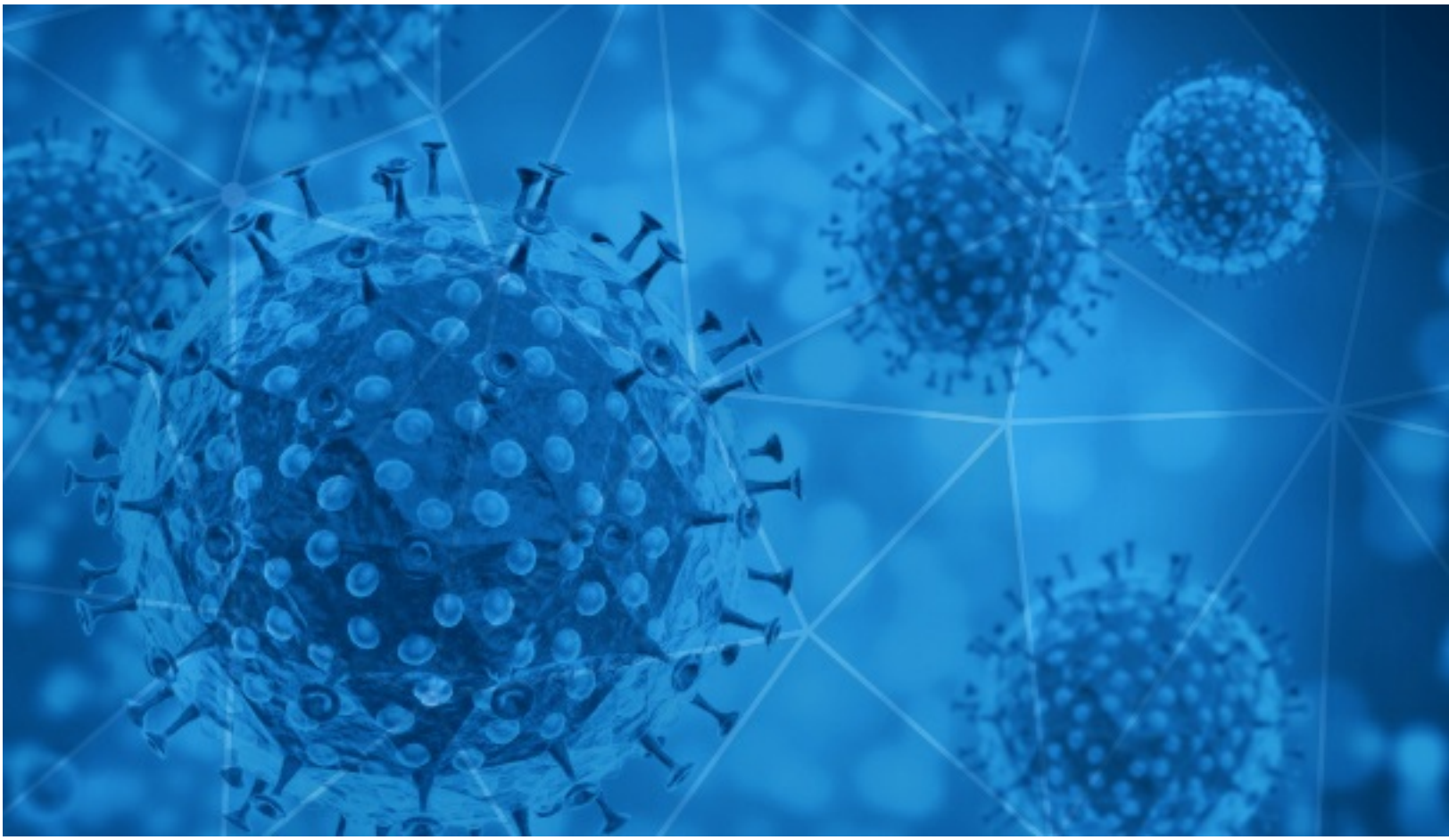
RiskIQ i3:

