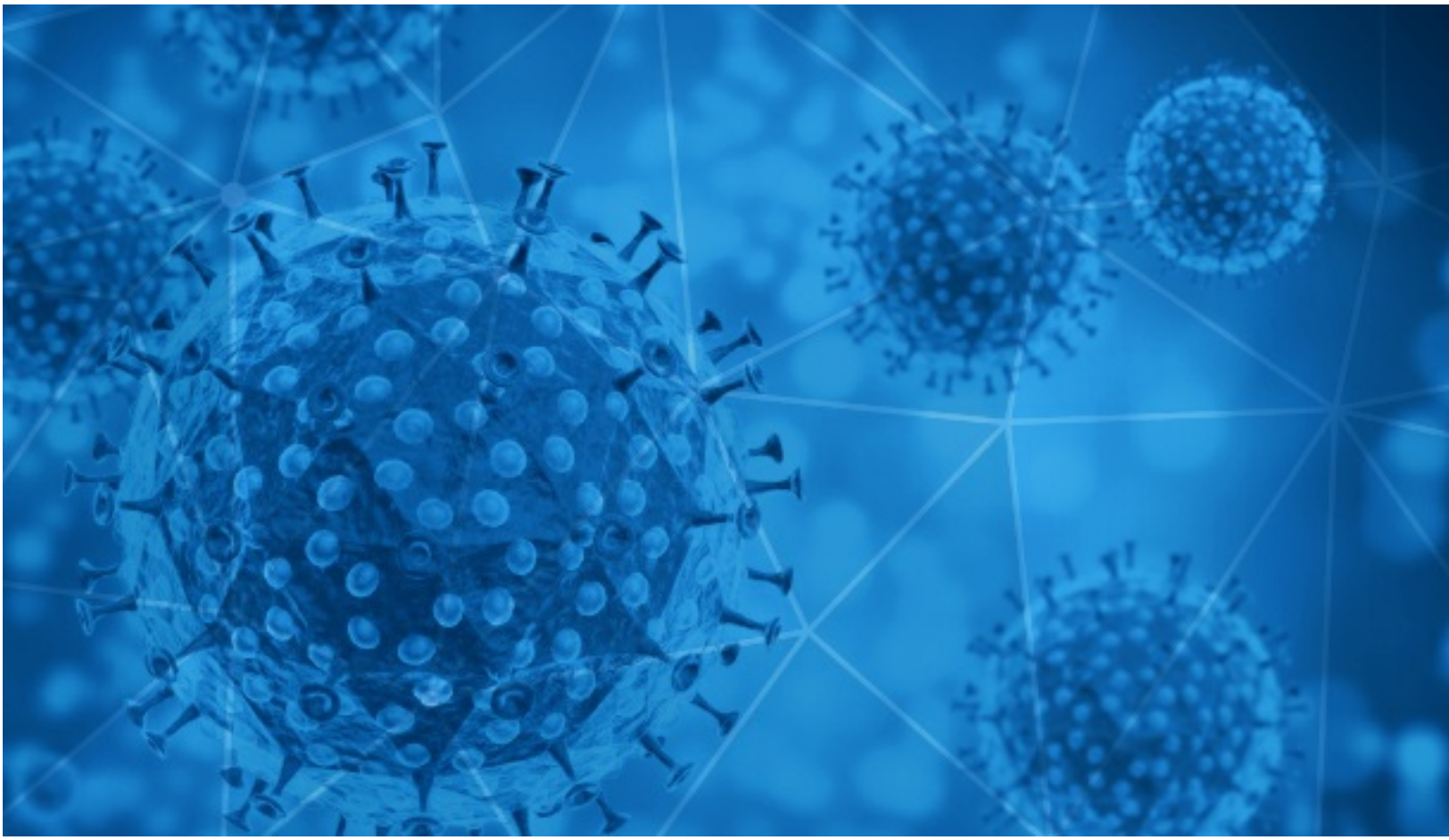
RiskIQ i3:

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

2021-01-22



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 2021-01-21 to 2021-01-22. During this period, RiskIQ analyzed 34,253 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 6,438 unique subject lines observed during the reporting period. The spam emails originated from 2,270 unique sending email domains and 4,033 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

