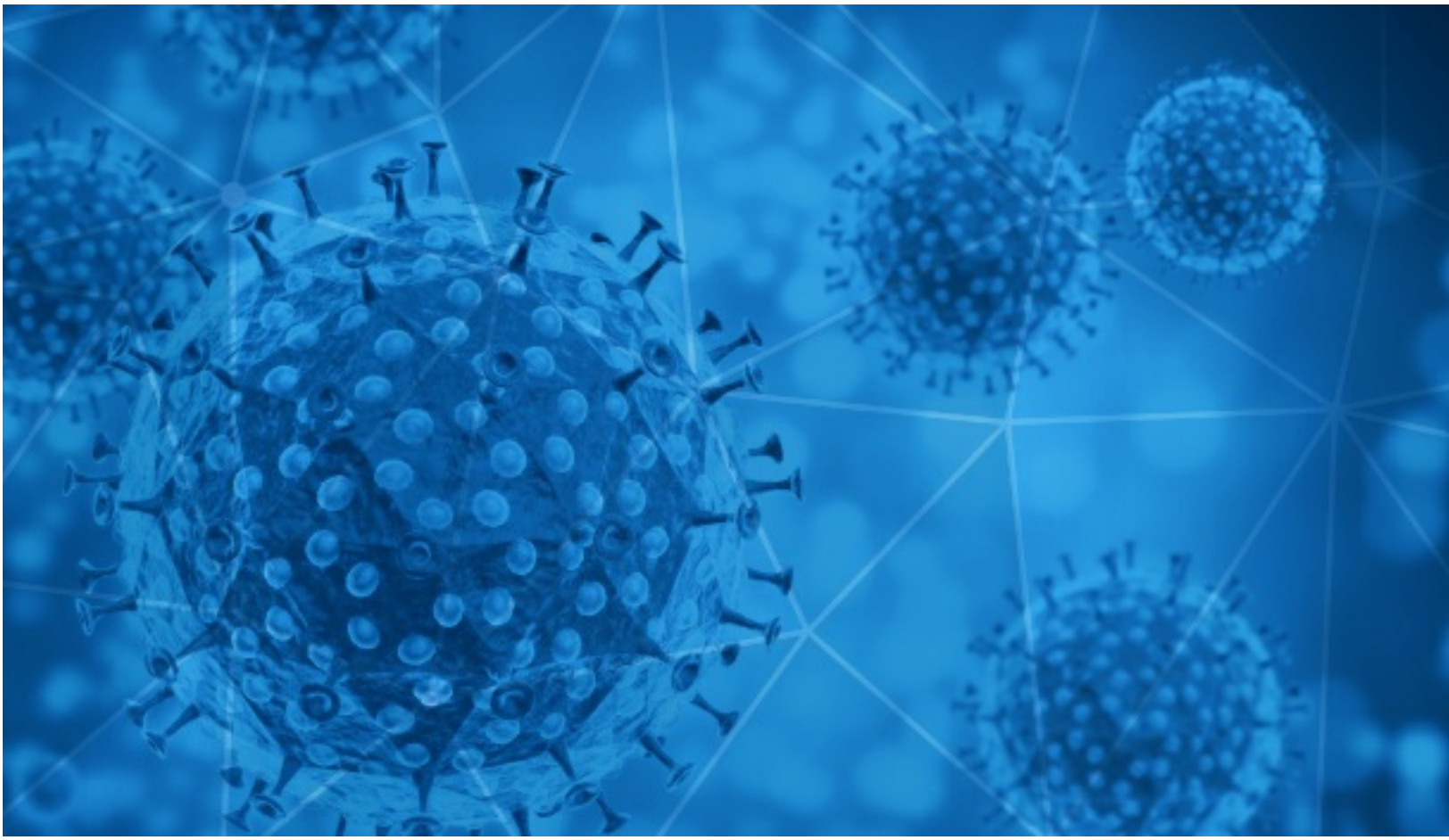
RiskIQ i3:

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

2020-07-10



RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

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

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 2020-07-09 to 2020-07-10. During this period, RiskIQ analyzed 27,440 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,576 unique subject lines observed during the reporting period. The spam emails originated from 2,044 unique sending email domains and 3,917 unique SMTP IP Addresses. Analysts identified 120 emails which sent an executable file for Windows machines.

