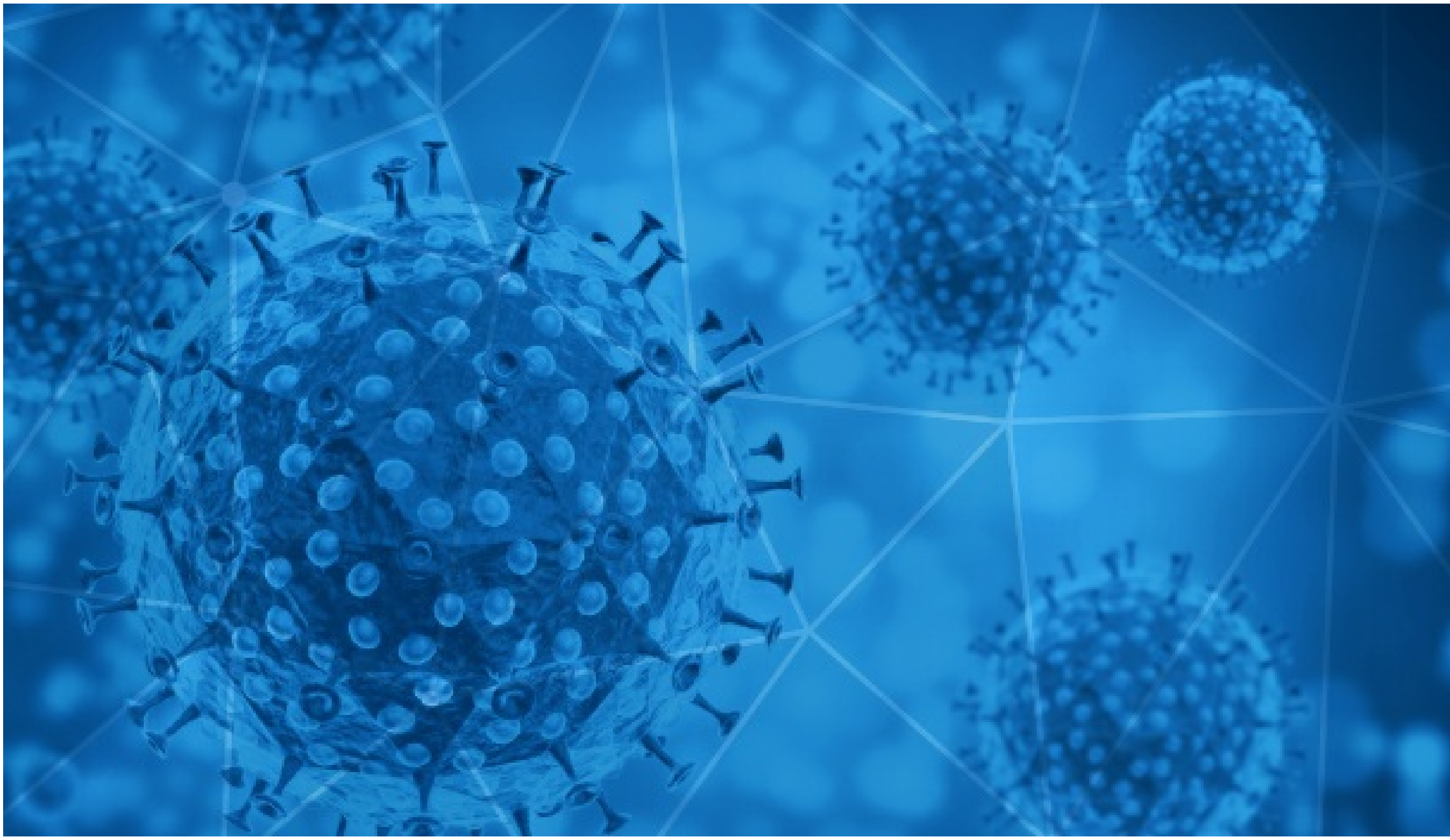
RiskIQ i3:

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

2020-06-23



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 2020-06-22 to 2020-06-23. During this period, RiskIQ analyzed 30,769 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,880 unique subject lines observed during the reporting period. The spam emails originated from 2,210 unique sending email domains and 3,928 unique SMTP IP Addresses. Analysts identified 749 emails which sent an executable file for Windows machines.

