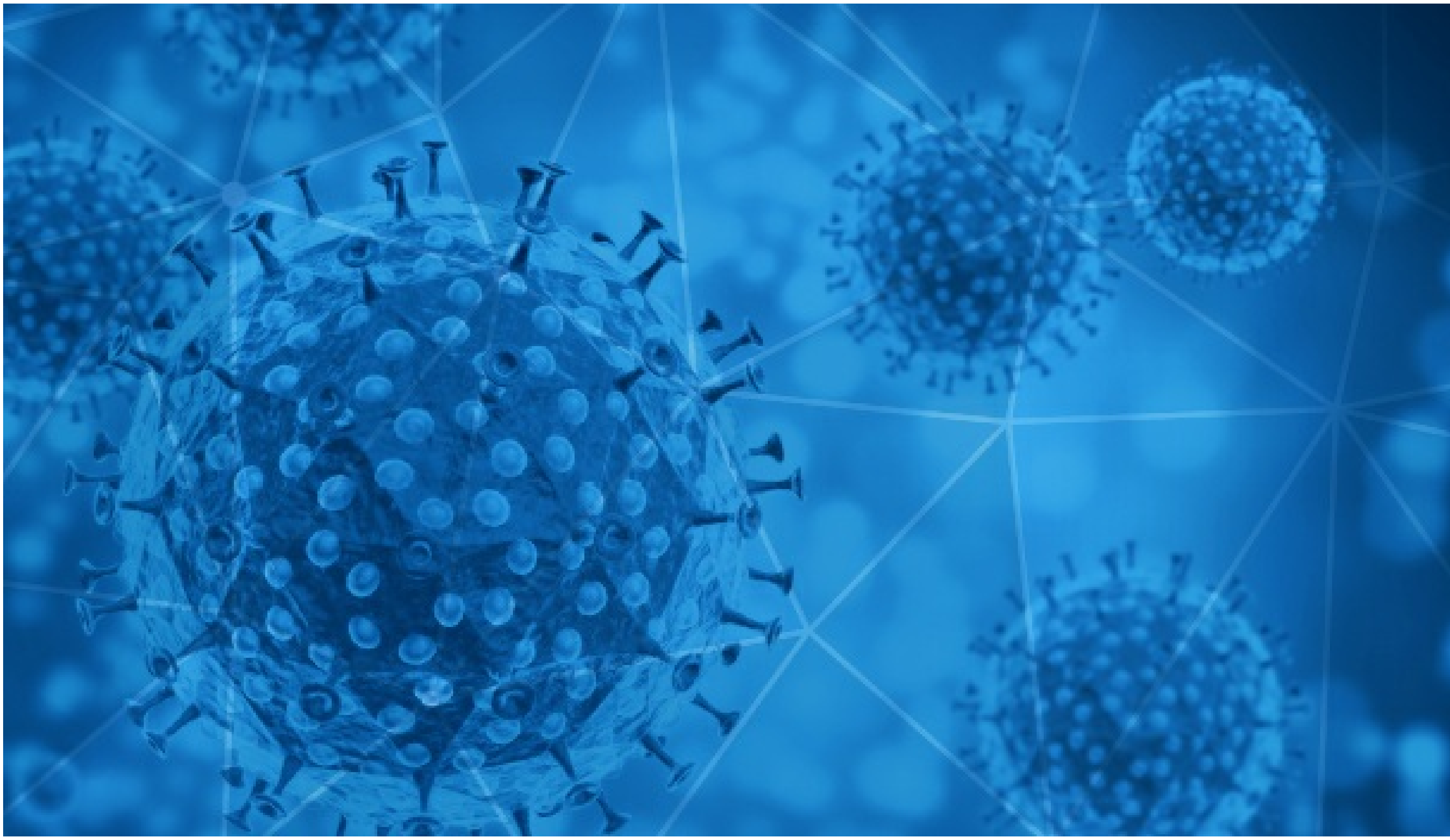
RiskIQ i3:

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

2020-08-04



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 2020-08-03 to 2020-08-04. During this period, RiskIQ analyzed 36,139 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,921 unique subject lines observed during the reporting period. The spam emails originated from 1,773 unique sending email domains and 3,885 unique SMTP IP Addresses. Analysts identified 18 emails which sent an executable file for Windows machines.