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

2021-02-04



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 2021-02-03 to 2021-02-04. During this period, RiskIQ analyzed 55,392 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 6,607 unique subject lines observed during the reporting period. The spam emails originated from 2,296 unique sending email domains and 4,505 unique SMTP IP Addresses. Analysts identified 10 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	20093
Coronavirus .�bergewichtige Menschen in Gefahr!	4983
The Corona Letter: A boost for single doses	3791
COVID TASTE RESULT	3619
COVID-19 Pantallas Protectoras	1068
COVID-19	979
CALABRIA: al via la seconda edizione bis di "Riapri Calabria". Contributo una tantum alle imprese interessate dagli effetti negativi dell'emergenza epidemiologica da Covid-19. Domande dal 10 al 15 febbraio 2021.	460
Controla el COVID de Forma Efectiva y Segura en tu Empresa	437
Re: Corona virus Protection Pills.Order confirmation	335
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!!!	281
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove...etc.	278
Flu/Covid-19 Weekly questionnaire - Reminder week 5	266
Vandenbroucke: ‘Hoge nood aan kappersbezoek, maar zeker geen verdere versoepelingen’ - Hoe zit het nu eigenlijk met de kabbelende coronacijfers?- Antwerpse leerling bouwt school volledig na in computerspel - ‘Ook mensen met psychiatrische...	244
CE FDA 510K GLOVES covid-19 Vaccine ,back to me	239
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW...	232
Mi seguro insumos covid 19 protege a tu familia	221
Your Ultimate Protection against COVID-19. US FDA Registered	217
Public Relation Facebook Covid-19 Lottery	216
COVID-19: Employer support – live webinars	212
, See how Covid 19 Affected Your Pension Fund	211
[CND Español - 4329]. El Caribe se lanza a la desesperada con las pruebas de Covid	209
COVID LOANS FROM UNITED NATIONS	199
Restock On KN95 Certified Masks, America's #1 'Anti-COVID19' Face Protective Mask	187
NCJ Daily - HumCo Records 31st COVID Death, 22 New Cases. Huff Blasts GOP. Standoff in Westhaven. Vax Town Hall Today.	180
Join the Bowser Administration for a Community Leader Telephone Townhall on Coronavirus	173

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	20095
gmail.com	4776
dell.com	4065
timesofindia.com	3791
hospiramedical.co.uk	2065
mailinator.cl	1068
yandex.com	980
upc.at	919
163.com	904
tecademicsmail.com	696

Top-15 IPs Sending COVID Spam

115.238.247.228	3049
107.174.142.107	1935
188.166.230.198	978
103.225.52.66	723
103.225.53.120	722
114.104.155.95	639
103.225.54.193	594
103.225.54.216	540
103.225.52.239	484
103.225.54.79	463

Top-15 Countries Sending COVID Spam

JP	20501
US	9423
CN	5035
RU	4601
IN	4060
FR	2121
IT	2075
SG	1037
BR	840
--	661

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Healthy Driven | One of the most baffling aspects of COVID-19, and more	2
URGENT TENDER#675320 (covid19 kits)	1

Top-15 Subjects Containing doc/xlsx Files

WEBINAR COVID 19 Sicurezza Lavoro: adempimenti anti-contagio, controlli e responsabilità-29/3/21	44
ADEFARMA y B+SAFE se unen para blindar las farmacias madrileñas frente al COVID	3
Fwd: HKUEAA Webinar - Engineer's Contribution in Combating COVID-19 - Planning and Construction of Quarantine Camps	3
NP El efluvio telógeno agudo, otro efecto secundario derivado del coronavirus	3
Las asociaciones de pacientes solicitan que las personas con enfermedades reumáticas reciban la vacunación del coronavirus lo antes posible	2
RE: UNICEF FUNDS catalytic funds covid 19	2
***IMPORTANT* Bulk Quote Request-Covid19**	2
Re: Thoughts and advocacy on COVID vaccines please	2
RV: SEGUIMIENTO PACIENTES COVID	1
WG: CoronavirusPandemie - Info: Freistellung von der Arbeit zur Betreuung von Kindern	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: 141,195
Domains with Potential Mail Servers: 2,564
Email-Capable Domains and Hosts: 51,216
Live Hosts and Domains Not Parked: 43,904

Mobile Apps

Apps in Official Stores: 510

by Store

Apple	252
Google	241
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,072

by Store Type:

Hybrid	1061
Secondary	944
Affiliate	67

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1