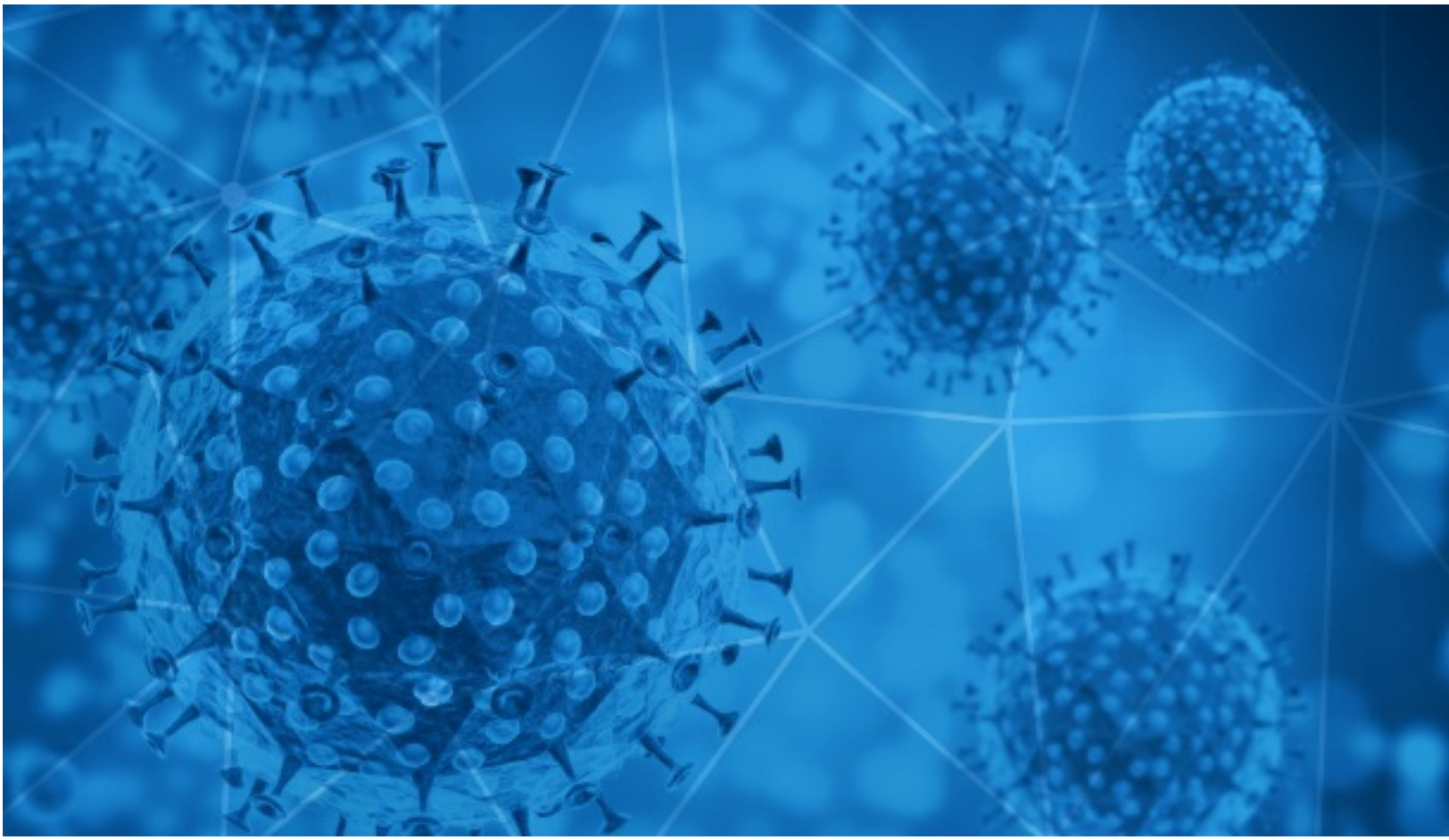
RiskIQ i3:

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

2020-07-06



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 2020-07-05 to 2020-07-06. During this period, RiskIQ analyzed 22,838 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,187 unique subject lines observed during the reporting period. The spam emails originated from 1,624 unique sending email domains and 2,965 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Let's talk mental health	2969
Corona-Finanz-Check	1169
STAR GOLD MEDICS COVID-19 PROTECTION EQUIPMENTS	1097
Deadlier than the coronavirus	1025
COVID-19 - Custom Projects | Mobile Application | SEO !! -etc [REDACTED_DOMAIN]	851
High-quality Disposable Medical Kit, which are reliable products protecting from COVID-19	657
COVID-19 - Mobile App Development/ PHP, Magento, Drupal, E-Commerce -etc texelglobal.com	646
COVID PPE Clearance Sale for July 4th!	567
Insumos de Protección COVID-19	471
We Produce Covid-19 (Face Mask,Isolation Gown,Head/Shoe/Sleeve Cover,Vinyl Gloves ,PE Gloves,Apron)	469
Tienes Disponible unÂ Credito FOGAPE - COVID-19	466
Korea Trend News-COVID19(4)	345
Mantene tu lugar de trabajo libre de covid19	327
Evita el Covid19 en tu lugar de trabajo	318
Covid-19-Darlehensangebot	318
WHO versus 239 scientists: Is the coronavirus airborne?	277
Re: Estamos adaptados a la nueva situacion Covid-19	257
Re: Hay que adaptarnos a la situacion Covid-19	251
Re: Nos adaptamos a la nueva situacion Covid-19	237
Re: Adaptados a la nueva situacion Covid-19	236
Re: Hay que adaptarse a la nueva situacion Covid-19	225
Extra editie: Richtlijnen voor gebruik airco in coronatijden	219
Re: Tenemos que adaptarnos a la situacion Covid-19	216
Re: Nos tenemos que adaptar a la situacion Covid-19	215
Re: Estamos adaptados a la situacion Covid-19	213

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	3224
timesofindia.com	2969
flixkredit.de	1169
stargoldmedics.com	1133
countermail.com	645
163.com	574
seorazor.com	509
protonmail.com	474
enlinea.cl	467
decobertores.com	460

Top-15 IPs Sending COVID Spam

46.228.192.33	1168
198.102.14.18	1097
157.119.122.135	665
82.70.113.62	469
81.95.112.26	369
223.38.21.12	345
157.119.122.138	343
170.10.161.204	326
200.128.35.9	319
157.119.122.139	303

Top-15 Countries Sending COVID Spam

IN	4762
US	4486
DE	3645
CN	1603
--	1266
GB	803
BE	749
AR	723
FR	696
KR	449

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

ANC Weekly COVID-19 Reports	26
IMPORTANT : post-coronavirus	8
COVID-19 RELIEF FUNDING	7
MANTA 9 JULIO NUEVAS REFORMAS LABORALES Y DISPOSICIONES LEGALES ESTABLECIDAS EN LA LEY ORGANICA DE APOYO HUMANITARIO PARA COMBATIR LA CRISIS DEL COVID 19 PUBLICADA EN EL REGISTRO OFICIAL EL 22 DE JUNIO DEL 2020	4
9 JULIO NUEVAS REFORMAS LABORALES Y DISPOSICIONES LEGALES ESTABLECIDAS EN LA LEY ORGANICA DE APOYO HUMANITARIO PARA COMBATIR LA CRISIS DEL COVID 19 PUBLICADA EN EL REGISTRO OFICIAL EL 22 DE JUNIO DEL 2020	2
Reporte de resultados Covid	1
Re: Covid	1
(H P E) Invitation to register for the Webinar on "Implementing CBME in COVID times" at SRM Medical College	1
Covid-19 compensation fund	1
Comunicado de Prensa OCGC 05072020 07-2020 Conagua e iniciativa privada entregan suministros para la atención de la emergencia sanitaria por COVID-19 en Veracruz	1

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: 111,959
Domains with Potential Mail Servers: 2,761
Email-Capable Domains and Hosts: 42,430
Live Hosts and Domains Not Parked: 54,519

Mobile Apps

Apps in Official Stores: 313

by Store

Apple	174
Google	130
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 846

by Store Type:

Hybrid	530
Secondary	280
Affiliate	36

Blacklisted Mobile Apps: 21

by Store Type:

Secondary	19
Hybrid	1
Official	1