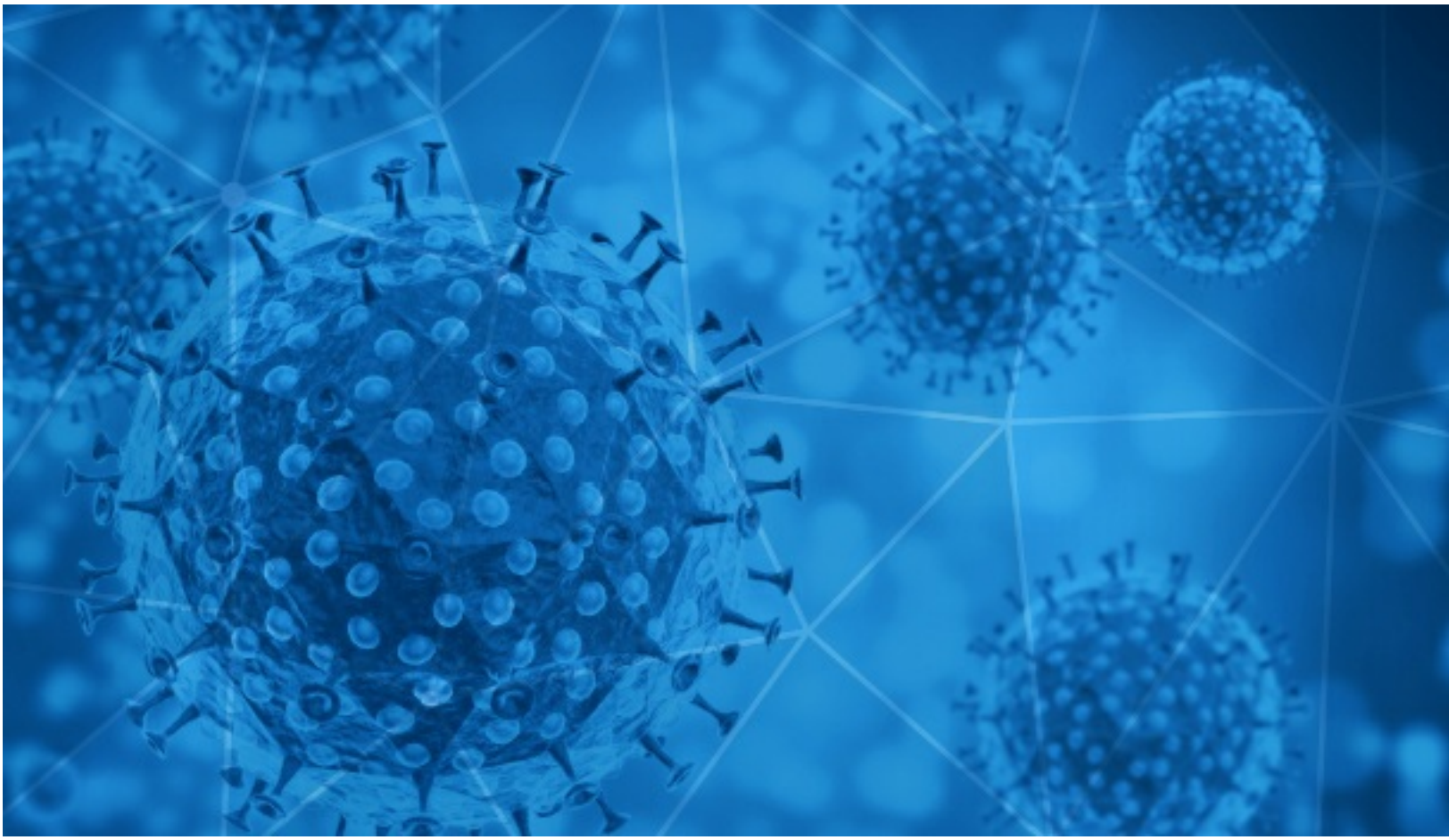
RiskIQ i3:

