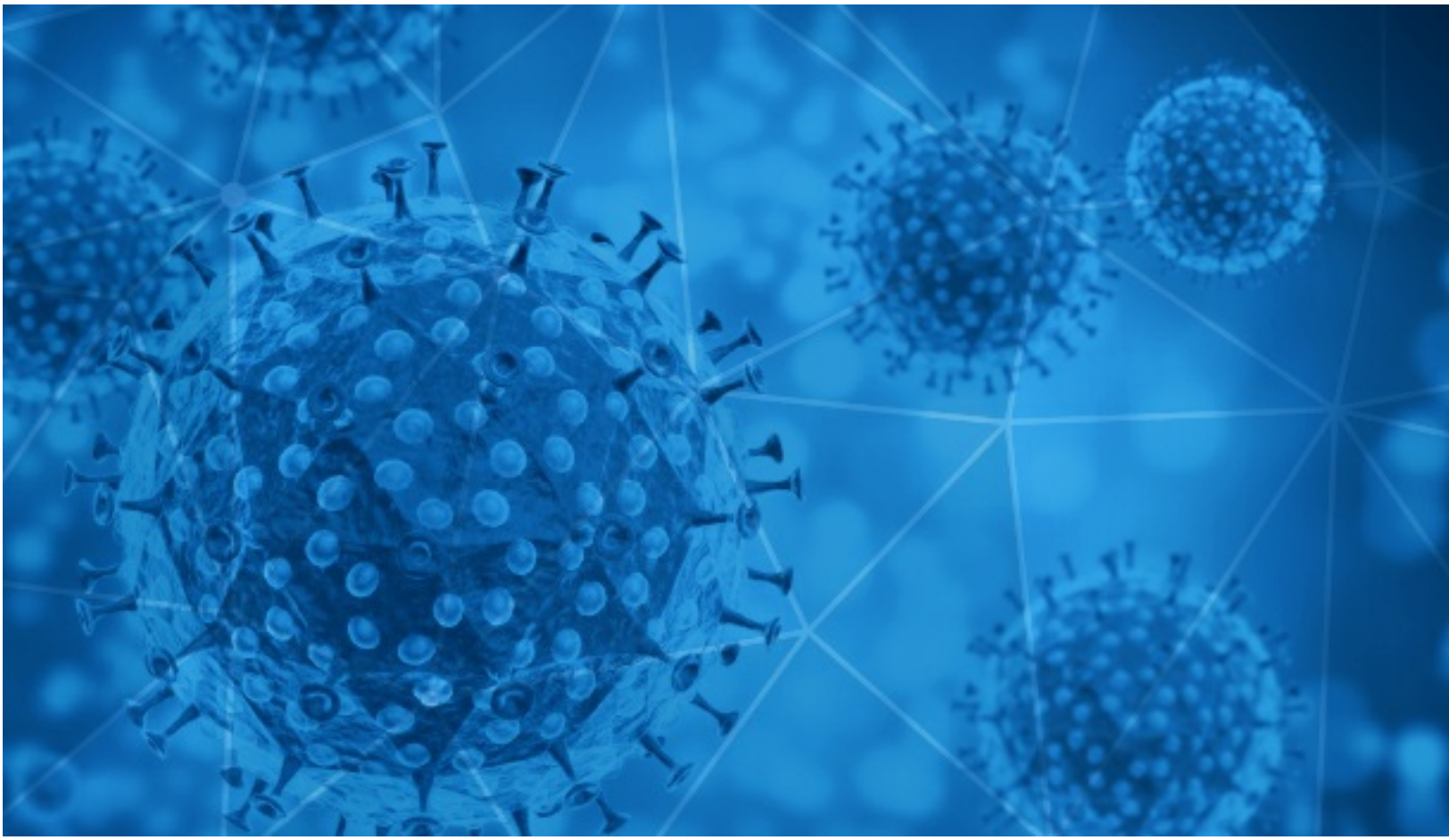
RiskIQ i3:

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

2021-01-13



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 2021-01-12 to 2021-01-13. During this period, RiskIQ analyzed 39,525 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,451 unique subject lines observed during the reporting period. The spam emails originated from 3,319 unique sending email domains and 4,216 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	12848
The Corona Letter: Another Covid strain rears up, this time in Japan	4337
Trump one step closer to second impeachment, lawmakers test positive for COVID-19 following attack, and more from Apple News	3888
What you should know about the COVID-19 vaccines	1599
Arma tu Kit contra el Covid-19	569
Covid-19 Test	500
Covid Test	490
Gran Venta Outlet - Productos Covid 19	424
Covid19 Relief Fund:	402
Re: Defeat Coronavirus, non contact fever alarm device	339
Defeat Coronavirus, Thermographic Camera	337
Thermographic Automation Camera defeat Coronavirus	324
Contactless infrared body temperature thermometer defeat Coronavirus	316
Coronamaatregelen verlengd tot 1 maart	241
[CND Español - 4313]. Covid: Los 10 países con más pérdidas en el turismo en 2020	238
Lampy sterylizujace UV-C jako dobry sposób walki z koronawirusem (covid-19)	237
Book your seat to know how COVID-19 impacted the EdTech	233
NCJ Daily - 93 New Cases, Two Hospitalizations. Weather Postpones Crab Season. Board to Consider COVID Resolution. Huffman Town Hall on Capitol Riot.	214
UNDF CASH DONATION (COVID-19)	211
Re: Personal, SME & Business Relief (COVID-19).	203
Save 50%!T(MISSING)oday Only On KN95 Certified Mask To Protect Against COVID19 Virus	185
Urgent Need__Project Manager_Southbury , CT (Remote Till COVID)	165
COVID 19 SPENDE	133
Funding The Fight agianst Covid19!	132
#Ask details for Covid-91 Relief F und	129

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	12849
timesofindia.com	4344
insideapple.apple.com	3891
subscriptions.cms.hhs.gov	1604
keyable.net	1316
gmail.com	573
mailinator.cl	569
webmail.co.za	402
163.com	321
126.com	249

Top-15 IPs Sending COVID Spam

113.116.205.233	1316
79.175.173.238	401
103.225.55.158	396
45.148.8.74	301
103.225.52.36	294
103.225.55.52	290
103.225.55.51	287
219.65.85.21	267
219.65.85.25	266
219.65.85.23	266

Top-15 Countries Sending COVID Spam

JP	12984
US	11044
IN	4582
CN	2225
--	1437
FR	1174
DE	642
GB	493
ES	471
BE	467

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

WEB on Line COVID-19 Equilibrio economico e continuità aziendale nel bilancio IAS/IFRS: aspetti contabili e fiscali 25/2/21	19
URGENT INFORMATION LETTER: COVID-19 APPROVED NEW VACCINES AND CASE REPORT	16
szkolenie z zasiłków ZUS w okresie covid 19	6
BVBM: Mời tham dự Hội thảo trực tuyến Đột quỵ trong bối cảnh COVID ngày 15/1/2021	3
PRUEBAS DETECCION DE COVID19 SEROLOGICAS Y DE ANTIGENOS	2
ENSEMBLE- JANSSEN COVID-19 VACCINE TRIAL Site #US10156_ Data cleaning_ Actions needed by EOB – Pls reply	2
COVID-19 Monoclonal Antibodies - Los Angeles County Department of Public Health	2
Buletin de presa 12.01.2021 + comunicat actiuni COVID	2
Vaccination anti COVID 19	2
COVID-19 Office Update	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: 139,264
Domains with Potential Mail Servers: 2,574
Email-Capable Domains and Hosts: 53,053
Live Hosts and Domains Not Parked: 48,090

Mobile Apps

Apps in Official Stores: 502

by Store

Apple	245
Google	241
WindowsPhone	15
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,014

by Store Type:

Hybrid	1039
Secondary	912
Affiliate	63

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1