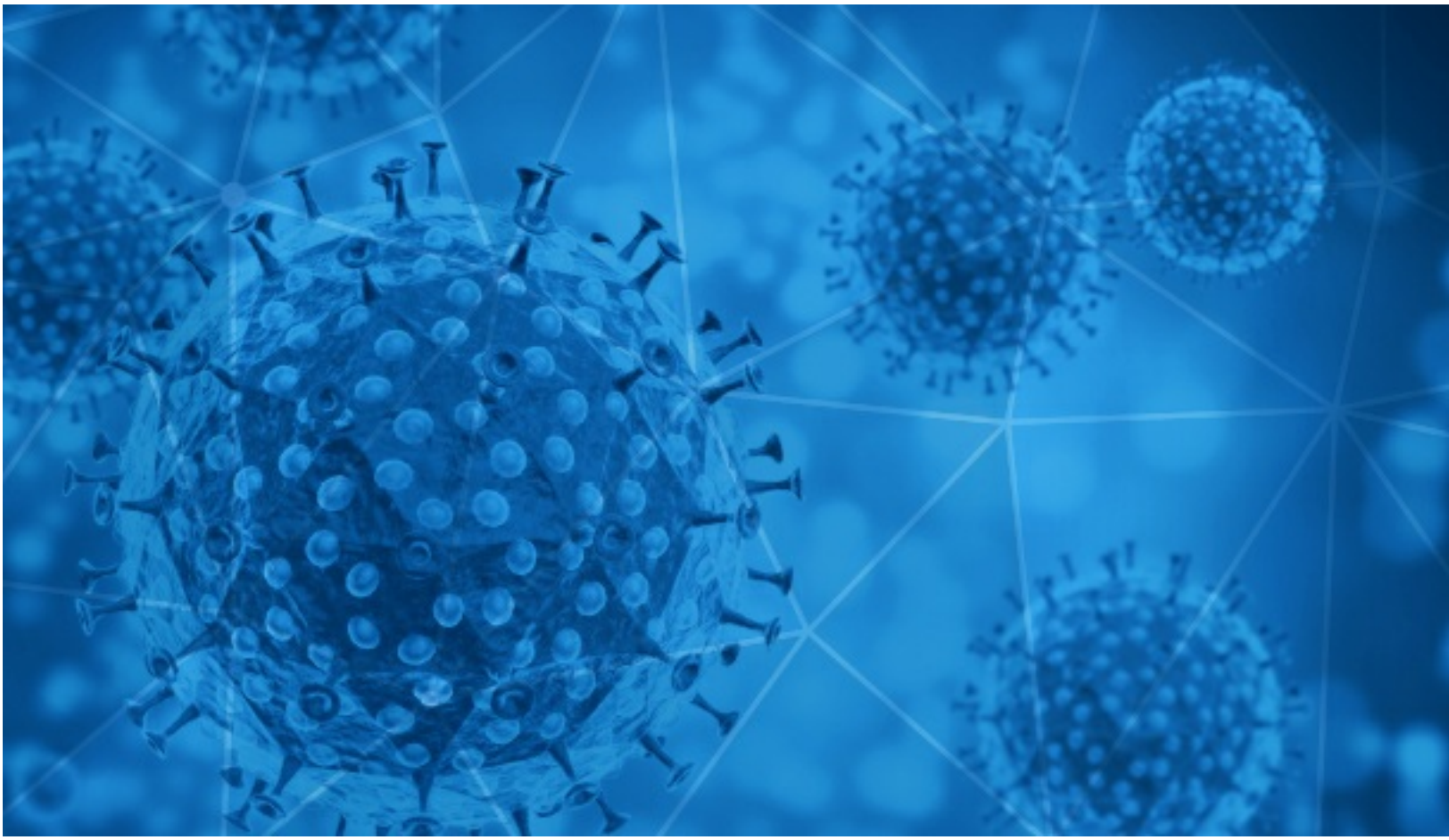
RiskIQ i3:

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

2020-11-18



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 2020-11-17 to 2020-11-18. During this period, RiskIQ analyzed 35,087 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,600 unique subject lines observed during the reporting period. The spam emails originated from 2,868 unique sending email domains and 5,092 unique SMTP IP Addresses. Analysts identified 4 emails which sent an executable file for Windows machines.

