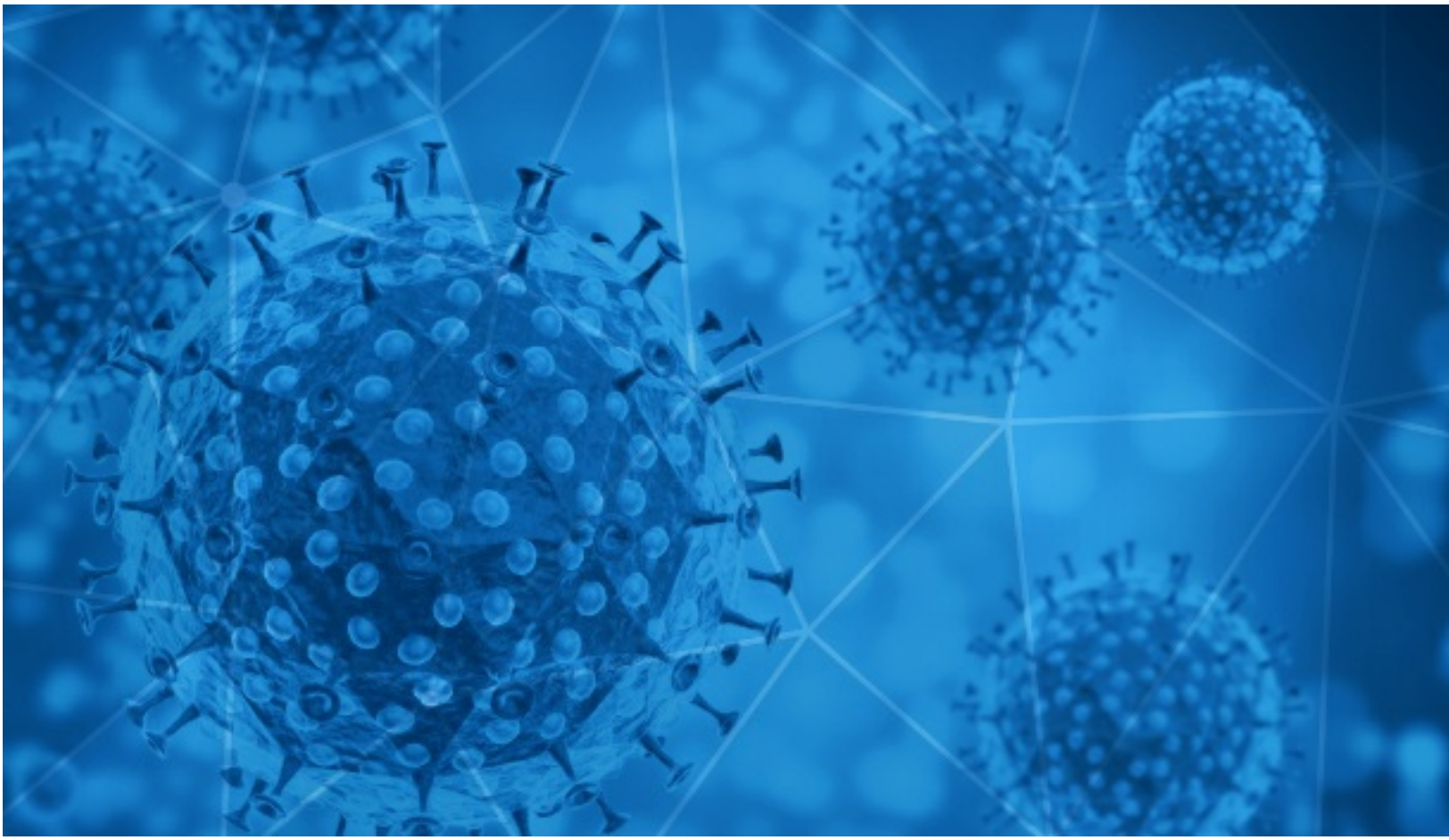
RiskIQ i3:

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

2020-06-04



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 2020-06-03 to 2020-06-04. During this period, RiskIQ analyzed 39,129 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 5,348 unique subject lines observed during the reporting period. The spam emails originated from 4,364 unique sending email domains and 7,432 unique SMTP IP Addresses. Analysts identified 23 emails which sent an executable file for Windows machines.

