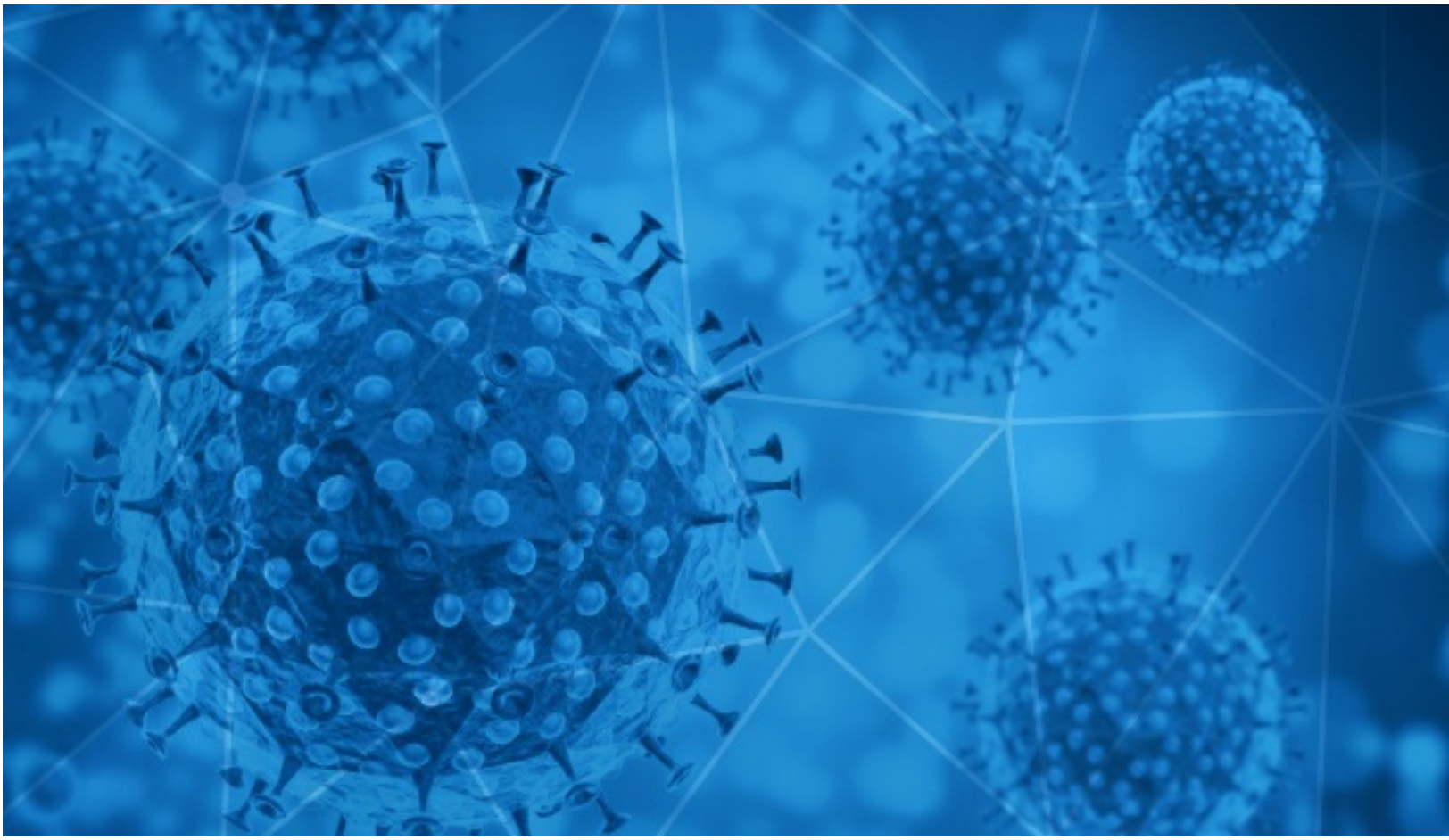
RiskIQ i3:

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

2020-06-03



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 2020-06-02 to 2020-06-03. During this period, RiskIQ analyzed 45,990 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 5,657 unique subject lines observed during the reporting period. The spam emails originated from 4,226 unique sending email domains and 7,254 unique SMTP IP Addresses. Analysts identified 34 emails which sent an executable file for Windows machines.

