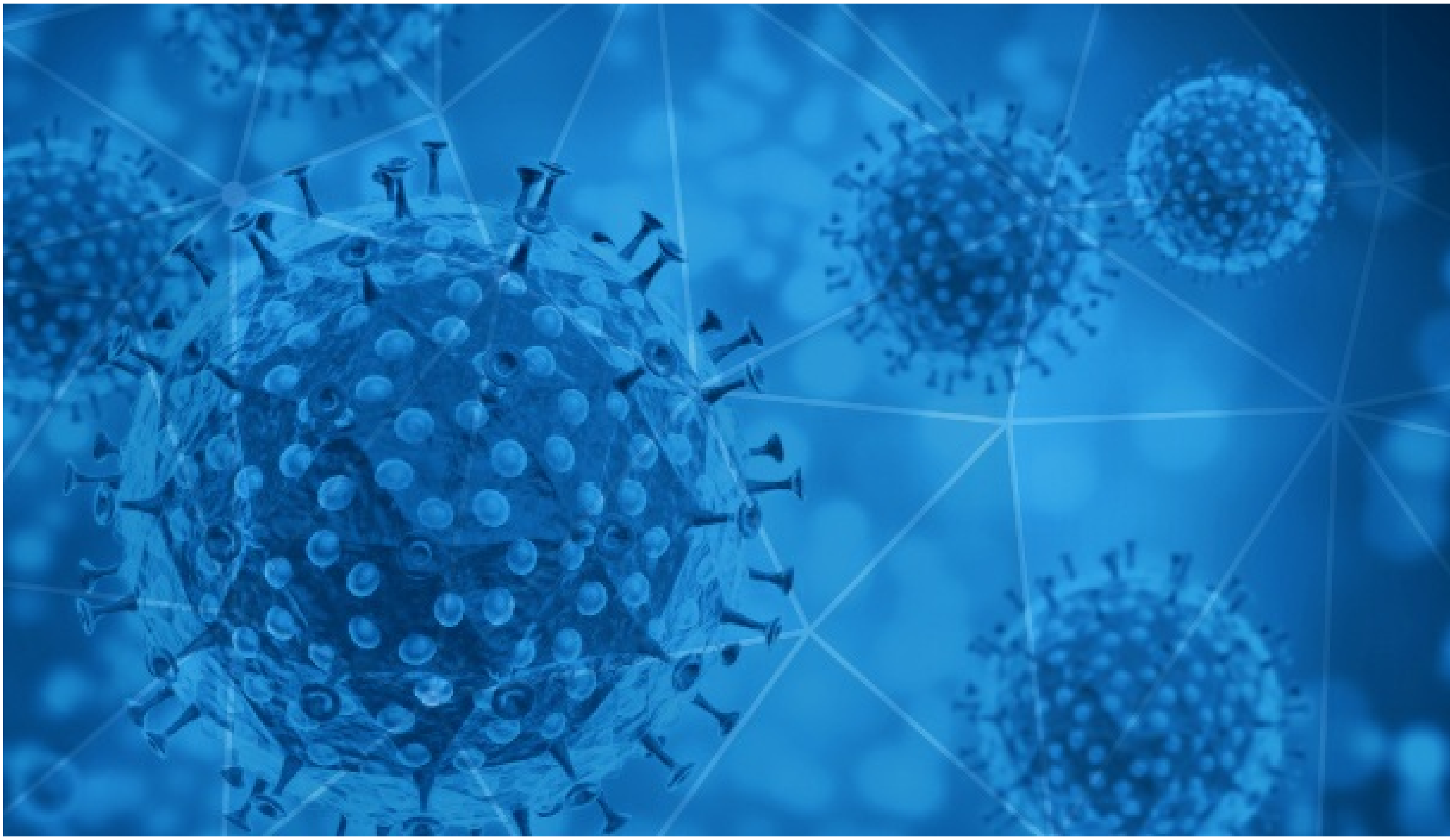
RiskIQ i3:

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

2020-12-04



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 2020-12-03 to 2020-12-04. During this period, RiskIQ analyzed 37,878 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 7,467 unique subject lines observed during the reporting period. The spam emails originated from 2,389 unique sending email domains and 5,712 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Can we vaccinate the kids now?	3651
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	2566
United Nations 2020 Covid-19 Compensation Payment.	2406
How I Lost My Job to COVID-19 and Ended Up Making Triple My Old Salary!	1691
Corona Schnelltest	1323
THIS Kills Way More Americans Than Coronavirus	1234
Corona-Hype - Trotzdem Frauen treffen	1074
Get your Corona-virus Mask while supplies last!	784
New Corona-virus Mask!	782
Reduce your risk of Corona-virus with this Mask	721
Traveling soon, wear this mask to fight chances of getting Corona-virus	691
Respuestas gerenciales para el post Covid19	593
World Health Organization Awards Department – Covid 19	424
Join the Bowser Administration for a Community Leader Telephone Townhall on Coronavirus	375
Covid-19 vï¿½dï¿½maszk hivatalos minï¿½sï¿½tï¿½ssel!	318
covid-19 vaccines	307
Trabajo Seguro Covid-19 Serprom Spa	280
India Means Business : Despite COVID-19, Foreign Direct Investment Doubles in Q2	251
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	235
Covid 19 benefit..(Get back to me fast)!	231
Re: Defeat Coronavirus, non contact fever alarm device	223
Contactless infrared body temperature thermometer defeat Coronavirus	220
Testy kasetkowe na COVID19 - chroń siebie lub firmę - 99% skutecznoci	210
covid-19 pandemic relief fund-2020	208
Re: COVID-19 RESPONSE FUND	207

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

mscbs.gob.es	4310
timesofindia.com	3656
clrvisor.net	2978
protonmail.com	2248
gunlock.buzz	1691
gmail.com	1610
covid-19-schnelltests-24.de	1323
kihiio.cam	1234
zanthia.de	1074
163.com	850

Top-15 IPs Sending COVID Spam

69.94.140.109	2977
150.95.82.182	2406
107.158.49.34	1690
193.223.106.171	1234
46.20.37.54	1074
190.247.242.189	455
101.79.49.115	424
113.89.41.141	421
117.30.167.231	307
120.229.72.140	229

Top-15 Countries Sending COVID Spam

US	12650
RU	4619
IN	3982
SG	2650
--	2625
CN	2018
DE	1898
GB	1268
AR	650
KR	544

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

“COVİD-19-la mübarizədə birlikdə güclüyük” vebinarı keçirilib Evdə müalicə zamanı yaranan ağırlaşmalar müzakirə olunub	5
Press Release; Source4Less to Bring Full Line of Wood Products to Middle East in Response to post-COVID Construction Trends	5
FW: Returnees due to Covid 19 Pandamic	2
COVID-19 Update for Businesses:	2
+++ VACCINAZIONI IN GRAVIDANZA: GLI IMMUNOLOGI, PROTEGGERSI DA INFLUENZA E PERTOSSE IN ATTESA DELL'ANTI-COVID	2
RE: 49100001 - F300 - Batches UCORONA	1
Covid-19 Questionnaire	1
NP-Disponen financiamiento para adquirir equipos de cadena de frío en vacunas contra la COVID-19	1
Info Covid : La tenue des AG et CA à distance est prorogée jusqu’au 1er avril 2021	1
Fwd: ENC: PLACAS PARA IMPRESSÃO EM PS E ADESIVO - NOVA CAMPANHA COVID	1

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: 134,634
Domains with Potential Mail Servers: 2,606
Email-Capable Domains and Hosts: 51,350
Live Hosts and Domains Not Parked: 45,109

Mobile Apps

Apps in Official Stores: 477

by Store

Apple	240
Google	222
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,846

by Store Type:

Hybrid	954
Secondary	833
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1