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

2021-01-21



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 2021-01-20 to 2021-01-21. During this period, RiskIQ analyzed 29,662 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,813 unique subject lines observed during the reporting period. The spam emails originated from 2,272 unique sending email domains and 4,023 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Hesitancy's hitting vaccination targets	3505
Re:Happy New Year! Your Covid-19 Grant .	1332
Are you Alive? (Covid -19 Security Alert)	1065
Puricador y Sanitizador de Aire, Estirilización contra Coronavirus	960
Evita contagio masivo en tu EMPRESA, despistaje de COVID-19 Prueba Hisopado en 15 minutos, somos IMPORTADORES	922
COVID-19 Pantallas Protectoras	787
Tell us your opinion on the Covid Vaccine and select from several offer rewards!	542
Gran Venta Outlet - Productos Covid 19	535
Re:Happy New Year! Your Covid-19 Grant .	533
Finally, Painless COVID19 Testing At Home- All New Pulse Oximeter Will Detect Traces Of Virus In Blood	456
Know If You Have COVID19 In Minutes Using All New Pulse Oximeter- Painless Test At Home	420
Painless COVID19 Testing At Home, Find Results In Minutes- Take An Additional 50 Percent Off Today	400
Defeat Coronavirus, Thermographic Camera	374
Re: Defeat Coronavirus, non contact fever alarm device	359
Contactless infrared body temperature thermometer defeat Coronavirus	351
Thermographic Automation Camera defeat Coronavirus	351
HERZLICHEN GLÜCKWUNSCH, CASH COVID-19 PALLIATIVEN AUS MEINEN LOTTERIEGEWINNEN	315
LJC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation	299
COVID-19 Relief Fund	298
Re: Corona virus Protection Pills.Order confirmation	294
COVID19 LOAN FROM THE UNITED NATIONS WITH NO INTEREST RATE	289
Re:Your Covid-19 Grant .	288
Arma tu Kit contra el Covid-19	272
Formación obligatoria para los trabajadores sobre COVID-19	258
Re: Digital signage solution for Covid-19	246

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	3512
teemanjay.net	2155
gmail.com	1670
keyable.net	1435
hospiramedical.co.uk	1347
taliskerwhiskychallenge.com	1276
yahoo.com	1154
correosmasivos.cl	960
focazen.com	922
mailinator.cl	673

Top-15 IPs Sending COVID Spam

113.116.206.80	1352
194.116.228.140	1274
180.235.232.196	1064
185.215.150.204	832
51.83.246.183	794
195.62.32.240	542
82.223.21.194	533
86.104.194.112	515
221.148.30.225	503
180.235.192.5	444

Top-15 Countries Sending COVID Spam

US	6052
IN	3735
FR	3273
CN	2294
--	1862
NL	1322
ES	1133
JP	1130
KR	824
RU	727

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

COVID 19 WEB ON LINE ANTICORRUZIONE E TRASPARENZA: proroga al 31/03/2021 del PTPCT – 24/02/2021	7
Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	6
CCS /11145 La vacuna COVID-19 se aplica sin contratiempos en Chihuahua: Secretaría de Salud	2
Estou compartilhando o arquivo 'FICHA PARA REGISTRO DE VACINAÇÃO CONTRA COVID-19- versão região Leste' com você	2
IMSS FOTO NOTA.- Inauguran Unidad Médica Temporal en Saltillo para convalecientes de COVID-19 (LINK VIDEO)	2
В Италии активно идет вакцинация от Covid'19 - Пресс-релиз	2
NOTA DE PRENSA - Minsa entrega camas UCI a Hospital Santa Rosa para ampliar la capacidad de atención a pacientes COVID-19	2
New Format Covid-19	1
NOTA COVID EN LA LIGA MX	1
UNICEF-FAO-WFP-WHO joint press release economic impact of COVID-19 and worsening inequalities will fuel malnutrition for billions in Asia and the Pacific	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: 140,265
Domains with Potential Mail Servers: 2,568
Email-Capable Domains and Hosts: 52,825
Live Hosts and Domains Not Parked: 45,615

Mobile Apps

Apps in Official Stores: 506

by Store

Apple	249
Google	240
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,042

by Store Type:

Hybrid	1050
Secondary	927
Affiliate	65

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1