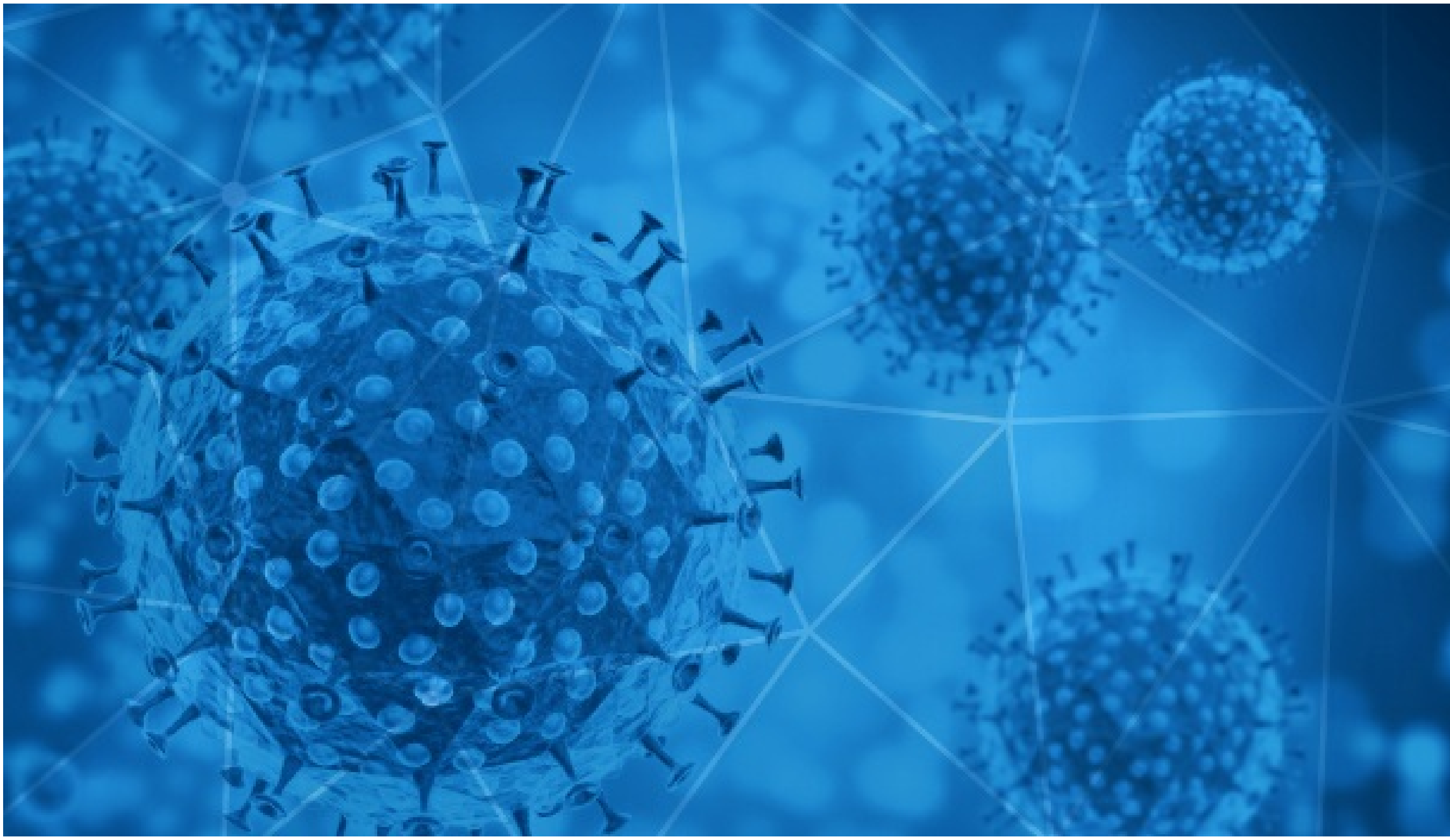
RiskIQ i3:

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

2020-08-10



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 2020-08-09 to 2020-08-10. During this period, RiskIQ analyzed 21,762 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,406 unique subject lines observed during the reporting period. The spam emails originated from 755 unique sending email domains and 2,602 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: A call to protect doctors	2383
financial support for this COVID-19	1463
Help the world's response to Covid-19 with the most protective mask on the market.	922
Covid-19 Face Mask	855
Wearing a KN95 mask is your best defense against coronavirus	836
Charter Air Service/Fast Air service/Mask /Covid-19 test/Medical equipment	715
17-Y-O DAD killed, 20 injured as gunmen open fire @ block party + US coronavirus cases top 5 MILLION	687
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	578
Incontri online in Italia (no corona)	487
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	424
Desinfeccion Preventiva Covid19	363
Desinfectamos su ambiente de coronavirus	360
Re: Vanity upon Vanity COVID-19..	352
Desinfeccion covid19 mediante termoniebla	349
Re: Nos tenemos que adaptar a la situacion Covid-19	338
Re: Tenemos que adaptarnos a la situacion Covid-19	321
Re: Estamos adaptados a la situacion Covid-19	314
Re: Adaptados a la nueva situacion Covid-19	311
Contactless infrared body temperature thermometer defeat Coronavirus	304
Re: Estamos adaptados a la nueva situacion Covid-19	298
Re: Hay que adaptarnos a la situacion Covid-19	292
Industrial plant, Covid-19 Mask	291
Re: Nos adaptamos a la nueva situacion Covid-19	281
Re: Defeat Coronavirus, non contact fever alarm device	277
Re: Hay que adaptarse a la nueva situacion Covid-19	272

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmail.com	3299
timesofindia.com	2384
126.com	1673
hotmail.com	1127
countermail.com	1072
proationizes.work	879
sleiched.casa	879
oceanbridgecargo.com	716
caribbeanfever.com	687
keyable.net	581

Top-15 IPs Sending COVID Spam

45.143.223.105	1463
170.130.213.72	878
170.130.213.73	876
106.75.37.217	854
103.30.17.20	715
190.247.223.99	645
113.89.41.8	525
5.199.131.7	487
181.46.136.168	424
60.255.137.67	352

Top-15 Countries Sending COVID Spam

US	5435
CN	4078
DE	3131
IN	2486
AR	1530
--	1501
HK	716
KR	421
BR	410
BE	254

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

ANC Weekly COVID-19 Reports	23
COVID-19 RELIEF FUNDING	8
Covid-19 compensation fund	4
Boletín SEP no. 212 - Anuncia SEP programa de servicio social para que jóvenes universitarios apoyen a disminuir el rezago educativo provocado por COVID-19	3
DEAR LUCKY WINNER:__YOU HAVE WON RS 7 CRORE AND 2 LAKH RUPEES :_From (W.H.O. WORLD HEALTH ORGANISATION COVID-19 AWARD DONATIONS PROMO 2020.	3
IMSS VERSIÓN ESTENOGRÁFICA Y AUDIO. Palabras de la jefa de Nutrición y responsable del Banco de Leche UMAE HGO 4, Minerva Lara Fuentes, Conferencia Coronavirus en México, Palacio Nacional	2
R: COMUNICATO STAMPA CONGIUNTO COMITATI FAMILIARI VITTIME COVID EMILIA ROMAGNA E CODACONS EMILIA ROMAGNA	2
GlobalSurg-CovidSurg Week study: invitation	2
■■■ 48 ■■■■■■■■■■ ■■■■■■■■■■■■■■ ■ ■■■ ■■■■■■■■■■ ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ BRN ■■■■■■■■■■■■ ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ COVID – ■■ ■■■■■ ■■■■■■■■■■	1
Re: KHẢO SÁT VỀ TÌNH HÌNH DỊCH BỆNH COVID 19	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: 118,694
Domains with Potential Mail Servers: 2,884
Email-Capable Domains and Hosts: 43,165
Live Hosts and Domains Not Parked: 65,091

Mobile Apps

Apps in Official Stores: 380

by Store

Apple	201
Google	170
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,008

by Store Type:

Hybrid	639
Secondary	327
Affiliate	42

Blacklisted Mobile Apps: 24

by Store Type:

Secondary	21
Official	2
Hybrid	1