Top-25 Subjects

COVID-19 Protection Gears	3571
Products for COVID-19	2219
Covid19- Fund Compensation Notice./Paying Center	2146
CORONAVIRUS RELIEF FUND (CRF) 2020	1858
The Corona Letter: The middle seat math	1780
COVID-19	1642
COVID-19 EMERGENCY DELIVERY OF YOUR CONSIGNMENT BOX TODAY.	993
Insumos Protectores Covid-19 Despachos a Todo Chile	556
Rencontrer des femmes (édition Corona)	459
IRS COVID-19 Relief Fund	405
Protege tu espacio del covid-19	386
Test Rapido Covid 19	382
Covid-19 Compensation Relief Funds :	382
Seminario: Nuevas Medidas Tributarias en Tiempos de COVID-19	374
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	357
Campaña Covid 19	356
Your Covid-19 Empowerment Fund Package	346
Front Sight's Response to Nevada's Current COVID-19 Restrictions…	298
Mamparas de proteccion contra el coronavirus	277
Protejase del Covid-19, Productos Certificados	269
Productos para la contingencia covid-19 !!! Encuentra todo en un solo lugar	267
Mamparas de proteccion COVID19	266
Sale Masks , Corona Virus test Kit,Ventilator machine and Protective Clothing with quality certificates.	262
WB/UNITED NATIONS SCAM VICTIMS COMPENSATIONS PAYMENTS (COVID-19 2020)	242
Coronavirus Relief,	242

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

medicproduction.com	7345
gmail.com	5612
outlook.com	2563
timesofindia.com	1939
163.com	1691
hotmail.com	1203
126.com	1172
frontsight.com	730
focazen.com	594
insumosprotectorescovid19.com	556

Top-15 IPs Sending COVID Spam

209.58.149.66	7320
91.212.153.94	2143
177.23.28.38	1858
209.123.15.146	729
167.99.191.76	556
5.199.131.165	459
113.88.158.38	425
61.247.224.43	393
134.122.89.71	384
177.129.73.9	382

Top-15 Countries Sending COVID Spam

US	18594
CN	4341
IN	3403
BR	2568
--	2560
DE	1964
FR	1943
CA	1405
AR	1205
CL	575

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

COVID-19 Update	19
Urgent Quotration due to Covid-19	12

Top-15 Subjects Containing doc/xlsx Files

Financial Accounting Impact of COVID-19- An In-depth Look at IFRS	37
Бесконтактная антивирусная ручка для двери! Решение против COVID-19 !	10
RV: CUMPLIMIENTO DE PROTOCOLOS DE BIOSEGURIDAD PARA MANEJO DE PANDEMIA CORONAVIRUS - COVID19	4
Infos Covid 19 : Dispositif 2S2C	3
PROTEGE A TU EMPRESA FRENTE AL COVID	3
Hygienestation. Coronabekaempfung.	2
Junio 06 - RETENCIONES EN LA FUENTE DEL IMPUESTO A LA RENTA / Liquidación de compras y prestación de servicios / Aplicación de ley Humanitaria / Gestión financiera en COVID / Retenciones en la fuente del IVA / Formación de Asistente de RRHH	2
[NYAPRS Enews] FINAL REMINDER: COVID Impact Survey for Recipients of Services and Families	2
NP_ Fumadores tienen mayor riesgo de complicaciones graves al contraer covid-19	2
CORONA VIRUS.docx	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: 102,416
Domains with Potential Mail Servers: 3,071
Email-Capable Domains and Hosts: 38,979
Live Hosts and Domains Not Parked: 41,657

Mobile Apps

Apps in Official Stores: 283

by Store

Apple	164
Google	111
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 615

by Store Type:

Hybrid	366
Secondary	221
Affiliate	28

Blacklisted Mobile Apps: 19

by Store Type:

Secondary	18
Official	1