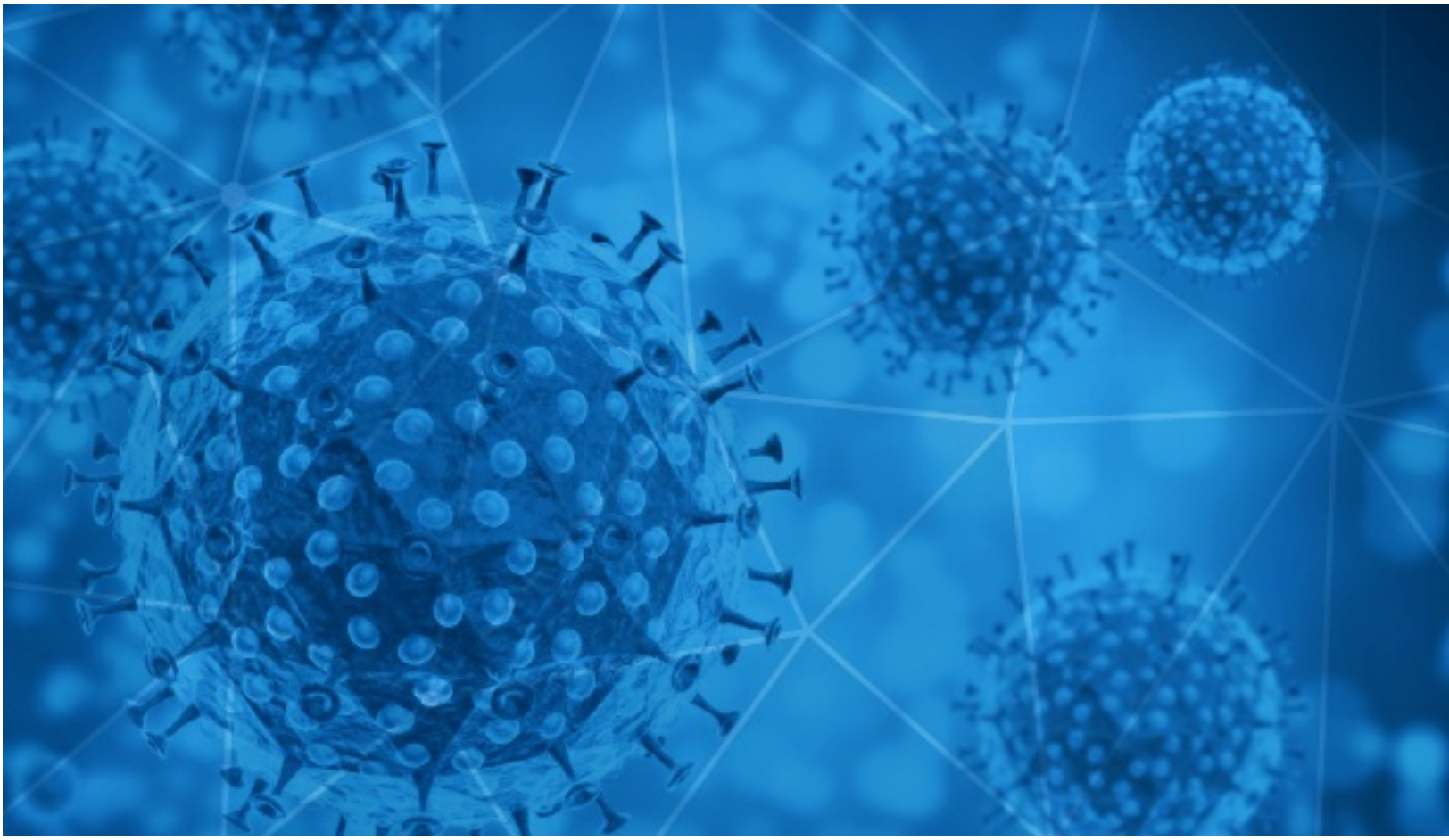
RiskIQ i3:

