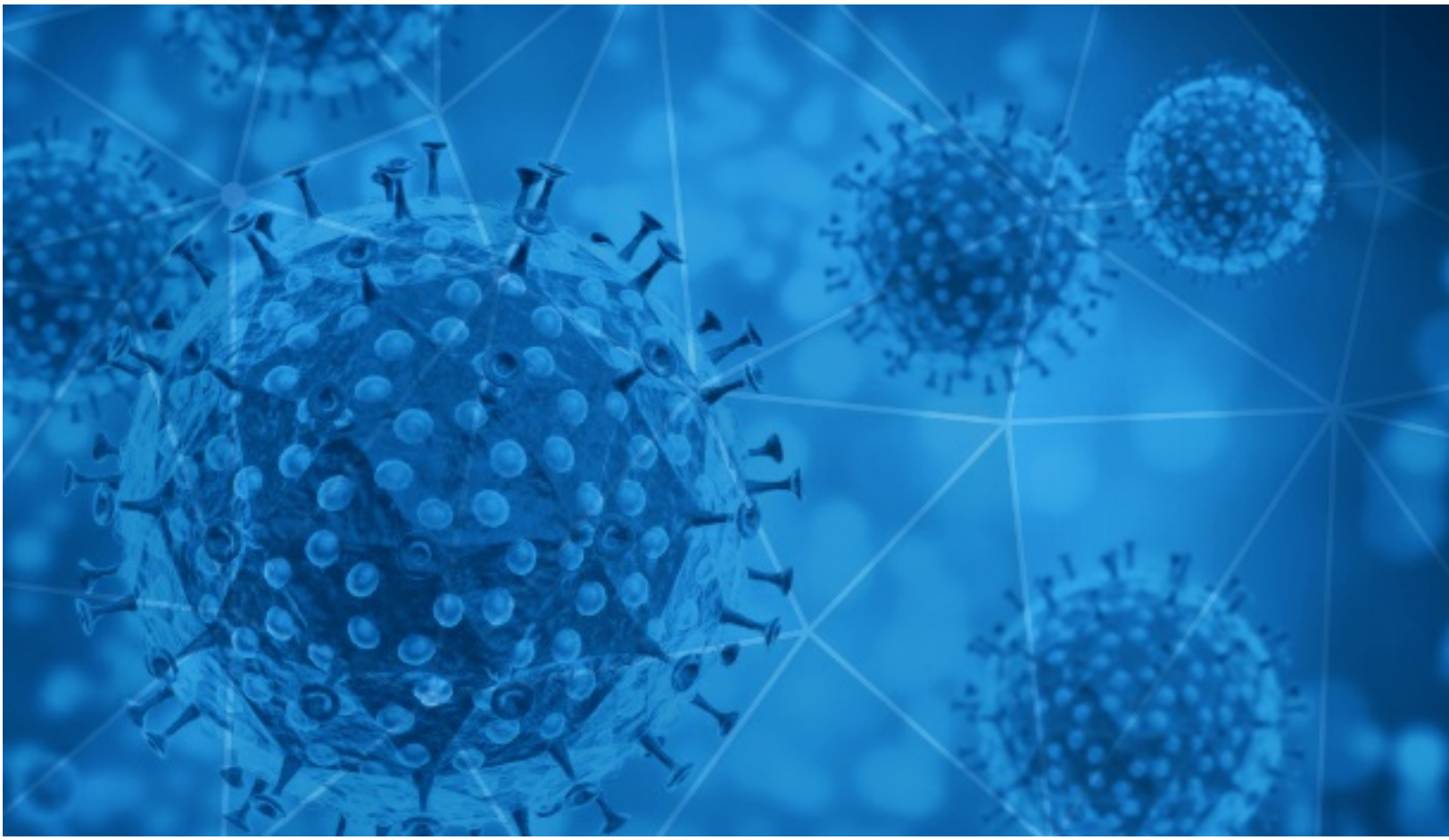
RiskIQ i3:

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

2020-11-09



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 2020-11-08 to 2020-11-09. During this period, RiskIQ analyzed 39,466 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,580 unique subject lines observed during the reporting period. The spam emails originated from 939 unique sending email domains and 2,671 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	18567
The Corona Letter: Weaker antibodies in kids ain't bad	4783
SPENDE / COVID 19 UNTERSTÜTZUNG.	1253
Equipos de Protección y Prevención del COVID-19	1247
Cambios en ICO Covid	1022
Mejoramos los precios en Test Covid-19-Test de Alcohol y EPP	516
Covid-19 Impacts Babies with Birth Defects!	403
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	395
November Covid-19 palliative Award USD$3,500,000.00	373
Re: Defeat Coronavirus, non contact fever alarm device	368
Contactless infrared body temperature thermometer defeat Coronavirus	328
Help to fight COVID-19 fever alarm security door	322
Covid 19 Command Center	301
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	260
Atencion covid Estudio Contable Legal e Impositivo para tu negocio	255
Re: Re: Covid-19 acrylic shield(Support OEM)	249
(□□) □□□ 19(COVID-19) □□□□□□□□□ □□ □□ □□ □□□□	234
Re: Covid-19 Protective acrylic sneeze guards(1/5 lower than your purchase price)	221
Congratulation!!! You have been awarded United Nations Covid-19 funds	214
□□Как восстановиться после COVID? Ссылка на занятие в сообщении↴□	192
Corona prijs verlaging	190
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products).	182
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products).	179
Arrêtons Covid 19 ensemble	177
Re:COVID-19 RESPONSE AND RECOVERY FUND OF $1,500,000.00 USD	166

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

epc-store.com	18571
timesofindia.com	4783
yahoo.com	1275
focazen.com	1251
yeah.net	1188
gmail.com	1168
keyable.net	1018
sabaziusii.com	979
126.com	963
wangzichuxing.cn	403

Top-15 IPs Sending COVID Spam

200.17.137.44	1253
113.89.40.36	967
103.225.54.80	611
103.225.53.241	544
103.225.55.59	515
103.225.54.69	477
103.225.53.43	457
103.225.55.165	422
103.225.53.42	409
170.106.84.7	403

Top-15 Countries Sending COVID Spam

JP	18598
IN	4999
CN	4166
US	3295
ES	1318
BR	1283
DE	710
AR	640
FR	601
IT	518

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	31
[editors--peacevoice] submission: op-ed: Biden, agenda, executive orders, coronavirus, relief package, rejoin treaties, rejoin WHO	2
COVID PIEMONTE, L'ASSESSORE REGIONALE ALLA SANITA', LUIGI ICARDI: «L'APPELLO DELL'UNITA' DI CRISI NON INTENDE SNATURARE IL RUOLO DEI MEDICI E DEGLI INFERMIERI, CHIARIREMO EVENTUALI EQUIVOCI»	2
3-5 GRADE COVID TESTING REMINDER DUE TOMORROW	2
FW: 201105 Brief verwanten coronabesmetting Groningen.docx	1
Fwd: COVID medical Assessment	1
PARTE COVID-19 DEL 08NOV2020 EESTP PNP TRUJILLO	1
Orari i Mjekeve ne njesine Covid 3, Klnikat Interne	1
Биотек - Барање за р��зервација на COVID 19	1
Fw: Fraser Health Authority - [COVID19 Protocol for Masjid Al Salaam] - UPDATES - Nov 7	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: 132,054
Domains with Potential Mail Servers: 2,658
Email-Capable Domains and Hosts: 50,276
Live Hosts and Domains Not Parked: 45,908

Mobile Apps

Apps in Official Stores: 470

by Store

Apple	236
Google	219
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,714

by Store Type:

Hybrid	900
Secondary	755
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1