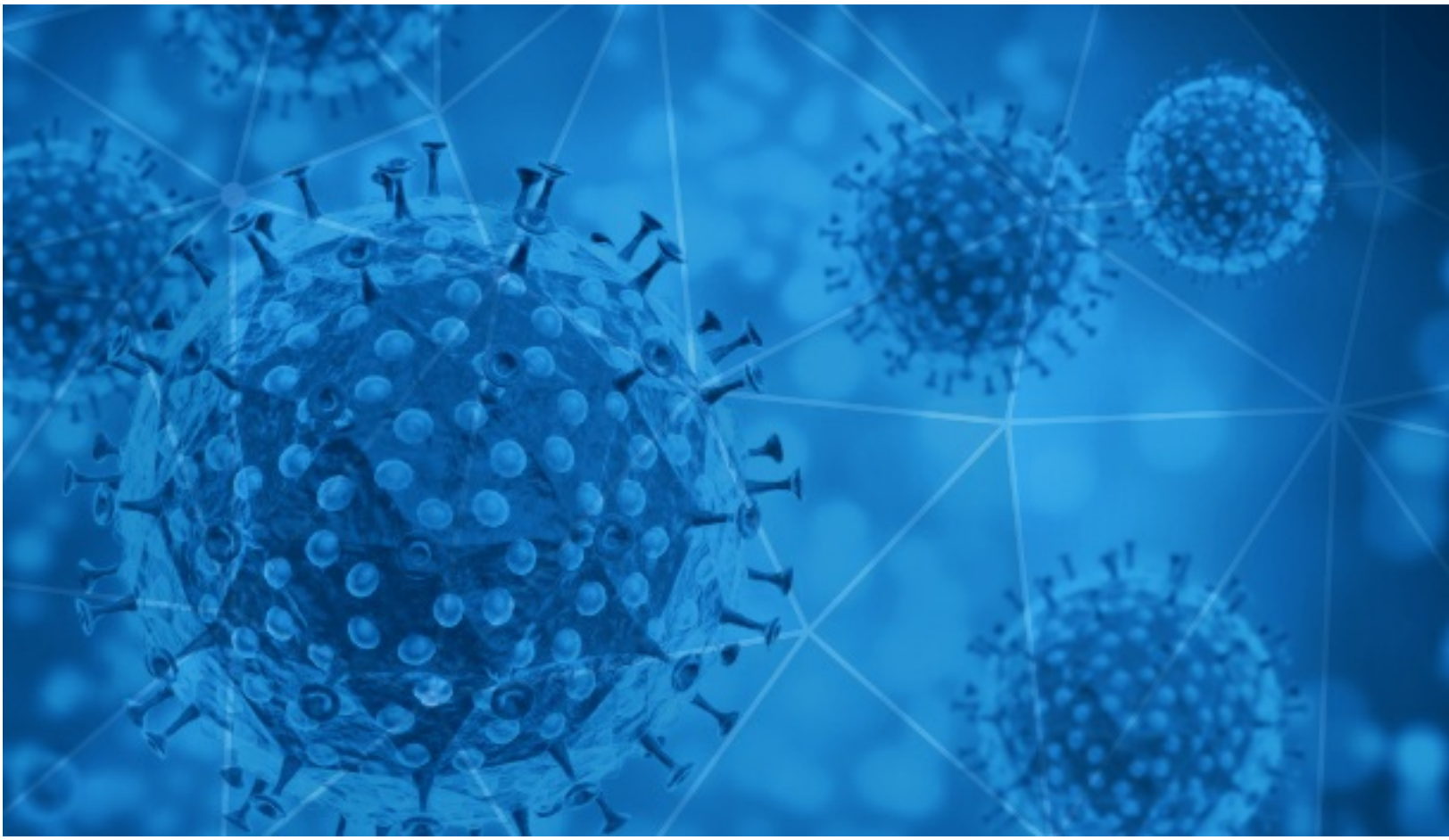
RiskIQ i3:

