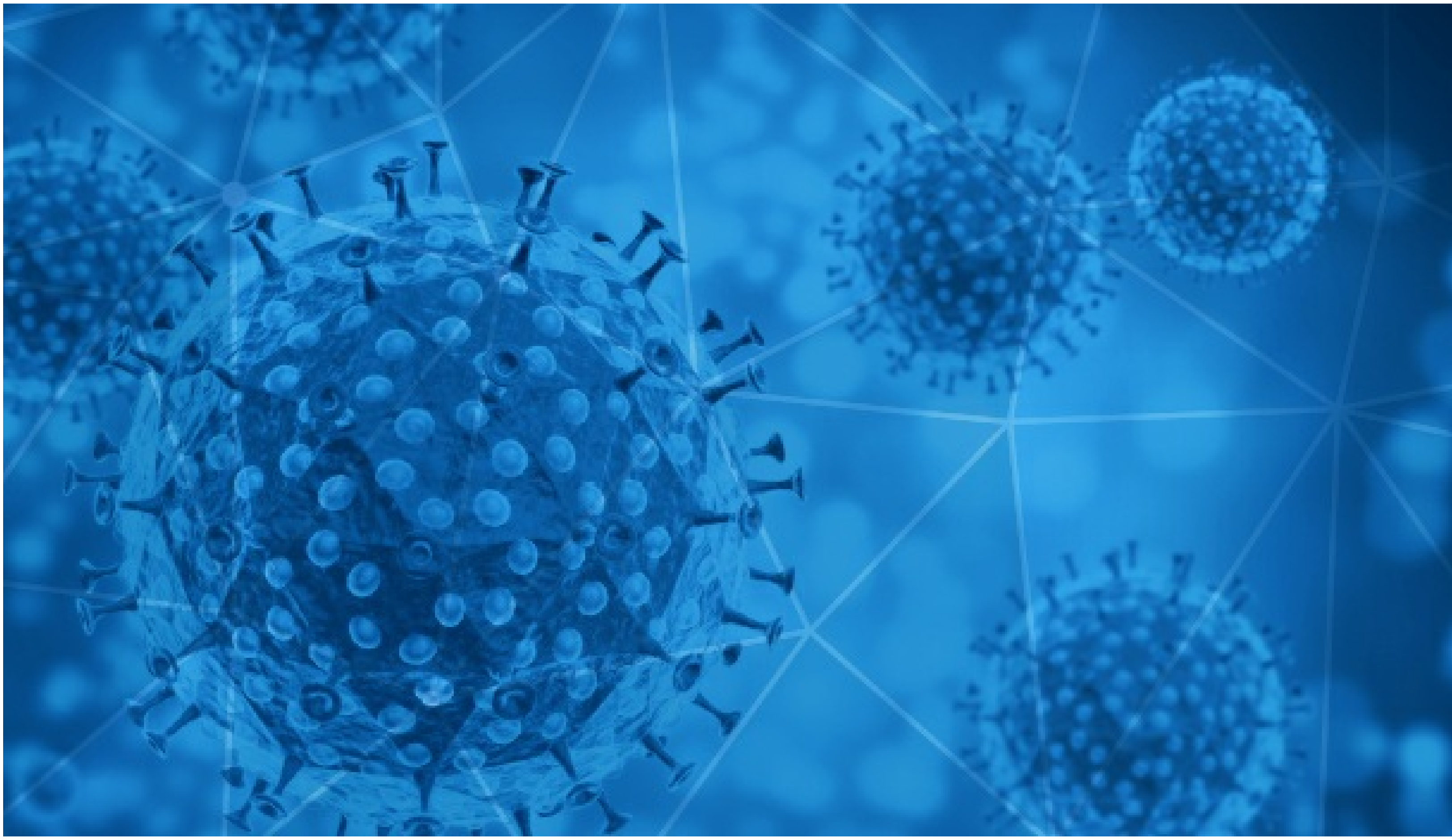
RiskIQ i3:

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

2020-06-19



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 2020-06-18 to 2020-06-19. During this period, RiskIQ analyzed 40,172 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,196 unique subject lines observed during the reporting period. The spam emails originated from 2,705 unique sending email domains and 5,080 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

