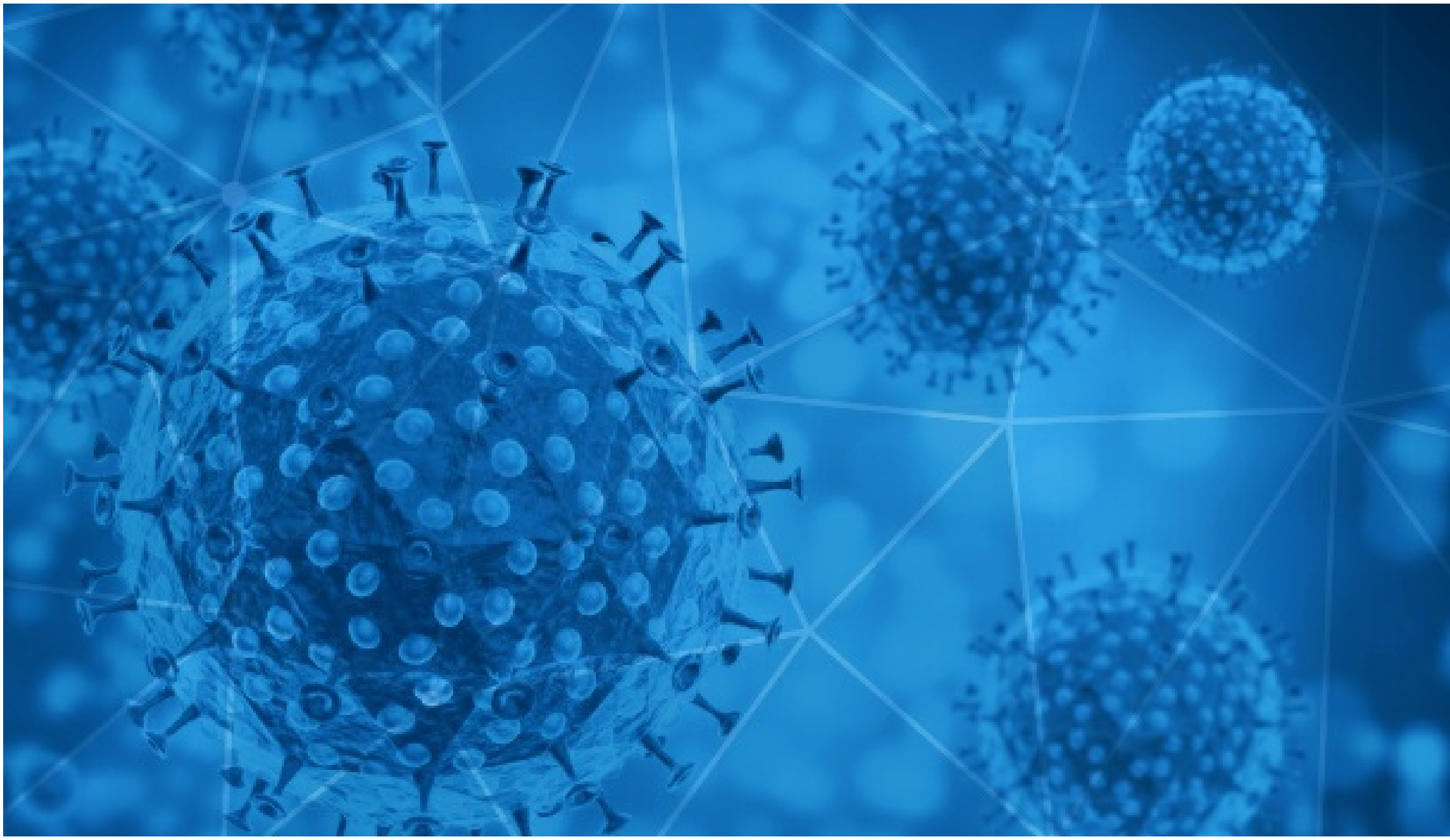
RiskIQ i3:

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

2020-08-12



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 2020-08-11 to 2020-08-12. During this period, RiskIQ analyzed 47,085 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,209 unique subject lines observed during the reporting period. The spam emails originated from 1,925 unique sending email domains and 4,536 unique SMTP IP Addresses. Analysts identified 2 emails which sent an executable file for Windows machines.

