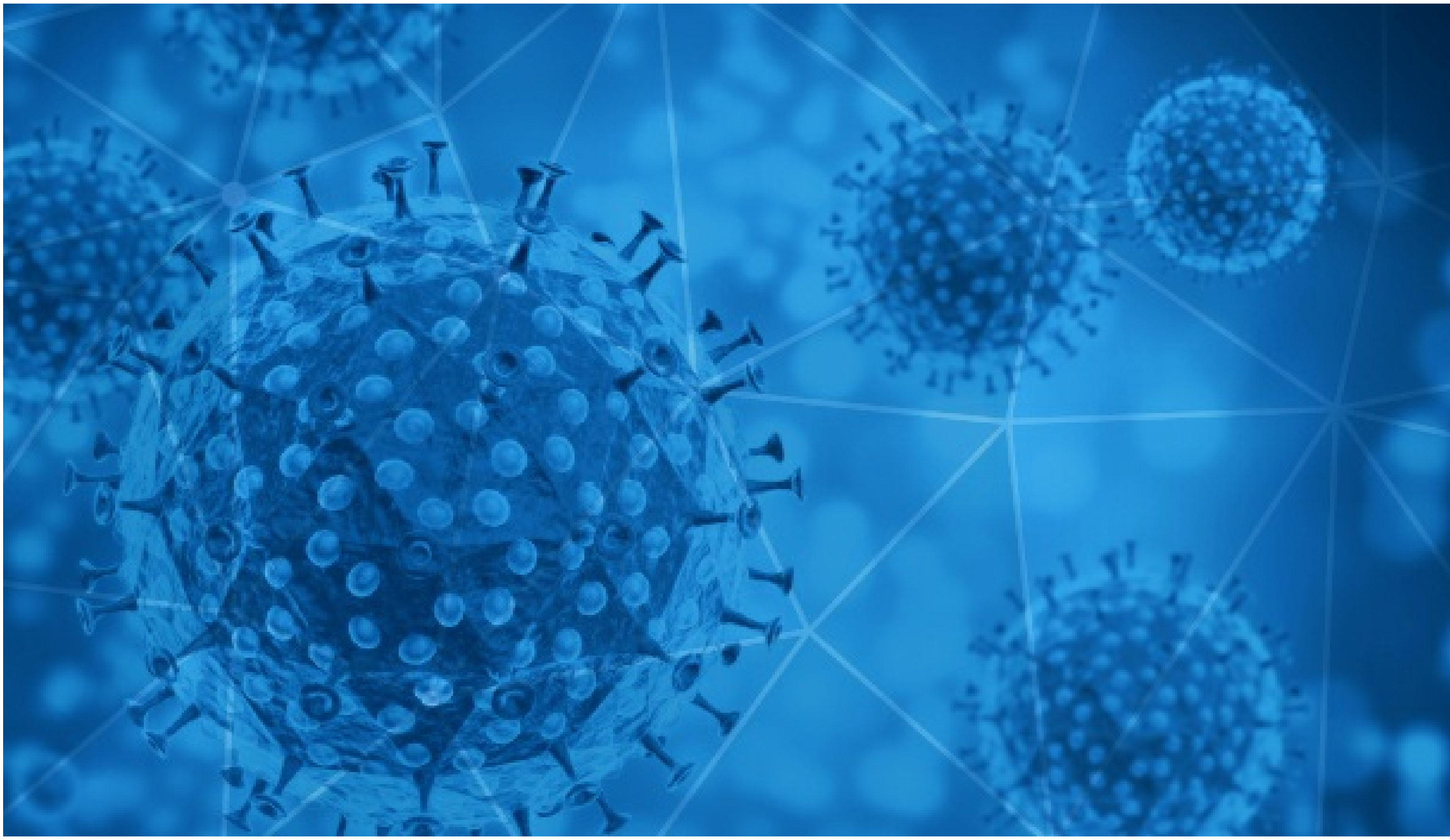
RiskIQ i3:

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

2021-03-12



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

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 2021-03-11 to 2021-03-12. During this period, RiskIQ analyzed 27,101 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,840 unique subject lines observed during the reporting period. The spam emails originated from 2,319 unique sending email domains and 4,255 unique SMTP IP Addresses. Analysts identified 33 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: What is clinical trial mode?	3596
¡No dejemos de cuidarnos, Pruebas de detección Covid-19!	1493
Agenda tu cita para la vacuna contra el COVID19	1412
SIAMO A PRESENTARLE IL NUOVO TEST SALIVARE COVID-19 ANTIGEN SPITTEST PCL.	1036
COVID-19 Vaccines for Rural Veterans, Employment Opportunities, Better Ways to Lose Weight	875
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	796
Protección contra el Covid	630
covid 19 financial support.	612
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove...etc.	361
Re: Digital signage solution for Covid-19	330
Gran Venta Outlet - Productos Covid 19	325
Google Alert - "You need this right nowfor fight Covid and Fun"	322
Pruebas de Antígenas para Covid-19 a empresas, envíos a todo el Perú	263
□Fiscalización Laboral ☝ últimos Cambios en Entorno Covid	249
Conheça as iniciativas da OAB no enfrentamento à pandemia de coronavírus.	229
Claim Your Fifty Dollar Johnson&Johnson COVID Vaccine Survey Reward	217
Kit de Pruebas Antígenas para COVID-19, Envíos a todo Perú.	212
Safety requirements for the new Corona - متطلبات السلامة لفيروس كورونا الجديد	184
Destination Thailand News - News Alert - How Long Will Take for Life Return to Normal After Covid?	180
Fiscalizacion Laboral últimos Cambios en Entorno covid	180
Re: covid-19 touch monitor	173
covid 19 financial support !	161
DirectAxis Special Covid-19 Offer at Lower Rate.	156
How COVID-19 has accelerated the need from an annual planning to an ongoing process	154
Arma tu Kit contra el Covid-19	151

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	3597
sanens.pe	1493
saludtotal.com.co	1422
sicurezzanews.it	1036
messages.va.gov	978
gmail.com	949
mail2royal.com	796
aol.com	699
mkpp31tn-liquidwebsites.com	563
126.com	503

Top-15 IPs Sending COVID Spam

200.31.17.85	1420
61.114.14.8	676
82.135.19.131	571
67.227.155.81	563
157.245.42.150	539
82.135.19.130	464
116.231.161.76	361
67.219.150.138	322
104.131.18.226	274
79.139.57.163	263

Top-15 Countries Sending COVID Spam

US	11012
IN	3771
DE	2003
AR	1634
CN	1136
JP	1068
FR	973
GB	700
BR	405
PL	383

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Invoice for Healt Product For Covid-19	30
PI: Dating während Corona: Lollipop-Selbsttests statt Video-Calls	1

Top-15 Subjects Containing doc/xlsx Files

Бесплатная раздача защитных комплектов от covid-19 (Минздрав РФ)	15
UA massifica testes à covid-19 combinando saliva, testes e plataforma digital	6
BLANK covid neg	3
IMSS Boletín 104.-Sistema de salud respondió como uno solo para atender la emergencia sanitaria por COVID-19 (LINK DE VIDEO Y FOTOS)	3
Presentación resultados encuesta del nuevo consumidor español en la era COVID: "mobile first", cada vez más digitalizado y exigente con las marcas	3
Interessensbekundung als Coronatesthelfende/r in den Einrichtungen der Eingliederungshilfe im Land Berlin	2
FW: .Mjere u cilju suzbijanja pandemije COVID-19 za period 10.03. - 17.03.2021.	2
Press Release: Global Immunization Possible by 2022 With Fair Vaccine Distribution, says WHO COVID-19 Special Envoy	2
Follow-up materials from today's meeting of the Finger Lakes Geriatric Education Center/University of Rochester AHRQ ECHO National Nursing Home COVID-19 Action Network	2
Protocol & Covid screening 24h prior appt	2

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: 149,098
Domains with Potential Mail Servers: 2,330
Email-Capable Domains and Hosts: 51,822
Live Hosts and Domains Not Parked: 46,240

Mobile Apps

Apps in Official Stores: 514

by Store

Apple	253
Google	244
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,184

by Store Type:

Hybrid	1110
Secondary	1006
Affiliate	68

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1