Test Rapido COVID 19	4650
The Corona Letter: Unlockdown, but conditions apply	2982
COVID-19 / DONATION FOR YOU	2074
when will covid 19 end? what can we do?	1969
Covid-19 Credit Facility Business Owners	1471
Long Lasting and Eco-Friendly Disinfectant to Fight Covid19…	1162
COVID-19 - Custom Projects | Mobile Application | SEO !! -etc [REDACTED_DOMAIN]	913
Relief Fund (Covid-19)	528
[SPAM] COVID 19 VICTIMS COMPENSATION FUND M.T.C.N: 793-864-3681	505
Implacable contra el COVID-19 AMONIOX	489
Re:Zuberi Finance SA Droogte / Covid-19-verligtingprojek	482
Credito fiscal COVID para innovacion	453
COVID-19 Financial Assistance	425
$ 9.990.- Test Rápido COVID-19	394
RE: Business is going down ? Due to COVID-19	372
Catálogo Covid para distribuidores y mayoristas	334
Como volver a la actividad post coronavirus?	292
□□□□□□□□□□□□□□COVID-19□□□□□□□□□□□□	291
Mantene tu lugar de trabajo libre de covid19	287
Cabinas para la prevencion del coronavirus?	286
□□□□□□□□□□□□□□□JAL□□□□□□□□□□□□□□□□□/JAL Mileage Bank's Special Response to the Spread of COVID-19	285
Soluciones para la prevencion del covid19	284
Evita el Covid19 en tu lugar de trabajo	267
Mamparas de proteccion contra el coronavirus	258
Hygiène Covid - Protégez vos collaborateurs, vos clients, votre activité	257

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	6996
trendingtopic.cl	4650
timesofindia.com	2982
countermail.com	2376
foxmail.com	1990
163.com	1195
csestock.com	1162
126.com	848
hotmail.com	727
irscovidrelief.org	528

Top-15 IPs Sending COVID Spam

212.227.254.175	2074
103.30.17.43	1969
51.77.33.43	1502
187.174.101.179	1471
51.77.33.44	1468
148.72.151.127	1313
51.77.33.39	803
201.231.19.65	642
201.231.27.226	627
93.95.154.3	505

Top-15 Countries Sending COVID Spam

US	9357
FR	5416
IN	4498
DE	3158
CN	3091
AR	2561
HK	2188
MX	1689
JP	1319
GB	819

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Fwd: 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

Cuestionan el uso de la dexametasona para COVID-19	5
NdP Propify || Chefs, Sporties y Smart Workers: los nuevos perfiles de inquilinos post-COVID	4
Se solicita Regularizar el Llenado de la Ficha 200(Ficha Epidemiológica en el sistema SISCOVID) de casos Covid19	4
BHP – obowiązki pracodawcy i pracownika w dobie Covid 19	3
CCS /9094 Llega Chihuahua a 3 mil 152 contagios por COVID-19 y 541 defunciones	2
Sale!!! New Covid Safety Kits with custom imprint option as low as $3.28 per kit - 3-5 day lead time for non-logod- from GreatSunrise06172020.docx	2
IMSS Boletín 407.- En Pabellón COVID, los cumpleaños de los pacientes no pasan desapercibidos	2
ofrecimiento de nota- Tratamiento con suero para pacientes con COVID 19 ingresa a fase clínica- Agencia CTyS UNLaM	2
FAO SLT: Exciting and informative Covid-19 and Post Covid-19 Training Covering Attachment, Anxiety, Full Return to School	2
finger clip pulse oximeter working to monitor patients with coVID-19	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: 108,059
Domains with Potential Mail Servers: 2,726
Email-Capable Domains and Hosts: 41,442
Live Hosts and Domains Not Parked: 44,132

Mobile Apps

Apps in Official Stores: 298

by Store

Apple	168
Google	122
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 727

by Store Type:

Hybrid	446
Secondary	247
Affiliate	34

Blacklisted Mobile Apps: 20

by Store Type:

Secondary	19
Official	1