Top-25 Subjects

Russia approves experimental COVID-19 vaccine, how scientists are keeping Antarctica coronavirus-free, and more from Apple News	4424
Covid-19 Face Mask	3307
Help the world's response to Covid-19 with the most protective mask on the market.	3265
Wearing a KN95 mask is your best defense against coronavirus	3243
The Corona Letter: From Russia, in secrecy	2115
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	1104
Precios Imbatibles / Productos COVID 19	976
Protect Scores During Coronavirus	809
COVID-19 And Your Credit Health	792
Will COVID-19 Impact Your Credit Scores?	778
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	585
REDEEM COVID-19 RELIEF PAYMENT AND RECEIPT	484
Contactless infrared body temperature thermometer defeat Coronavirus	461
Re: Defeat Coronavirus, non contact fever alarm device	451
Seminario Taller Fiscalización de La Dirección del Trabajo en Covid 19	425
ANTI-COVID "Touchless" Thermometer. Laser tech let's you take their temp from a distance!	418
Avoid COVID with this "touchless" infrared thermometer.	384
Re: keep away from Covid-19	372
PRODUCTOS DE PROTECCION COVID 19	347
Marketing during Covid19 - Keep your Brand Moving Forward	347
Desinfectamos su ambiente de coronavirus	316
Financial global Covid-19 pandemic helping hand	293
Desinfeccion covid19 mediante termoniebla	287
Desinfeccion Preventiva Covid19	279
COVID 19 Pandemic	271

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

insideapple.apple.com	4603
hotmail.com	3485
righla.casa	2379
timesofindia.com	2115
126.com	1902
gratueberates.cyou	1797
gmail.com	1750
ithimple.cyou	1685
extric.icu	1617
ithimple.casa	1404

Top-15 IPs Sending COVID Spam

82.223.122.119	3307
23.231.110.144	2374
170.130.213.97	1797
23.231.110.135	1684
170.130.213.96	1615
23.231.110.134	1391
198.199.121.161	1103
113.89.41.239	603
69.94.156.26	582
190.247.226.46	565

Top-15 Countries Sending COVID Spam

US	24344
ES	4301
CN	3904
IN	2776
DE	2170
FR	1272
AR	1100
CL	771
--	670
NL	576

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

TR: Etude PERSO-COVID : suivi sérologique et clinique post COVID-19	1

Top-15 Subjects Containing doc/xlsx Files

Czas pracy kierowców 2020 z uwzględnieniem zmian COVID-19 - szkolenie on-line	4
COVID-19 RELIEF FUNDING	3
Informasjon og egenerklæring Covid 19	2
Press Release: Taulia: Over 60%!o(MISSING)f Businesses Are More Interested in Early Payment as a Result of COVID-19 - Order# 52264107	2
PRESS STATEMENT: Polio vaccination campaigns resume in Afghanistan and Pakistan after COVID-19 disruptions leave 50 million children unimmunized.	2
“PROMOVIENDO LA SOSTENIBILIDAD AMBIENTAL EN LAS MIPYMES EN EL CONTEXTO DEL COVID-19”I	2
SDPI Press Release (URDU & English) for today’s online consultative dialogue ‘Textile sector's competitiveness amid Covid19’ organised by SDPI at Islamabad	2
REMITE REPORTE COVID 19 DEL PERSONAL CAS DE LA EESTP-PNP-TRUJILLO DEL DIA MARTES 11AGO2020.	2
Covid-19 Related Products Price List	2
NHSN LTC COVID-19 Data Quality Webinar	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: 118,947
Domains with Potential Mail Servers: 2,893
Email-Capable Domains and Hosts: 43,848
Live Hosts and Domains Not Parked: 65,567

Mobile Apps

Apps in Official Stores: 383

by Store

Apple	201
Google	173
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,030

by Store Type:

Hybrid	648
Secondary	340
Affiliate	42

Blacklisted Mobile Apps: 24

by Store Type:

Secondary	21
Official	2
Hybrid	1