Top-25 Subjects

Coronavirus Pandemic Loan (COVID-19)	2698
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	2240
The Corona Letter: Surprising findings on household transmission	2194
PyMEs contra el COVID19	1138
COVID-19 And Your Credit Health	962
Will COVID-19 Impact Your Credit Scores?	913
Protect Scores During Coronavirus	909
OPPORTUNITA' Credito di imposta "COVID19" per le spese di sanificazione, acquisto DPI	818
Are you even more susceptible to COVID-19 complications?	676
covid-19 and children - how does it affect them?	623
Is your weight increasing your chances of COVID-19 complications?	616
Solución contra Covid-19: Medición de temperatura sin contacto	607
Re: Tenemos que adaptarnos a la situacion Covid-19	497
Re: Hay que adaptarse a la nueva situacion Covid-19	494
Re: Adaptados a la nueva situacion Covid-19	485
Re: Nos tenemos que adaptar a la situacion Covid-19	477
Re: Hay que adaptarnos a la situacion Covid-19	454
Re: Nos adaptamos a la nueva situacion Covid-19	449
Re: Estamos adaptados a la nueva situacion Covid-19	440
Re: Estamos adaptados a la situacion Covid-19	420
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	415
Let’s fight together to get through the COVID-19	360
Test Rapido Covid-19 Mascarillas e Insumos	333
Covid 19 Wohltätigkeitsfonds	326
Glimpses of our various COVID-19 relief activities	317

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmail.com	3618
gov-sba.us	2698
blankellie.icu	2665
timesofindia.com	2195
countermail.com	1822
126.com	1356
miracleredmyx.us	1292
sicurezzanews.it	818
seorazor.com	658
renaultplanargentina.com	636

Top-15 IPs Sending COVID Spam

170.130.213.102	2662
181.46.136.168	2240
104.140.224.150	1291
201.231.83.182	895
185.164.7.139	600
201.231.4.61	590
185.164.5.223	543
185.164.7.181	509
185.164.7.121	464
82.135.19.130	430

Top-15 Countries Sending COVID Spam

US	10448
DE	5005
AR	4386
CN	3075
IN	2743
AT	2555
FR	1502
--	1254
BR	649
BE	602

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

RE: Delayed Payment Due To COVID-19 Situation	16
SIGNALE : Enquête surcoûts covid 19 BOP 303 et 104	1

Top-15 Subjects Containing doc/xlsx Files

CUMPLIMIENTO DE PROTOCOLOS DE BIOSEGURIDAD PARA MANEJO DE PANDEMIA CORONAVIRUS - COVID19	9
PHHS 8 3 2020 COVID 19 End of Day Summary	5
AHF hace un llamado de urgencia al Gobierno de República Dominicana a tomar medidas y acciones para detener la pandemia de COVID-19.	4
PPE Dashboard downloaded from NDOH Covid Dashboard - 3rd August 2020	2
Tagliaferri (Fdi): Bonaccini pretenda chiarezza sui documenti tecnici sul Coronavirus	2
Covid 19 Questionnaire in live	2
Hospital Daily EMResource COVID-19 Reporting Results - 8/3/2020	2
Re: QA Automation Engineer @ Englewood Cliffs, NJ (Remote During COVID)	2
RE: Covid-19 articles par levels - REVISED V.05 ship request 1-08-20	2
Post Covid, tiempo para desaprender y volver a aprender nuevas formas de trabajar	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: 117,817
Domains with Potential Mail Servers: 2,864
Email-Capable Domains and Hosts: 44,389
Live Hosts and Domains Not Parked: 67,140

Mobile Apps

Apps in Official Stores: 368

by Store

Apple	195
Google	164
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 947

by Store Type:

Hybrid	610
Secondary	297
Affiliate	40

Blacklisted Mobile Apps: 23

by Store Type:

Secondary	20
Official	2
Hybrid	1