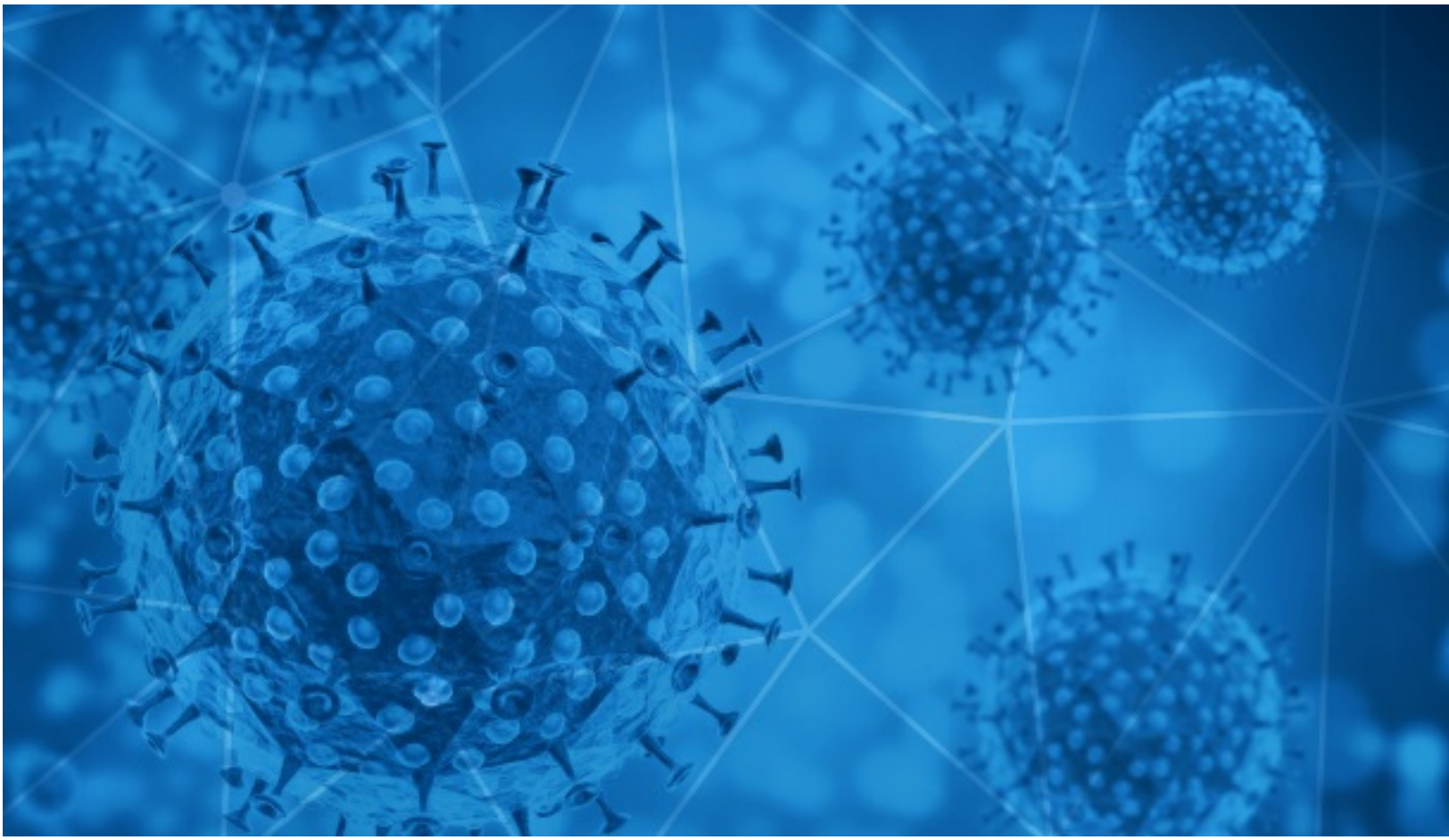
RISKIQ®

RiskIQ i3:

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

2020-07-08



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 2020-07-07 to 2020-07-08. During this period, RiskIQ analyzed 23,551 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,396 unique subject lines observed during the reporting period. The spam emails originated from 2,350 unique sending email domains and 4,050 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Oscillating between lockdown and unlock	1492
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	1177
COVID-19 - Mobile App Development/ PHP, Magento, Drupal, E-Commerce -etc [REDACTED_DOMAIN]	1063
IMF COVID-19 DSP	816
RE: COVID-19.	668
Test Rapidos COVID -19	465
PyMEs contra el COVID19	375
Implacable contra el COVID-19 AMONIOX	331
RE: Delayed SOA Payment Due To COVID-19 Situation	311
Oferta Test Rápidos COVID-19, Mascarillas, Alcohol Gel y Amonio Cuaternario.	306
Kit test covid - Aprovechalo desde 5490	301
Test Rapido Covid 10.000 CLP	271
PRODUCTOS PREVENCIÓN COVID-19	255
COVID protective gear in stock!	244
Covid 19 Wohltätigkeitsfonds	236
Covid-19 relief payments	231
Deadlier than the coronavirus	229
Medcorp Equipments COVID-19 Products Promo Sales - 20% Discount	205
Korea Trend News-COVID19(4)	199
TWÓJ COVID-19 FUNDUSZE ZWROTÓW / ZWOLNIENIA	195
Re: keep away from Covid-19	191
YOUR COVID-19 REIMBURSEMENT / RELIEF FUNDS	188
Did you make any of these 6 money mistakes in coronavirus crisis? A financial advisor could have helped	184
COVID-19	183
RE:The way to live under COVID 19	173

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	3558
126.com	1627
timesofindia.com	1492
countermail.com	681
googlemail.com	668
163.com	551
daum.net	410
serviciosrentables.cl	331
daehoshipping.com	311
correosmasivos.cl	306

Top-15 IPs Sending COVID Spam

157.119.122.139	885
133.223.65.52	668
122.34.222.210	591
119.122.89.175	500
119.122.91.254	392
164.68.105.141	370
203.124.11.192	341
164.90.181.158	331
103.125.191.59	311
142.93.6.221	254

Top-15 Countries Sending COVID Spam

US	6951
IN	3078
CN	2397
DE	967
JP	963
FR	952
AR	945
KR	823
--	759
RU	573

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

We Are Necessarily Strengthening Our COVID-19 Response	22
IMPORTANT ; post-coronavirus	14
Fwd: Measures to be taken to contain Covid 19	4
¿Sabe cuánto han perdido las empresas por Covid-19?	3
NdP_Los 5 tipos de usuarios de carsharing post-COVID	3
Comunicat | EUROPAfest vs Covid-19	3
Comercio exterior y Covid-19: el primer semestre exportaciones cayeron 9,9% e importaciones disminuyeron 18,5%	2
Reminder: Financial Accounting Impact of COVID-19- An In-depth Look at IFRS	2
Covid-19 compensation fund	2
[DDC4GARLANDEMCS] Hospital Daily EMResource COVID-19 Reporting Results - July 7th, 2020	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: 112,331
Domains with Potential Mail Servers: 2,771
Email-Capable Domains and Hosts: 42,564
Live Hosts and Domains Not Parked: 54,077

Mobile Apps

Apps in Official Stores: 319

by Store

Apple	174
Google	136
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 856

by Store Type:

Hybrid	537
Secondary	283
Affiliate	36

Blacklisted Mobile Apps: 21

by Store Type:

Secondary	19
Hybrid	1
Official	1