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

2021-02-22



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 2021-02-21 to 2021-02-22. During this period, RiskIQ analyzed 38,055 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,688 unique subject lines observed during the reporting period. The spam emails originated from 1,095 unique sending email domains and 2,131 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	18654
The Corona Letter: Is single dose of vaccines good enough?	4356
Trump, Pence Warn us About COVID-19 Hysteria	3823
Trump Exposes COVID-19 Hoax	1847
Re: Apply For Covid19 Grant	1212
COVID19 Diferencia entre certificado de aislamiento e incapacidad	1167
Your compensation $2,500,000.00, dou coronavirus(Covid-19).	720
Re: Personal, SME & Business Relief [COVID-19].	377
"Corona-varianten gaan markt inpalmen" - NMBS verwacht opnieuw grote drukte - Kobe Ilsen wil vaderschap "wél doen zoals het hoort"	245
[SPAM] RE:COVID-19 Compensation Claim....	231
COVID19 LOAN RELIEF OFFER / INVESTMENT	228
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	175
(□□)□□□□19(COVID-19)□ □□ □□□□□□□□□□□□ □□□□□	152
Re: covid-19 touch monitor	141
Coronavirus: 968 nuovi casi, età media 44 anni. 15 decessi	116
PLAN PROVINCIAL PÚBLICO GRATUITO, Y OPTATIVO CONTRA COVID-19 - Información turno vacunación	111
Donation For Covid Relief	107
COVID-19 BENEFITS.	94
Is Your Mask Protecting You? Shop KN95 For Ultimate Protection Against COVID19	93
COVID19 #'s Are Increasing, Stock Up On KN95 Masks And Stay Protected	73
COVID LOANS FROM UNITED NATIONS	64
Wearing a KN95 mask is your best defense against coronavirus	62
COVID-19 Relief Fund"	60
AN AID EMPOWERMENT FOR (COVID-19)	60
Covid 19 Vaccine Center	57

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	18655
windseason.buzz	5670
timesofindia.com	4370
gib-gov.com	1212
saludtotal.com.co	1167
usa.com	720
gmail.com	642
cmbmutualfunds.com	377
nieuwsblad.be	249
aliyun.com	231

Top-15 IPs Sending COVID Spam

195.62.46.162	5669
200.31.17.85	1166
103.225.52.69	761
64.57.250.165	720
103.225.54.172	607
103.225.52.187	528
103.225.54.37	472
103.225.52.143	445
103.225.54.168	420
103.225.55.97	404

Top-15 Countries Sending COVID Spam

JP	18685
--	5939
IN	4386
US	2782
AR	1336
SY	1212
PH	377
GB	330
DE	288
ID	284

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	26
21-02 Comunicat ref sprijin acordat de catre România autorităților din Republica Slovacia în eforturile de combatere a pandemiei COVID-19	3
CCS/11441 Suman 52 mil 960 los casos confirmados de COVID-19 en el estado	2
Gửi bản mềm: Quyết định thành lập BCĐ, bìa sơ mi, phân công nhiệm vụ trong phòng chống dịch Covid-19	2
CCS/11441 (CON CORRECCIÓN EN CIFRA DE FALLECIDOS EN JUÁREZ) Suman 52 mil 960 los casos confirmados de COVID-19 en el estado	2
Revised Students List - Covid 19 Vaccination Programme (22.02.2021)	2
IMSS Boletín 078.- Trabajo coordinado entre IMSS y gobiernos estatales, estrategia clave para atender la pandemia de COVID-19 y recuperar servicios (FOTOS)	2
Fwd: CVASU COVID-19 Testing Lab report on 21/02/21	2
21.02.2021 ein Jahr Corona	1
COVID 19 Natore(21.02.2021)	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: 146,734
Domains with Potential Mail Servers: 2,562
Email-Capable Domains and Hosts: 53,484
Live Hosts and Domains Not Parked: 44,784

Mobile Apps

Apps in Official Stores: 515

by Store

Apple	255
Google	243
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,116

by Store Type:

Hybrid	1075
Secondary	973
Affiliate	68

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	26
Official	2
Hybrid	1