Top-25 Subjects

Biden ramps up pressure on Trump, states announce new COVID-19 restrictions, and more from Apple News	7212
The Corona Letter: A deep-dive into mRNA vaccines	3020
COVID-19 Update: We are open and now offering Free Virtual Consultations	2417
Coronavirus (Covid19) Bailout Fund	974
Help Curve COVID Virus, Get Your KN95 Mask 50%!O(MISSING)ff	490
Test Rápido Covid-19 Segunda Generación	489
CORONA-VIRUS RELIEF FUND UNITED NATION OFFICE,GEVEVA	431
Reserve Your Seat . Thriving not just surviving post-COVID	402
Re: Digital signage solution for Covid-19	394
Fight COVID-19 With $100 at Amazon Gift Card!	393
Mi seguro insumos covid 19 protege a tu familia	359
Aprovecha productos COVID en oferta!!!	339
Atencion covid Estudio Contable Legal e Impositivo para tu negocio	314
Let’s fight together to get through the COVID-19	293
Aprovecha Productos COVID en Oferta!	275
VRT.Nu moet inbinden in beheersovereenkomst - Van Ranst: ‘Wij hebben domweg geen goed coronabeleid’ - Obama geeft weinig hoop op samenwerking Republikeinen - Nederlandse bibliotheken halen Zwarte Piet-boeken weg - ‘Nog te veel ex-gedetineerden maken…	271
Re:::Your Covid-19 Fund Benefit	244
Re: Corona virus Protection Pills.Order confirmation	227
Good morning, SA | Zuma attacks Zondo commission, NICD can't confirm Covid-19 reinfection, matric maths paper leaked	211
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	204
Covid-19 hospitalization expenses covered with HDFC ERGO	192
Van Ranst maakt gehakt van coronabeleid - Heisa over filmpje boksclub - Sam De Bruyn neemt afscheid	190
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	187
Facing another surge of the coronavirus	181
Re: Covid-19 acrylic protect shield	175

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

insideapple.apple.com	7214
timesofindia.com	3020
gmail.com	2075
offeryouu.xyz	1812
126.com	873
yeah.net	621
exlusivehub.tech	606
mambaforthree.com	493
163.com	468
timesjobs.com	402

Top-15 IPs Sending COVID Spam

174.138.43.204	1811
45.5.200.6	974
134.209.113.213	606
194.116.229.70	490
66.43.119.17	426
219.65.84.186	313
202.59.10.41	244
67.219.150.138	227
112.111.163.33	222
104.248.10.217	216

Top-15 Countries Sending COVID Spam

US	18192
IN	3736
CN	2662
FR	1249
BR	1213
DE	1197
BE	924
--	681
GB	512
CA	394

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 novelty Identifiers	2
17-11-20 - Nouvelles fiches COVID - FAQ DGAFP	1
10. Corona-Information für unsere Gemeindemitglieder	1

Top-15 Subjects Containing doc/xlsx Files

COVID 19 WEB DIRETTA STREAMING DIGITALIZZAZIONE, DEMATERIALIZZAZIONE, A.I., Big Data e GDPR: processi, competenze e DPO 1/12/20	27
Producătorii români de dezinfectanți, semnal de alarmă: Atenție cum vă protejați împotriva coronavirusului	5
Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	5
TUTELA DEGLI ANZIANI DAL COVID-19: CONTROLLI DEI CARABINIERI NAS SU 232 STRUTTURE	3
COVID 19 WEB DIRETTA STREAM GESTIONE RISCHIO IMPRESA: obbligatorietà adeguati assetti e MOG 231, equilibrio finanziario 2/12/20	3
COVID-19 Forms & FFCRA Form	2
Ihr Corona-Abstrichergebnis	2
Fwd: Cartes familles COVID-19	2
CCS 10631 Se suma personal de UTCH Sur a la campaña de Monitores COVID	2
Oswestry Youth Music Festival COVID risk assessment	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: 132,845
Domains with Potential Mail Servers: 2,643
Email-Capable Domains and Hosts: 50,502
Live Hosts and Domains Not Parked: 45,903

Mobile Apps

Apps in Official Stores: 474

by Store

Apple	238
Google	221
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,751

by Store Type:

Hybrid	918
Secondary	774
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1