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

2021-02-09



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 2021-02-08 to 2021-02-09. During this period, RiskIQ analyzed 36,348 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,756 unique subject lines observed during the reporting period. The spam emails originated from 2,043 unique sending email domains and 4,053 unique SMTP IP Addresses. Analysts identified 20 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	12561
The Corona Letter: Some clarity on vaccine safety, please?	3564
First member of Congress to die from COVID + Teacher Charged with 19 Counts of Child Molestation	1864
COVID TASTE RESULT	1669
NY's empty COVID vaccination centers+Commuter, slashed across the face with box cutter on NYC subway	1611
Re:Please Reply Fast To Claim Your Covid-19 Grant!!	691
Re: Personal, SME & Business Relief (COVID-19).	603
TermoScanner e strumenti DPI Anti-Covid in pronta consegna con sconti oltre il 70% e prezzi a partire da Euro 39,00 + spedizione gratuita. Non Abbassiamo la guardia!!!	588
Looking for the perfect COVID PROOF BUSINESS TODAY!?	482
European Union Compensation Funds for Covid19 Victims	444
Entschädigungsfonds der Europäischen Union für Covid19-Opfer.	316
Your Ultimate Protection against COVID-19. US FDA Registered	243
Euroopa Nõukogu: Covid-19 vastu vaktsineerimist ei tohi teha kohustuslikuks	226
Get your Corona-virus Mask while supplies last!	202
Riscaldamento globale, ruolo chiave nel Covid-19 | Tè verde e caffè riducono mortalità da infarto e ictus - 8 Febbraio 2021	201
Public Relation Facebook Covid-19 Lottery Department	200
New Corona-virus Mask!	199
Reduce your risk of Corona-virus with this Mask	193
Traveling soon, wear this mask to fight chances of getting Corona-virus	191
UN Covid-19 Winning Notification	159
Good Morning, SA | AstraZeneca vaccine proven ineffective against SA Covid-19 strain, Durban in chaos as alcohol use spikes, Lamola takes aim at Zuma	142
COVID-19 Relief Fund	116
YOU ARE COVID-19 REWARD BENEFICIARY	112
Re: covid-19 touch monitor	111
Urgent Requirement - Sr. UI Engineer - (Must have 10+ yrs. Exp) - Santa Clara, CA (Remote till the COVID-19 is over) - 12 + Month Contract.	108

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

giant-pw.com	12563
timesofindia.com	3564
caribbeanfever.com	3475
gmail.com	2924
clearvice.com	785
teemanjay.net	691
livejob.it	628
cmbmutualfunds.com	603
herculist.com	474
tecademicsmail.com	468

Top-15 IPs Sending COVID Spam

210.5.156.90	1672
63.81.84.26	785
87.248.52.51	766
202.104.175.244	691
185.221.173.42	628
103.225.55.214	541
216.87.190.231	475
120.89.46.92	410
103.225.55.70	395
103.225.54.50	386

Top-15 Countries Sending COVID Spam

JP	12713
US	9593
IN	3716
CN	2895
IT	1814
PH	609
BR	589
FR	422
GB	414
NL	409

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

URGENT TENDER#675320 (covid19 kits)	18
Rapid Test Kits Covid-19 – Caroline Diment-VAT exemption form	1

Top-15 Subjects Containing doc/xlsx Files

***IMPORTANT* Bulk Quote Request-Covid19**	20
Fujitsu prepara a su Canal SELECT para las nuevas oportunidades tecnológicas y de negocio derivadas de los cambios producidos por la pandemia mundial de Covid 19	8
WEB OnLine COVID 19 Organizzazione lavoro PA e Spa pubbliche: remote working, contenuti POLA (entro 31/3), sicurezza 16/2/21	8
Benjamin Locicero New admit, COVID negative	3
Planowanie i rozliczanie czasu pracy w 2021 roku oraz w dobie covid-19.	3
For Tomorrow's Release :DP WORLD, UAE REGION ROLLS OUT ITS COVID-19 VACCINATION DRIVE	3
COVID Vaccine information for your upcoming appointment	2
GdF Catania - Comunicato stampa - Controlli nella Provincia di Catania. Denunciato un soggetto positivo al COVID-19	2
PR "Atvestās AstraZeneca vakcīnas pret Covid-19 gaida apstiprinājumu tālākai izmantošanai"	2
Fw::invitación al webinar Telemedicina y Covid - 25 de febrero	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: 142,937
Domains with Potential Mail Servers: 2,586
Email-Capable Domains and Hosts: 51,869
Live Hosts and Domains Not Parked: 44,492

Mobile Apps

Apps in Official Stores: 511

by Store

Apple	252
Google	242
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,075

by Store Type:

Hybrid	1062
Secondary	946
Affiliate	67

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1