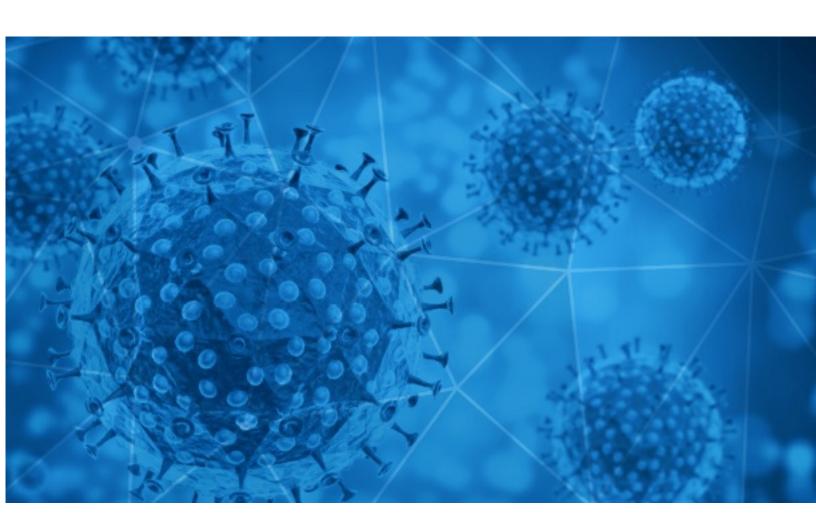**RiskIQ i3:**

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

2020-06-15

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

- CONFIDENTIAL -

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 2020-06-14 to 2020-06-15. During this period, RiskIQ analyzed 0 spam emails containing either "*corona*" or "*COVID*" in the subject line. There were 0 unique subject lines observed during the reporting period. The spam emails originated from 0 unique sending email domains and 0 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

- CONFIDENTIAL -

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

Top-15 IPs Sending COVID Spam

Top-15 Countries Sending COVID Spam

- CONFIDENTIAL -

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

- CONFIDENTIAL -

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: 107,048
Domains with Potential Mail Servers: 2,702
Email-Capable Domains and Hosts: 41,235
Live Hosts and Domains Not Parked: 42,066

Mobile Apps

Apps in Official Stores: 296

by Store

Apple	168
Google	120
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 684

by Store Type:

Hybrid	412
Secondary	239
Affiliate	33

Blacklisted Mobile Apps: 20

by Store Type:

Secondary	19
Official	1