Top-25 Subjects

COVID-19 pandemic outbreak	2383
re: Test Rapido de Diagnostico COVID-19	1721
COVID-19 - Mobile App Development/ PHP, Magento, Drupal, E-Commerce -etc [REDACTED_DOMAIN]	1277
Sistema de detección Térmico Contra Covid-19	1142
The Corona Letter: The price you pay in a market of fear	902
PyMEs contra el COVID19	658
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	601
IMF COVID-19 DSP	570
Test Rápidos Covid Entrega Inmediata	561
COVID-19 RELIEF FUND	478
96-Y-O Woman Stabbed to Death with Pitchfork + Going to a BAR or CHURCH poses higher COVID-19 Risks	444
Test Rapido Covid-19 Individual	411
(Ams-149)....COVID-19 Personal Protective Equipments(PPE)/Medical Items bulk Supply.	404
Oferta Test Rápidos COVID-19, Mascarillas, Alcohol Gel y Amonio Cuaternario.	396
Pruebas rapidas de Covid 19	332
Implacable contra el COVID-19 AMONIOX	317
Korea Trend News-COVID19(4)	242
FA-TD5,el sistema de fichaje para la nueva normalidad anticovid 19: Control de presencia y control térmico por reconocimiento facial con mascarilla.	242
Plan de Vigilancia y Registro de SICOVID modelo y manual	231
Features: Lessons from Elders; Rethinking Life Purpose?; Caretaker's Financial Guide; Your Covid Go-Bag	229
Mantene tu lugar de trabajo libre de covid19	227
Evita el Covid19 en tu lugar de trabajo	224
UIF Support During Coronavirus Pandemic Approved	215
Re: keep away from Covid-19	203
Let’s fight together to get through the COVID-19	199

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmail.com	4530
mailbox.com	2383
seekscanenchile.com	1142
126.com	1115
countermail.com	1109
163.com	909
timesofindia.com	902
relief.nedbank.co.za	479
caribbeanfever.com	444
irmo-gov.gq	404

Top-15 IPs Sending COVID Spam

209.58.149.87	2316
201.223.116.236	1721
159.65.80.166	1141
157.119.122.135	609
119.122.91.133	582
122.34.222.210	570
59.120.179.14	479
113.88.158.190	437
185.98.21.5	404
201.231.6.60	393

Top-15 Countries Sending COVID Spam

US	10264
IN	2527
CN	2406
CL	2181
GB	1630
FR	1586
AR	1175
KR	830
DE	628
TW	482

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

India- New Government Regulations Effective July 15, 2020 COVID-19 the Corona Virus.	90
Customer Advisory on COVID-19 -- ONE INDIA - Update 6	28
RE: Delayed Payment Due To COVID-19 Situation	2

Top-15 Subjects Containing doc/xlsx Files

Re: covid -19 urgent order request	73
Customer Advisory on COVID-19 -- ONE INDIA - Update 6	30
PHHS 7 8 2020 End of Day COVID 19 Response Summary	4
COVID-19 RELIEF FUNDING	3
RV: LINEAMIENTOS COMPLEMENTARIO PROTOCOLO COVID 19	3
COVID-19 Products New Pricing	3
COVID/VITORIA	2
Coronavirus Assessment Letter	2
Fwd: Invio per posta elettronica: informativa_COVID_19, comunicato_varchi_sito, autocertificazione_COVID_19, RIPARTIZIONE_VARCHI_DA_A	2
ENC: TESTAGEM DE COVID-19 - COSAP	2

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

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: 112,925
Domains with Potential Mail Servers: 2,785
Email-Capable Domains and Hosts: 42,728
Live Hosts and Domains Not Parked: 59,517

Mobile Apps

Apps in Official Stores: 329

by Store

Apple	178
Google	142
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 869

by Store Type:

Hybrid	546
Secondary	286
Affiliate	37

Blacklisted Mobile Apps: 21

by Store Type:

Secondary	19
Hybrid	1
Official	1