COVID Notice: Hospital-Grade Disinfectant made available to public here	4506
Kahve Demlemenin Püf Noktaları ı 18-24 Ocak Haftası Burç Yorumları ı Covid Aşısı Hakkında Merak Edilen Her Şey ı Buse Terim'den Cilt Bakım Önerileri ı Futuristik Robotlar Hayatı Kolaylaştırıyor ı 2021de görevimiz Aşık Olmak	3296
The Corona Letter: The strong case for intranasal vaccines	3220
Re:Happy New Year! Your Covid-19 Grant .	1042
LJC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation	878
Re:Happy New Year! Your Covid-19 Grant .	720
Puricador y Sanitizador de Aire, Estirilización contra Coronavirus	610
Government’s Darkest Secret sees the light of day due to Coronavirus Situation.	594
COVID-19 RELIEF FUND CONTRIBUTION	503
Productos Covid 19, entrega inmediata !!	471
COVID-19 Pantallas Protectoras	469
Covid-19 Palliative F und	447
Gran Venta Outlet - Productos Covid 19	375
INFO: Glicyryzyna hamuje replikację COVID-19	293
Surviving Covid-19	278
Covid-19 relief funds	269
Re: Digital signage solution for Covid-19	242
[Earn Credits] --*--*--_FINALLY__THE__END__TO__COVID19?_--*--*--	226
Direct Client Req:: Need SAP Security Analyst, Tallahassee, FL, Release Train Engineer,& Organization Change Management, &Agile, Coach/Scrum Master, St. Paul, MN REMOTE Until COVID!!	212
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO ANTE EL COVID19	191
COVID-19 Wholesales: Ventilators, Hand Gloves, Face mask, Surgical Gowns, Hand Sanitizer.	189
Covid-19 Financial Relief	179
Defeat Coronavirus, Thermographic Camera	166
Are you Alive? (Covid -19 Security Alert)	163
Re: Defeat Coronavirus, non contact fever alarm device	161

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

landscapidea.buzz	4507
istandist.com	3296
timesofindia.com	3220
hospiramedical.co.uk	2645
teemanjay.net	1763
eremitmms.com	878
gmail.com	778
keyable.net	646
correosmasivos.cl	610
myoffers.club	594

Top-15 IPs Sending COVID Spam

23.228.115.29	4501
195.85.216.96	3296
194.146.24.99	2545
103.131.245.194	878
221.148.30.225	830
82.223.21.194	720
167.71.241.109	594
201.189.186.242	576
51.83.246.183	571
113.89.42.173	568

Top-15 Countries Sending COVID Spam

US	11082
--	7015
IN	3360
FR	1809
CN	1750
KR	1088
CL	855
ES	847
GB	762
DE	736

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

URGENT INFORMATION LETTER: COVID-19 NEW APPROVED VACCINES AND THE RISK	25
WEB on Line COVID-19 Equilibrio economico e continuità aziendale nel bilancio IAS/IFRS: aspetti contabili e fiscali 25/2/21	21
URGENT INFORMATION LETTER: COVID-19 NEW APPROVED VACCINES AND THE RISKS	21
URGENT INFORMATION LETTER: COVID-19 NEWLY APPROVED VACCINES AND THE RISKS	19
TEUTEUGA O POLOAIGA O LE COVID19 –Aso 21 Ianuari 2021	4
Ulazak privrednika u RS tokom trajanja pandemije Covid 19	3
Ivars Kalviņš atklāj, kā izvēlēsies vakcīnu pret Covid-19	2
Fagforbundets vurdering ang. Covid 19 - med vedlegg	2
RE: REPORTE COVID PEDREGAL	2
Covid 21012021	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: 140,346
Domains with Potential Mail Servers: 2,568
Email-Capable Domains and Hosts: 51,993
Live Hosts and Domains Not Parked: 44,965

Mobile Apps

Apps in Official Stores: 506

by Store

Apple	249
Google	240
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,045

by Store Type:

Hybrid	1051
Secondary	929
Affiliate	65

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1