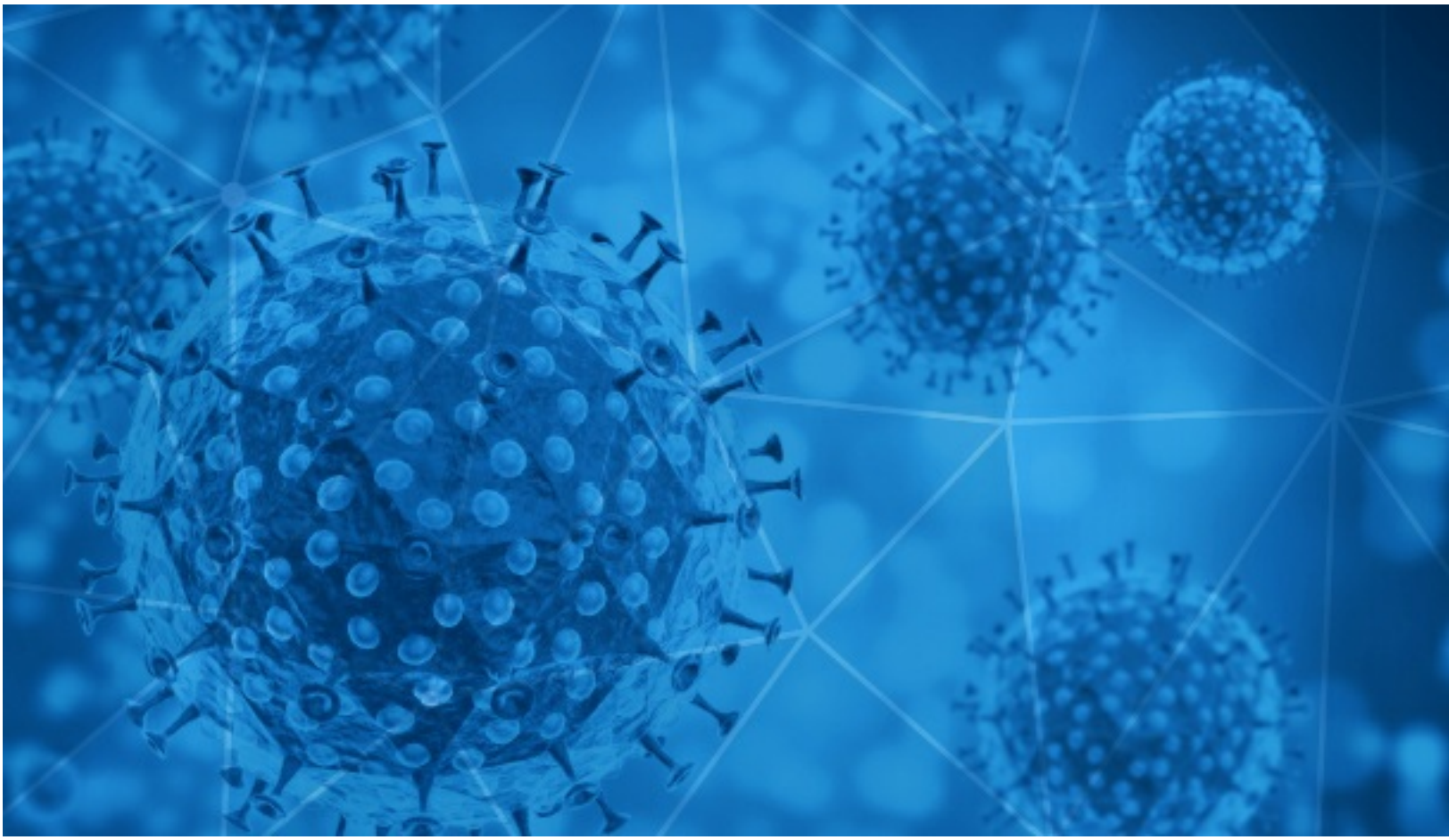
RiskIQ i3:

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

2020-11-30



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 2020-11-29 to 2020-11-30. During this period, RiskIQ analyzed 13,657 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,420 unique subject lines observed during the reporting period. The spam emails originated from 913 unique sending email domains and 1,876 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: The task of vaccinating a billion people	4129
TEST COVID19 de detección rapida al menor costo	926
Covid19_Relief (HMRC) - You are eligible for a grant.	598
Respuestas gerenciales para el post Covid19	416
Re: COVID-19 RESPONSE FUND	415
COVID -19 STIMULUS PAYMENT	411
Re: Digital signage solution for Covid-19	320
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	272
Help fight Covid-19: Support Nutrition for Children	242
Wintergloed in Brugge afgelast in afwachting van nieuwe maatregelen - Jeroen Olyslaegers: 'De samenleving heeft wat hypocrisie nodig om de vrede te bewaren' - 25 procent meer enkelbanden uitgedeeld tijdens coronacrisis	217
Re: Personal, SME & Business Relief [COVID-19]	200
Govt announces new COVID guidelines from 1 Dec, More Details	158
Oferta de Tests Rápidos COVID-19	146
Re: Use This Fund To Help Re-covered Corona-19 Victims In UK	131
Please Help and Join the COVID-19 Vaccine Trial	127
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	123
United Nations 2020 Covid-19 Compensation Payment.	122
¿En qué consiste la prueba de Antígeno Covid?	116
Know your Covid-19 Risk	112
Let’s fight together to get through the COVID-19	111
[Earn Credits] covid 19 cure ?	110
Re: Corona virus Protection Pills.Order confirmation	102
Global Pandemic Relief Fund 3 Million Pounds In 2020 Coca Cola Covid-19 Pandemic Relief Award	98
**Re: COVID-19 - Projects| Website	Mobile Application	E-Commerce	SEO (Results Guaranteed) [REDACTED_DOMAIN]**	94
Corona virus compensation	84

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	4131
grupolylsalud.com	926
gmail.com	795
securesuite.uk	598
walla.co.il	416
almasraf.ea	411
126.com	320
vivaldi.net	279
cmbmutualfunds.com	274
consons.com.cn	272

Top-15 IPs Sending COVID Spam

197.81.195.127	598
201.231.5.7	551
212.227.254.175	428
181.239.232.96	412
198.187.28.218	411
181.47.94.27	375
216.117.171.61	242
219.65.85.23	235
219.65.85.17	230
219.65.85.27	223

Top-15 Countries Sending COVID Spam

IN	4387
US	3092
AR	1383
CN	732
ZA	674
DE	670
FR	306
PH	274
BE	252
--	200

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

ANC Weekly COVID-19 Reports	29
United Nation Covid-19 Relief Fund (Phase2)	12
NDP - Falla Corona conmemora el aniversario UNESCO con una instalación urbana de literatura festiva en el barrio del Carmen	3
Promocion Guatemala 2 x 1 promocion Post Covid.	2
FW: COVID-19 (Building list checked result) - 28 Nov (full)	1
Hope you and your family are staying safe from corona virus_Office Address Change Notice_Fee Schedule 0f 2020	1
Copy of Modified copy of Modified copy BRITS HOSPITAL COVID19 (Autosaved).xlsx 14April 2_1_1_1_1 (9)_1 - Copy..xlsx	1
Atbalstīsim mdiķus Reģionālajās slimnīcās, kas strādā Covid frontē!	1
UPDATED COVID PATIENT LISTS	1
RE: REPORTE COVID-19 RAICA 29.11.2020 (CORTTE: 07.00 HORAS)	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: 134,303
Domains with Potential Mail Servers: 2,611
Email-Capable Domains and Hosts: 51,219
Live Hosts and Domains Not Parked: 45,099

Mobile Apps

Apps in Official Stores: 475

by Store

Apple	238
Google	222
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,821

by Store Type:

Hybrid	940
Secondary	822
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1