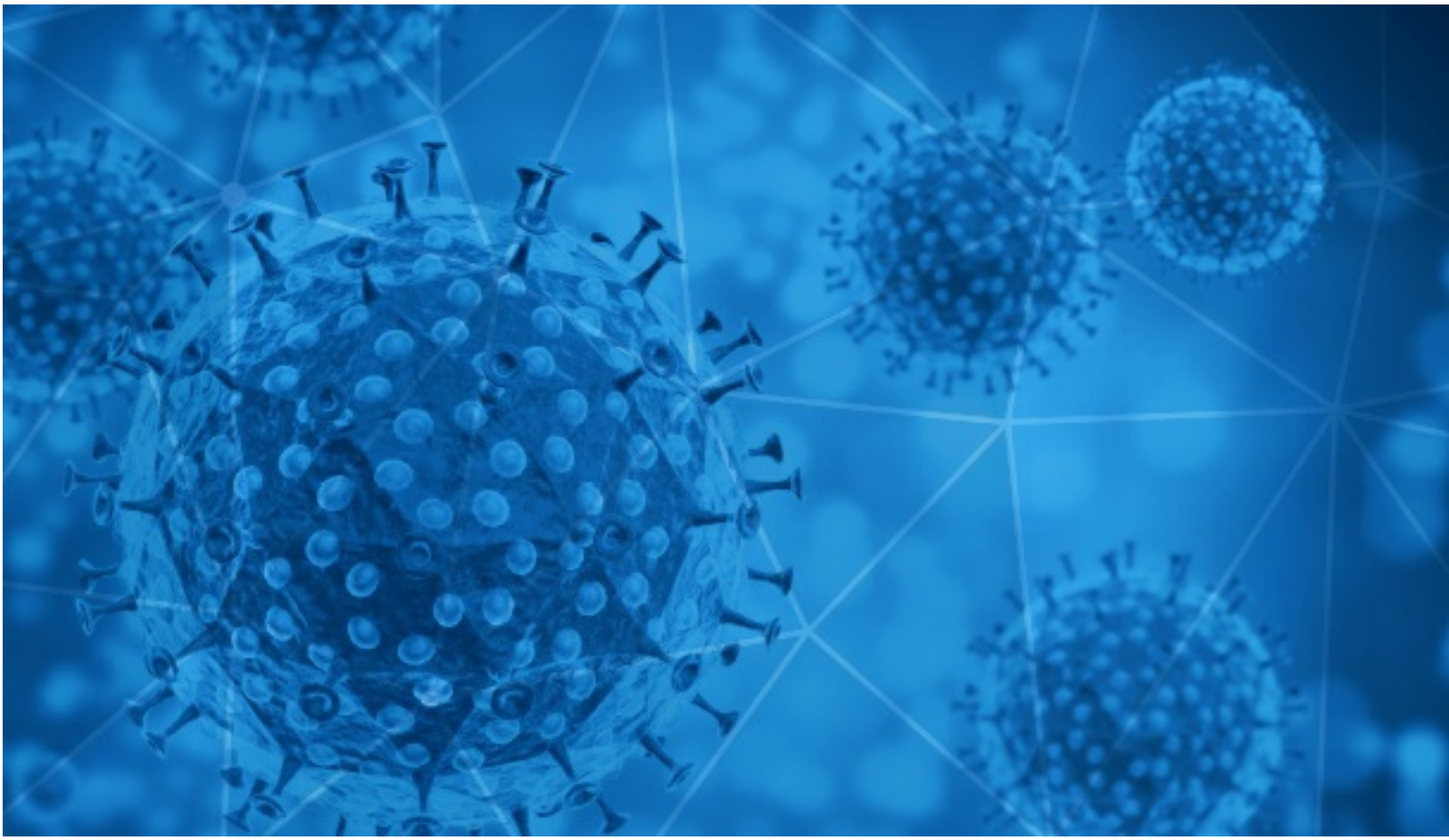
RiskIQ i3:

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

2020-10-26



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 2020-10-25 to 2020-10-26. During this period, RiskIQ analyzed 22,599 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,536 unique subject lines observed during the reporting period. The spam emails originated from 924 unique sending email domains and 2,299 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Have a Covid-safe festive season	4582
Test rapido para la deteccion del Coronavirus	1254
ICO Covid Inversión	977
Attention!Dear,UN. CORONA-VIRUS RELIEF FUND	777
Evite el coronavirus en su negocio	735
Salve sua família! Iniciativa Covid19	716
COVID-19 Asesoramiento contable para tu empresa	666
Limpieza y desinfeccion COVID 19	657
Covid-19 Intervention Relief Fund	653
ATENCION COVID-19 Estudio Contable, Legal e Impositivo para tu negocio	632
Llegaron los Test COVID19 de deteccion rapida	613
Ingresaron TEST COVID19 de deteccion rapida	605
Hurry! Register for a Free Webinar on 'Life with Corona - Healthy Heart' by SMC & BLK on 27th Oct, 5pm onwards.	560
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	494
Save your family! Covid19 initiative	385
Your COVID-19 Test Results	304
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	250
COVID-19 Compensation Claim	239
VERY IMPORTANT INFORMATION ,COVID 19 DEATH	230
Re: Re: Covid-19 acrylic shield	182
Re: Covid-19 Protective acrylic sneeze guards	181
Re: Covid-19 acrylic protect shield	180
"Er moeten lokale coronamaatregelen komen" - Verrassing: nieuw seizoen 'De mol' al ingeblikt - "Verdwijning van YouTuber valt volledig buiten het normale" - Buurt in de ban van dierendoder	153
UN. CORONA-VIRUS RELIEF FUND {66.43.119.68	141
Re: keep away from Covid-19	140

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

tutanota.com	5162
timesofindia.com	4583
gmail.com	2600
spockvii.com	894
126.com	845
yeah.net	787
smctradeonline.in	560
yahoo.com	445
nieuwsblad.be	334
dhs.wisconsin.gov	308

Top-15 IPs Sending COVID Spam

201.231.58.115	1788
201.231.115.144	1688
190.247.255.232	1685
66.43.119.17	918
23.239.14.157	649
61.95.233.70	560
181.46.136.168	494
167.114.185.59	275
185.153.228.135	273
219.65.85.27	257

Top-15 Countries Sending COVID Spam

AR	5722
IN	5225
US	3924
CN	2161
ES	1010
DE	690
CA	507
BE	470
FR	457
TR	289

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

PRODUTOS DE PROTEÇÃO INDIVIDUAL COVID PARA EMPRESAS	2
IMSS Boletín 723.- Avanza IMSS en reconversión hospitalaria en Ciudad Juárez, Chihuahua, para fortalecer atención a COVID-19	2
NP: Midis lanza portal “Súmate a la Red Amachay” para incluir a más personas vulnerables que urgen del cuidado de su salud contra el COVID-19	2
Buletin de presa 25.10.2020 + comunicat actiuni prevenire COVID19	2
Covid Blues Buster Package - Australia's No. 1 Emu Oil Expert	1
FIOTOS AJA SANTA MARTA******acciones de control y prevención del COVID-19 en el Mercado Público**	1
COVID-19 Site Impact Monitoring (Tableau)	1
PDD Epi covid Fonds Mondial	1
CONSOLIDADO DE LLAMADA CASO COVID-19	1
AISLAMIENTO DE PERSONAL POLICIAL POR COVID-19	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: 130,424
Domains with Potential Mail Servers: 2,677
Email-Capable Domains and Hosts: 49,316
Live Hosts and Domains Not Parked: 46,396

Mobile Apps

Apps in Official Stores: 466

by Store

Apple	235
Google	216
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,640

by Store Type:

Hybrid	869
Secondary	713
Affiliate	58

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1