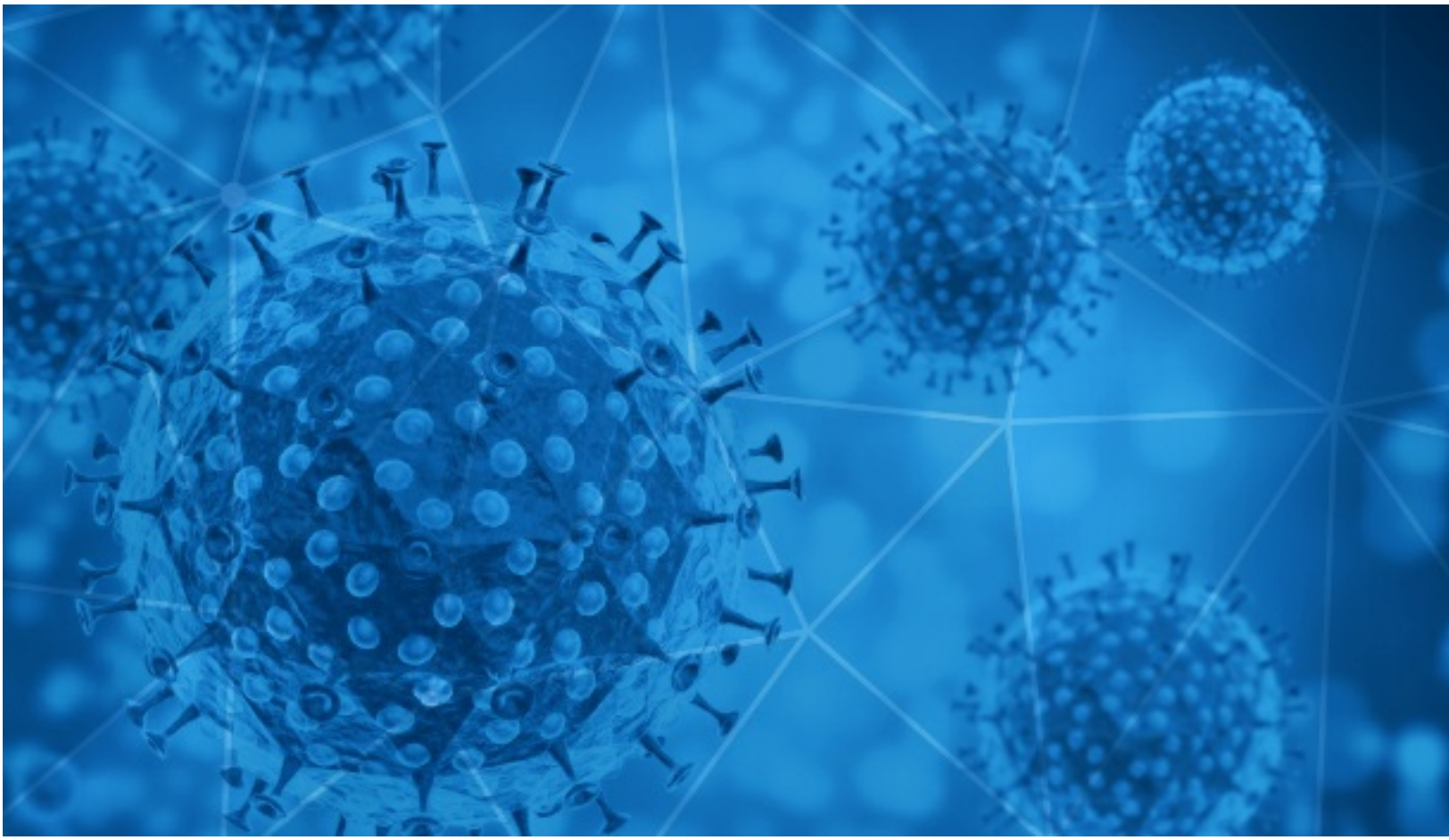
RiskIQ i3:

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

2020-12-15



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 2020-12-14 to 2020-12-15. During this period, RiskIQ analyzed 48,165 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,426 unique subject lines observed during the reporting period. The spam emails originated from 2,276 unique sending email domains and 6,048 unique SMTP IP Addresses. Analysts identified 14 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	5705
Respuestas gerenciales para el post Covid19	5523
TIMES TOP10: Which states will get how many Covid vaccines?	5133
The Corona Letter: Vaccines are here. What about treatments?	4016
First COVID-19 vaccines arrive today, codebreakers decipher Zodiac killer's message, and more from Apple News	3767
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	3389
Your Email Has Been Awarded 1 Million Pounds In 2020 Coca Cola Covid-19 Pandemic Award	2234
Puricador y Sanitizador de Aire, Estirilización contra Coronavirus	811
Re: Defeat Coronavirus, non contact fever alarm device	798
Contactless infrared body temperature thermometer defeat Coronavirus	782
Wearing a KN95 mask is your best defense against coronavirus	383
Let’s fight together to get through the COVID-19	354
Help the world's response to Covid-19 with the most protective mask on the market.	354
United Nations 2020 Covid-19 Compensation Payment.	317
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	293
COVID 19 SPENDE	254
Re: Covid-19 Donations..	226
You're Invited || Live Roundtable Discussion on "Enabling IT with Innovation in Post-COVID World" || December 15, 2020 @ 12:00 PM IST	188
COVID-19: Employer support – live webinars	181
No new cases of coronavirus?	173
The ONLY country with 1 single case of coronavirus recorded!	170
Influweb contro il coronavirus	165
Viajar a otra comunidad en la Navidad del coronavirus: familia, allegados, fechas, ...	160
Covid-19 Coronavirus: how to protect yourself	156
Are you safe from the coronavirus?	156

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	5705
walla.co.il	5523
bounce.indiatimes.com	5133
timesofindia.com	4016
insideapple.apple.com	3909
expjumaalsrreadyactivationtthird.com	2372
hotmail.com	2330
keyable.net	1580
gmail.com	1119
ecaptcdhorijumaontfourth.com	1014

Top-15 IPs Sending COVID Spam

201.231.6.45	4408
192.3.136.7	2233
113.116.205.241	1580
50.3.203.18	910
190.247.240.177	883
134.73.146.58	737
219.65.85.16	495
219.65.85.26	488
219.65.85.13	477
219.65.85.14	475

Top-15 Countries Sending COVID Spam

US	15154
IN	9798
JP	5935
AR	5596
CN	2684
DE	1446
FR	1260
GB	1190
NL	445
ID	440

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Re: Pfizer-BioNTech Covid-19 Vaccines First Interim	12
TransactionDesk Invitation Formulaire Envoyé par Sergio Coronado	1
Fwd: TransactionDesk Invitation Formulaire Envoyé par Sergio Coronado	1

Top-15 Subjects Containing doc/xlsx Files

SAVE THE DATE - Palisades Institute: The Impact of COVID-19 on Rockland County's Healthcare System	4
Completed: Please DocuSign: COVID Testing Letter 12.12.2020.docx, Coronavirus Resident Testing Consent.pdf	3
CDC Clinician Calls on COVID-19 Vaccine	3
Covid-19 Notice - Edison Middle School 12/14/20	3
Corona	2
BAD NEWS AFTER COVID - 19/ MAUVAISE NOUVELLE APRÈS COVID - 19	2
I am sharing 'COVID Ward Discharged Patients Report Dec 2020' with you	2
New COVID Protocol & Waiver	2
[SIARAN PERS] Meski Pandemi Covid-19 Berakhir, Perubahan Perilaku dan Preferensi Konsumen Indonesia Akan Terus Berlanjut	2
Covid 19- Return to Work and Workplace Preparedness Course 2021	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: 136,239
Domains with Potential Mail Servers: 2,621
Email-Capable Domains and Hosts: 51,871
Live Hosts and Domains Not Parked: 46,561

Mobile Apps

Apps in Official Stores: 484

by Store

Apple	243
Google	226
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,893

by Store Type:

Hybrid	974
Secondary	860
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1