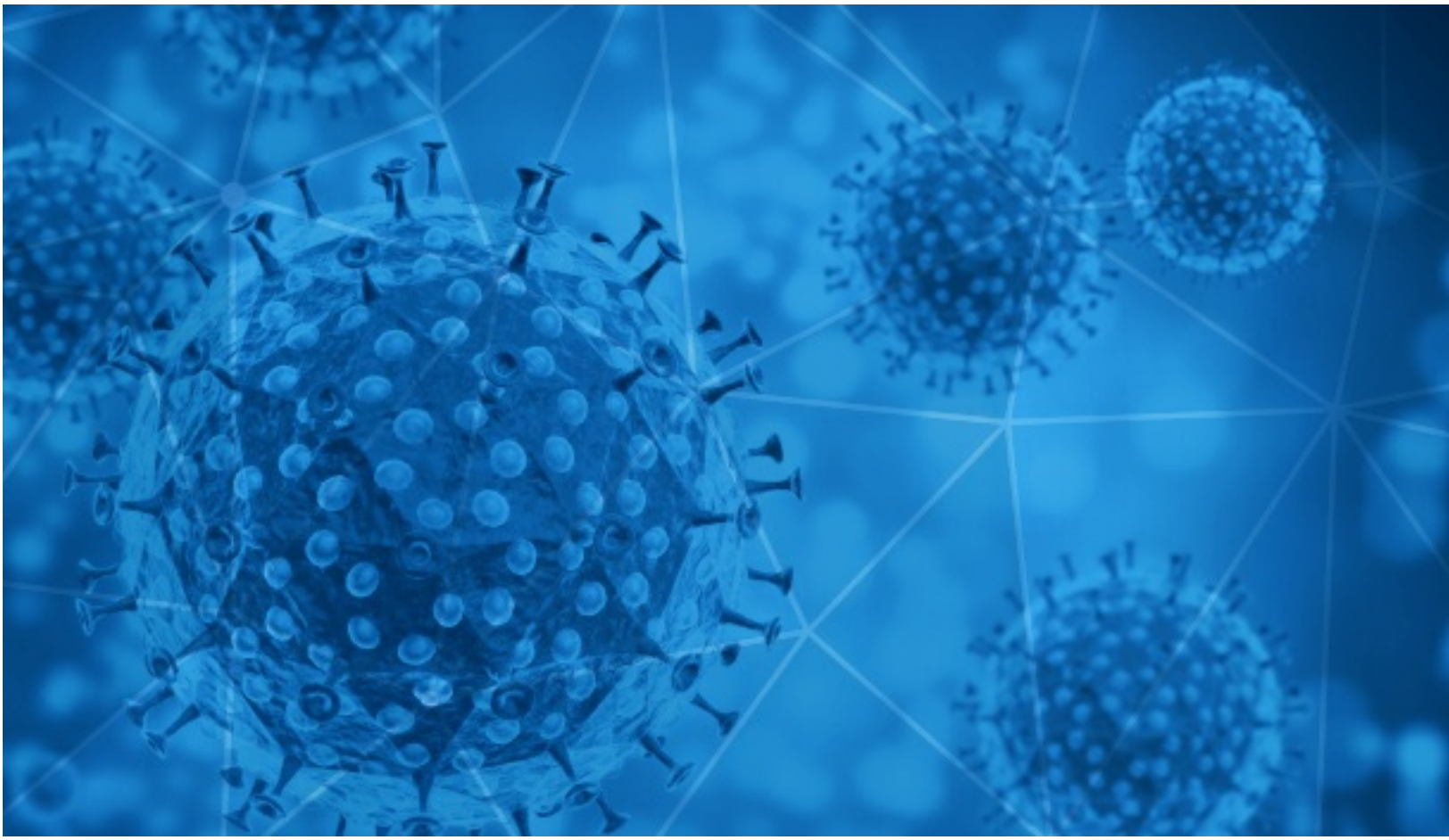
RiskIQ i3:

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

2020-12-29



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 2020-12-28 to 2020-12-29. During this period, RiskIQ analyzed 31,446 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,327 unique subject lines observed during the reporting period. The spam emails originated from 1,687 unique sending email domains and 3,337 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	14176
The Corona Letter: Is natural immunity queering vaccine push?	4253
[Earn Credits] ___A Covid19 Vaccine In a Pill___No_BS__See_Proof__	487
Let’s fight together to get through the COVID-19	418
SPECIAL REPORT: How Brits Are Earning Millions From Home During Coronavirus Pandemic Thanks To Celebrity Chef Gordon Ramsay	409
Offering N95 FACE MASK (3M 1860,1860S, Makrite 9500 N95,N95S,HARLEY, SAMPLING SWAB AND TUBE KITS,Novel Coronavirus (COVID-19) Test ,quick delivery in a couple days	283
No te relajes - Prevencion frente al Covid-19	277
Adhesivos Distanciamiento Social Covid-19	272
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	264
Coronavirus Is Spinning Out of Controlâ¦	245
PACK DESINFECCIÓN COVID-19 CON DESPACHO GRATIS	234
Promoción Insumos Covid-19 Especial Para Empresas	221
Van Gucht voorzichtig ondanks ‘kantelpunt’ - Jos Hermans (96) krijgt als eerste Vlaming het coronavaccin: ‘Laat maar komen’ - Scholen waren niet de aanjagers van Brusselse tweede golf	215
COVID ALLEVIATION STIMULUS PROGRAM [IMF]	214
Virtual Office Hours – Covid-19 (PPP/EIDL), 12/28 - 01/01	193
NCJ Daily - Fieri Fund. 45 New COVID Cases. NCJ Preview. Sneaker Wave Warning. Storm Rain Totals.	186
Influweb contro il coronavirus	179
Good Morning, SA | First take on Covid-19 second wave and one million cases in SA	164
Shop Now: COVID19s Biggest Defense Is The KN95 Certified Mask Health Official State	159
1,8 Milliarden Pakete: Deutsche Post mit Rekord im Corona-Jahr 2020	130
Fwd: AICTE's Webinar on Corona Safe Engineering Fellowship	126
GLOBAL COVID-19 PANDEMIC	125
Beanspruchen Sie Ihr Operation Covid-Paket	123
Re: Digital signage solution for Covid-19	122
Covid19 - Zahlung ist erforderlich.	119

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	14178
timesofindia.com	4253
gmail.com	750
websbestmarketing.com	487
163.com	314
hongchengco.com	291
consons.com.cn	283
armaproductora.com	277
transiente.cl	272
members.lasvegas.com	245

Top-15 IPs Sending COVID Spam

103.225.53.98	800
103.225.54.238	707
103.225.52.86	550
103.225.53.35	548
103.225.54.97	475
103.225.53.79	462
103.225.54.157	455
103.225.52.36	437
103.225.54.26	404
103.225.52.177	399

Top-15 Countries Sending COVID Spam

JP	14225
US	6358
IN	4374
CN	1141
GB	734
--	539
BE	480
AR	447
FR	345
ES	340

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

Ocena ryzyka zawodowego (aktualizacja pod względem COVID -19) / ZUS w praktyce	17
Emergenza COVID 19 WEB ON LINE Società a partecipazione pubblica: governo societario e equilibrio finanziario 17/2/20	11
El COVID-19 no ha frenado los tratamientos de fertilidad	2
Betreuergenehmigung Impfung Covid19	2
PR "Aktuālā informācija par vakcīnām pret Covid-19 vienuviet"	2
CCS/10964: Suman 45,559 casos confirmados y 4,203 defunciones por COVID-19	2
RE: REPORTE COVID PEDREGAL	1
Fwd: Geneva COVID Positive.xlsx	1
PI Coronazahlen	1
FW: Revised- SOP corona virus	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: 137,757
Domains with Potential Mail Servers: 2,589
Email-Capable Domains and Hosts: 52,481
Live Hosts and Domains Not Parked: 48,202

Mobile Apps

Apps in Official Stores: 498

by Store

Apple	244
Google	238
WindowsPhone	15
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,957

by Store Type:

Hybrid	1004
Secondary	893
Affiliate	60

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1