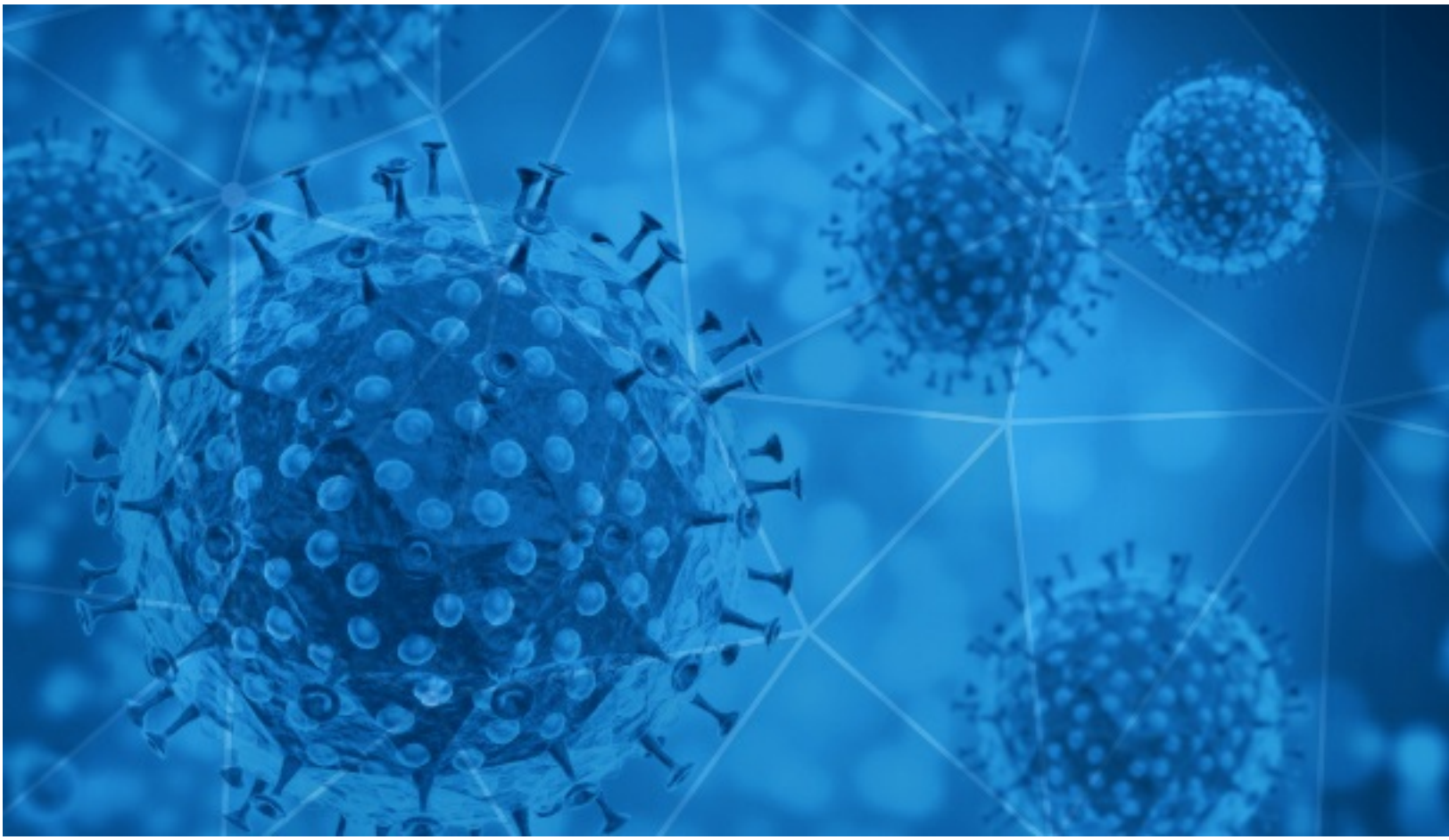
RISKIQ®

RiskIQ i3:

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

2020-09-24



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 2020-09-23 to 2020-09-24. During this period, RiskIQ analyzed 38,779 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,859 unique subject lines observed during the reporting period. The spam emails originated from 1,969 unique sending email domains and 4,405 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

More than 200,000 U.S. coronavirus deaths, the teens who became family breadwinners, and more from Apple News	4105
The Corona Letter: What of a vaccine for children?	3786
Products of COVID19	2709
Help to fight COVID-19 fever alarm security door	1229
My COVID-19 Donation	1155
Covid19 Essential Products	1117
Test de deteccion rapida COVID19	1102
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	1058
Prevencion de covid19	980
Videos para la prevencion de Covid	926
Re: COVID-19 - E-Commerce Website | SEO (Results Guaranteed) - [REDACTED_DOMAIN]	741
face mask against COVID-19	573
Reife Frauen zu Corona-Zeiten treffen	558
Mamparas de proteccion COVID19	524
Mamparas de proteccion contra el coronavirus	522
Post Covid-19 Report.	480
Test Rápido Covid-19 Segunda Generación - 10.000 Un Entrega Inmediata	474
Re:Corona virus Protection Pills and sex pills.	454
Regresa a tu empresa protegido - Especial Protección Covid-19	387
Resuming after Covid-19 Important Information	376
Re: COVID-19 : Boost Your Online Business - [REDACTED_DOMAIN]	303
Re: COVID-19 - Website Maintenance | SEO (Results Guaranteed) [REDACTED_DOMAIN]	289
Covid-19 Rapid Test Kits	273
Covid 19 Weekly questionnaire - Reminder 28	267
Prueba Rápida Covid-19 para Empresas y Domicilio	241

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	4570
insideapple.apple.com	4114
countermail.com	4054
timesofindia.com	3789
medicproduction.com	2709
126.com	1757
keyable.net	1229
stargoldmedics.com	1117
yeah.net	762
nbomeo.com	573

Top-15 IPs Sending COVID Spam

139.99.133.125	2709
190.247.226.160	2287
43.239.110.184	1154
113.116.204.170	1147
85.204.116.74	1117
190.247.240.114	1026
119.122.90.244	774
190.247.242.15	700
46.20.37.30	558
77.87.0.7	480

Top-15 Countries Sending COVID Spam

US	10275
IN	6944
CN	5482
AR	4108
AU	2725
DE	1209
RO	1133
GB	890
BE	744
PL	615

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

PRODUCTOS COVID PARA EMPRESAS	11
Profesjonalny sekretariat w dobie pracy zdalnej / BHP w dobie Covid19	7
Prawo pracy po zmianach - najnowsze przepisy a COVID 19	6
covid 19 pay out	5
COVID-19 Focus IAS/IFRS: novità contabili e fiscali, suggerimenti, soluzioni, rinvii Milano 21/10/20	4
Podsumowanie dzisiejszej debaty na temat priorytetów w profilaktyce chorób zakaźnych wśród personelu medycznego w dobie pandemii COVID-19.	3
Annie COVID-19 app, more uses for secure messaging and drive up flu shot clinic schedule which begins September 28th, 2020-November 6th, 2020	2
¡Últimas inscripciones! Taller en Planificación Estratégica: acciones post Covid-19 - Universidad de Chile	2
Την οικονομική ενίσχυση των μελισσοπαραγωγών της Κρήτης που έχουν πληγεί από τις συνέπειες του covid-19 ζητάει από τον Υπουργό Αγροτικής Ανάπτυξης Μ. Βορίδη ο Αντιπεριφερειάρχης Κρήτη Μ. Χνάρης	2
****NIPSA 521 MEMBERS** CHILDCARE SURVEY FOR PARENTS and CARERS NI SURVEY – CARING DURING COVID PART 2**	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: 126,537
Domains with Potential Mail Servers: 2,929
Email-Capable Domains and Hosts: 47,865
Live Hosts and Domains Not Parked: 70,204

Mobile Apps

Apps in Official Stores: 429

by Store

Apple	220
Google	194
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,444

by Store Type:

Hybrid	798
Secondary	591
Affiliate	55

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	25
Hybrid	2
Official	2