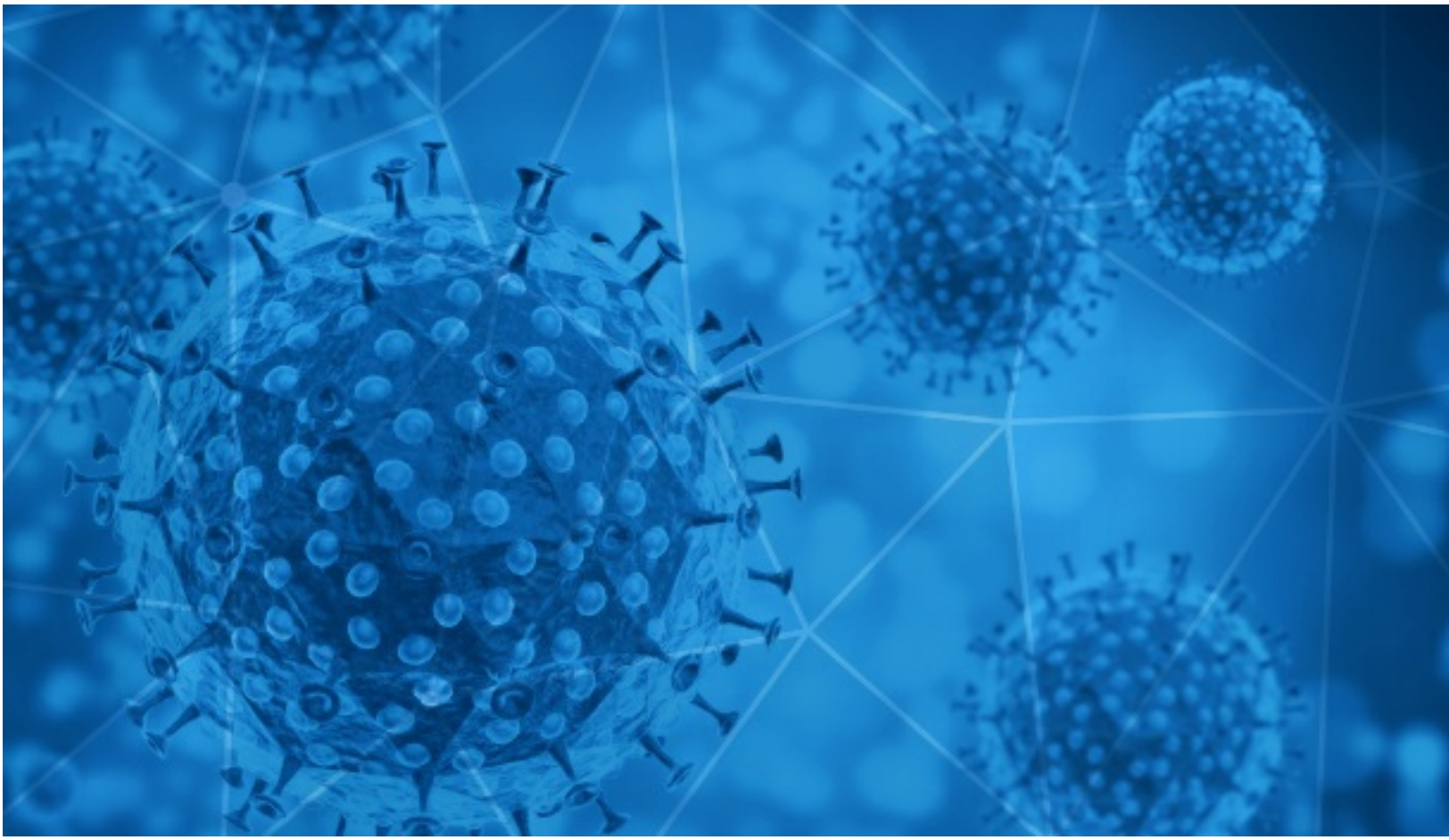
RISKIQ®

RiskIQ i3:

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

2020-11-12



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 2020-11-11 to 2020-11-12. During this period, RiskIQ analyzed 25,877 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,919 unique subject lines observed during the reporting period. The spam emails originated from 2,142 unique sending email domains and 4,308 unique SMTP IP Addresses. Analysts identified 188 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Why it's more difficult to tame the virus	3050
COVID-19 vaccine research studies	1700
Coronavirus 'Stay home - earning big money home'	789
Re: 500.000,00 USD Covid -19 Financial Relief Funds.	628
Taller , Jornadas de trabajo y su Implementación Práctica y normas especiales covid 19	349
(□□) [11□: □□□ □□ □□□] 'COVID-19 □□□ □□□ □□ □□ □□□□' - □□ □□□□ □□ □□□ □□!	324
Re: Corona virus Protection Pills.Order confirmation	306
Atencion covid Estudio Contable Legal e Impositivo para tu negocio	299
Precios IMPACTO / Productos COVID 19	299
Covid Support Fund	278
Re: Digital signage solution for Covid-19	272
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	240
Taller: Jornadas de Trabajo, su Implementación Práctica y Normas Especiales Covid 19	224
Re: Defeat Coronavirus, non contact fever alarm device	215
Contactless infrared body temperature thermometer defeat Coronavirus	210
Help to fight COVID-19 fever alarm security door	205
Adhesivos Distanciamiento Social Covid-19	201
Fwd: <<Drug Discovery Hackathon>> Verification Mail for [Webinar on Designing Drugs Against Corona Virus]	191
COVID-19 Support Donation	185
□ 8:00 TỐI NAY! COVID-19 đã ảnh hưởng như thế nào đến các công ty công nghệ Mỹ? □(AD)	183
Aprovecha Productos COVID en Oferta!	181
Reserve Your Seat . Thriving not just surviving post-COVID	175
Fwd: Coronavirus Tax Relief and Economic Impact Payments	168
Quickest And Safe Method For Home Screening - Avoid COVID	157
Re: Covid-19 Protective acrylic sneeze guards(1/5 lower than your purchase price)	157

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	3053
126.com	964
stargoldmedics.com	810
yeah.net	750
gmail.com	709
keyable.net	630
claimintl.com	628
sihovision.com	478
service.alibaba.com	458
lifecodexx.com	448

Top-15 IPs Sending COVID Spam

192.3.3.143	784
182.75.174.45	628
113.116.205.12	610
31.47.85.9	448
67.219.150.138	372
113.116.194.155	333
95.217.127.138	278
192.241.128.11	200
46.234.110.152	186
219.65.85.24	183

Top-15 Countries Sending COVID Spam

US	6652
IN	4830
CN	3900
DE	1375
FR	911
CZ	907
IT	696
KR	498
GB	471
ES	469

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Vacuna Covid de Pfizer: 11 cosas que necesita saber	63
Pfizer's Covid Vaccine: 11 Things You Need to Know	47
Update on Pfizer's Covid Vaccine:11 Things You Need to Know	46
Επείγουσα ενημέρωση COVID-19	26

Top-15 Subjects Containing doc/xlsx Files

COVID 19 WEB DIRETTA STREAMING SUPERBONUS 110%, ECOBONUS e cessione del credito: contratti, finanziamento e fiscalità 18/12/20	27
COVID 19 WEB DIRETTA STREAMING SUPERBONUS 110%!,(MISSING) ECOBONUS e cessione del credito: contratti, finanziamento e fiscalità 18/12/20	2
7°South Marketing/ COVID 19 Updates/ ADS	2
RE: REPORTE COVID PEDREGAL	2
COVID Update (with correct letter) :)	2
NV COVID-19 positive case 11/10/2020	2
Exceptional Event Report News □□□□□□□□□□□□ COVID-19 11 Nov 2020	2
NOTICE/SHARING: COVID -19 CDBG-CV 2 & ESG-CV2 Round 2 Grant Application RFP Notice	2
COVID Update 11/11/20	2
PLÁTICAS DE CIENCIA DE LA UMDI. POSIBLES DESTINOS DE LA SINDEMIA DE COVID-19 EN EL CONTEXTO MEXICANO.	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: 132,339
Domains with Potential Mail Servers: 2,657
Email-Capable Domains and Hosts: 50,347
Live Hosts and Domains Not Parked: 45,514

Mobile Apps

Apps in Official Stores: 474

by Store

Apple	241
Google	218
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,729

by Store Type:

Hybrid	908
Secondary	762
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1