Top-25 Subjects

COVID-19 Protection Gears	2191
The Corona Letter: Rural India's slippery slope	1503
Insumos Protectores Covid-19 Despachos a Todo Chile	1441
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	808
School is still not open, but you can study for free during this COVID-19 pandemic	750
Products for COVID-19	739
CORONAVIRUS RELIEF FUND (CRF) 2020	644
The COVID-19 Response Fund	614
COVID-19 EMERGENCY DELIVERY OF YOUR CONSIGNMENT BOX TODAY.	556
Elija su Kit de protección Covid19	544
COVID-19 Pandemic Grant Donation	521
Running essential errands? Here's how to stay safe and healthy during COVID-19.	493
Front Sight's Response to Nevada's Current COVID-19 Restrictions…	422
Covid-19 Compensation Relief Funds :	386
Covid19- Fund Compensation Notice./Paying Center	365
COVID-19 Response Fund	361
Free LinkedIn Premium for Caregivers and Veterans, Select Benefits Exams Resuming, COVID-19 VA Patient Dashboard	338
COVID-19	336
Protección COVID 19	316
Re: COVID-19 Financial Relief Funds for you	311
Ofertas Productos Covid 19	310
Stuck at home because of COVID-19 outbreak? Make money investing in netflix stocks	294
Maquina para Desinfecciones COVID por Termonebulización en $120	281
COVID-19 - Custom Projects | Mobile Application | SEO !! -etc [REDACTED_DOMAIN]	278
REPORT WITH REGARDS TO COVID-19 FOR ALL INDIAN PORTS	273

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	3735
medicproduction.com	3258
timesofindia.com	1587
126.com	1445
insumosprotectorescovid19.com	1441
outlook.com	1307
163.com	1233
frontsight.com	1058
myschool.com.ng	879
hotmail.com	679

Top-15 IPs Sending COVID Spam

209.58.149.66	2958
167.99.191.76	1439
209.123.15.146	1056
184.107.73.137	879
119.122.89.157	769
177.23.28.38	644
142.11.209.110	614
167.98.140.49	518
177.129.73.9	386
91.212.153.94	364

Top-15 Countries Sending COVID Spam

US	14022
CN	3811
IN	3699
CA	2706
FR	1824
BR	1333
GB	1325
DE	1283
ES	1268
--	817

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Urgent Quotration due to Covid-19	9
FW: Tender Kampong Bahru - Invitation to quote pharmaceutical and medical equipment for the treatment of COVID-19	7
COVID-19 Update	3
Auswirkungen der Corona-Pandemie (Newsmail 5) / uitwerkingen Corona-pandemie (newsmail 5)	1

Top-15 Subjects Containing doc/xlsx Files

Financial Accounting Impact of COVID-19- An In-depth Look at IFRS	10
PROTEGE A TU EMPRESA FRENTE AL COVID	4
Бесконтактная антивирусная ручка для двери! Решение против COVID-19 !	4
Press Release: FLIR Systems Installs Its EST Screening Solution at Pentagon to Support the Fight Against COVID-19 -- EN - 52228933	3
FAO: Headteacher/SENDCo/Pastoral Team: June 2020 Webinars for the COVID and POST-COVID era (Jennifer Nock Training)	3
Tras la crisis del Covid19, las tres claves del sector alimentación: “Hacer, informar y, después, comunicar”	3
COMUNICATO STAMPA Coronavirus, Confagricoltura: nel 2020 l’export agroalimentare nella UE partito bene, ma rallentato dalla pandemia	2
Cofidis, primera empresa del sector financiero en recibir el sello ‘Espacio COVID-19 protegido’	2
NdP_5 aspectos en los que el sector de la moda se ha reinventado tras el COVID-19	2
Covid-19 Compensation Fund	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: 103,442
Domains with Potential Mail Servers: 2,769
Email-Capable Domains and Hosts: 39,665
Live Hosts and Domains Not Parked: 40,983

Mobile Apps

Apps in Official Stores: 284

by Store

Apple	165
Google	111
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 622

by Store Type:

Hybrid	372
Secondary	222
Affiliate	28

Blacklisted Mobile Apps: 19

by Store Type:

Secondary	18
Official	1