Top-25 Subjects

COVID-19 Claim Promo	2891
The Corona Letter: Generics bring good news	2846
Your loan A/c with SBI: Relief under RBI's COVID-19 Package.	1109
(COVID-19) - CLAIMS!!	1076
Can UV Light Kill or Prevent Coronavirus?	995
COVID 19 SUPPORT ITEMS	731
D.L. Hughley Tested Positive for COVID19 + Noose Found in Black NASCAR Driver Bubba Wallace’s Stall	722
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	671
COVID-19 / DONATION FOR YOU	657
FW: *IMPORTANT* Bulk Quote Request-Covid19	601
Covid-19 Credit Facility Business Owners	482
Covid 19 Wohltätigkeitsfonds	471
l'ANTI COVID è la sanificazione quotidiana…	444
Long Lasting and Eco-Friendly Disinfectant to Fight Covid19…	421
Re: Washington Department of Licensing COVID-19 Updates and News	365
Ofertas COVID -19	362
COVID-19 Protection Products	362
Protección contra el COVID-19 - Te ofrecemos el mejor precio del mercado - ENTREGA INMEDIATA	342
Test Rápido Covid-19 Mascarillas e Insumos	305
Minimice el Riesgo de contagio del Coronavirus - Validacion Biometrica	270
Protección COVID-19	235
JUNE: CORONAVIRUS RELIEF FUND	223
[POSSIBLE-SPAM] Re: COVID-19 (CORONA VIRUS 2020 COMPENSATION FUNDS	212
COVID-19	206
Insumos de Protección COVID-19	191

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmail.com	4632
yahoo.com	3112
timesofindia.com	2850
126.com	1501
sbi.co.in	1109
foxmail.com	1017
163.com	902
caribbeanfever.com	724
countermail.com	633
outlook.com	608

Top-15 IPs Sending COVID Spam

190.211.241.74	2891
103.30.17.43	995
104.168.200.185	731
212.227.254.175	657
103.140.251.220	599
148.72.151.127	573
187.174.101.179	482
190.64.5.7	471
119.122.88.25	426
152.67.129.137	362

Top-15 Countries Sending COVID Spam

US	7528
IN	4405
CN	3078
PY	2892
DE	1900
TR	1188
HK	1029
CA	932
AR	768
--	693

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

COVID 19 SUPPORT ITEMS	731
FW: *IMPORTANT* Bulk Quote Request-Covid19	1
Fw: APPOINTMENT FOR PERIODIC COVID-19 SWAB TESTS IN PREPARATION FOR SAFE AND CONTROLLED RESTART OF CONSTRUCTION SECTOR	1

Top-15 Subjects Containing doc/xlsx Files

FW: *IMPORTANT* Bulk Quote Request-Covid19	178
Request for quote-COVID-19 protein and antibody.	113
Important : Post-Coronavirus	10
La Asociación Empresarial Hotelera de Madrid colaborará en el SICUR ESPECIAL COVID en su compromiso con el sector	6
La recogida neumática de basuras mantuvo operaciones 100% durante el periodo COVID-19	3
PHHS 6 22 2020 End of Day COVID 19 Summary	3
duyuru - COVID-19 Kapsamında Kurum İçi Düşük Katılımlı Toplantılarda Alınması Gereken Önlemler	2
NdP La ONCE reparte 25 millones en el primer fin de semana de sorteos tras el Covid-19	2
St. Francis Hospital Roslyn New York (CHSLI) COVID-19 Visitation Program	2
Hospital Plató de Barcelona implanta el primer sistema de videovigilancia de alta resolución para enfermos de Covid19	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: 108,629
Domains with Potential Mail Servers: 2,738
Email-Capable Domains and Hosts: 41,616
Live Hosts and Domains Not Parked: 44,998

Mobile Apps

Apps in Official Stores: 301

by Store

Apple	170
Google	123
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 745

by Store Type:

Hybrid	458
Secondary	253
Affiliate	34

Blacklisted Mobile Apps: 20

by Store Type:

Secondary	19
Official	1