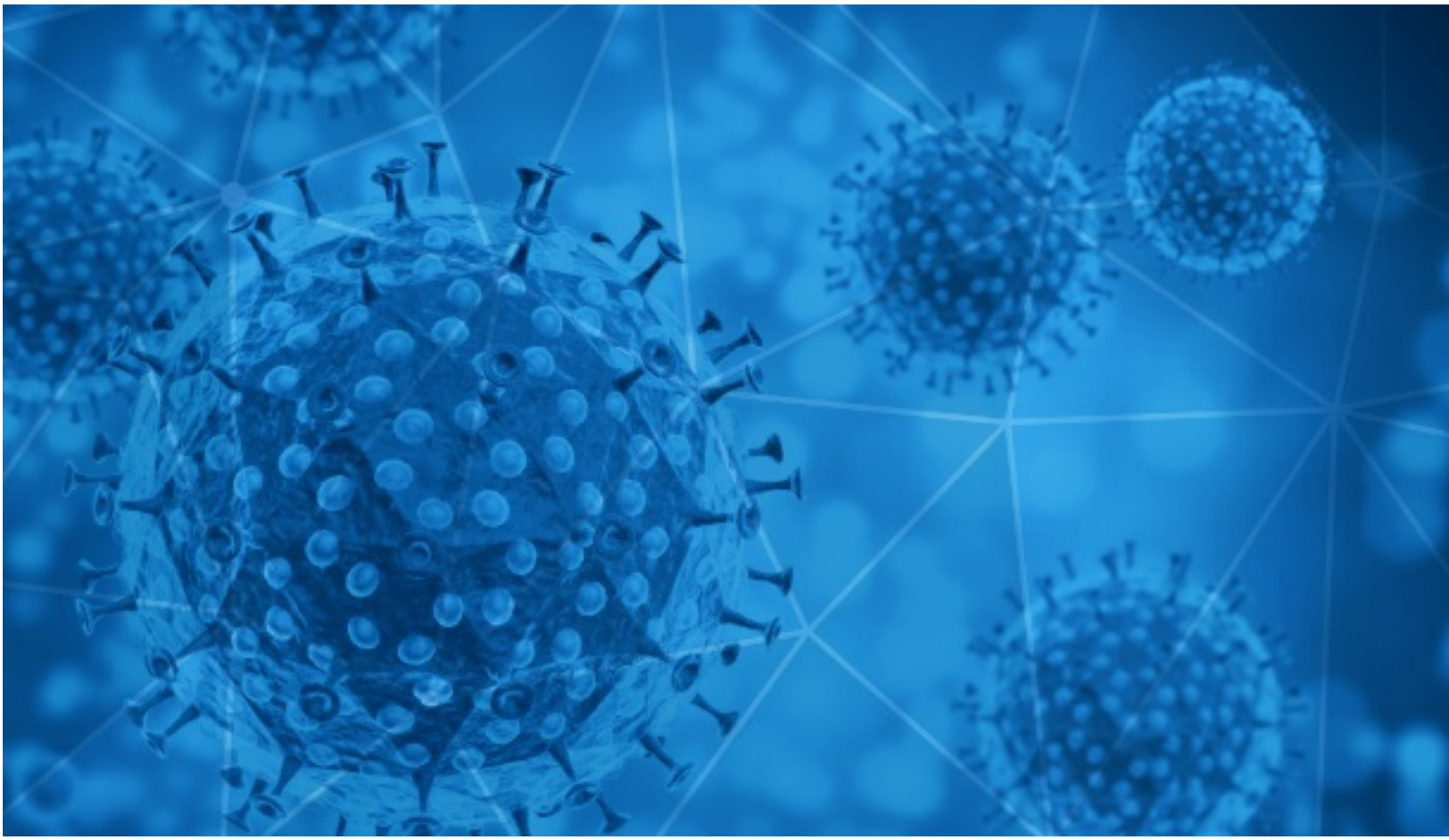
RiskIQ i3:

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

2021-01-05



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 2021-01-04 to 2021-01-05. During this period, RiskIQ analyzed 44,216 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,195 unique subject lines observed during the reporting period. The spam emails originated from 1,932 unique sending email domains and 3,562 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

Weiter vor Corona Infektionen schützen (Ab 0,16 pro St.)	8741
Vermeiden sie Corona Infektionen (Maske am 16 Cent)	6294
TCS bets big on this in-demand technology amid COVID-19 | Pros and Cons of Python programming language that every learner must know	5505
The Corona Letter: India's cold chain skew	4932
Know the Facts About COVID-19	833
Fake news about COVID-19 is spreading faster than virus	626
Covid-19 Inheritance	599
Todo En Insumos Covid 19	568
Let’s fight together to get through the COVID-19	409
Get your Corona-virus Mask while supplies last!	397
Reduce your risk of Corona-virus with this Mask	377
Traveling soon, wear this mask to fight chances of getting Corona-virus	376
New Corona-virus Mask!	374
Covid-19 Relief F und	342
COVID-19 Financial Support/Loan Program.	289
Covid-19 Relief Grant	253
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	235
BREAKING | Assange kan niet worden uitgewezen aan Amerika - De complexe zoektocht naar coronapatiënt nul - Vandenbroucke: ‘Verwacht nog geen versoepelingen’ - Victors vrouw was een ziekelijke ruziemaker: ‘Ik was altijd bang’ - Coronacommissaris Pedro…	222
Promoción Insumos Covid-19 Especial Para Empresas	216
Why Food Delivery Model is Essential for Restaurant Businesses post-Covid	211
UNITED NATIONS CORONAVIRUS RELIEF FUND (UNCRF)	210
Influweb contro il coronavirus	198
Good Morning, SA | KZN Covid cases edge up, SA diplomats lose bid to stay in Europe	188
Coronavirus au Maroc: 1.005 nouveaux cas, 33 décès	176
What is in the New Covid Relief Law	162

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

outlook.de	15037
techgig.com	5582
timesofindia.com	4933
gmail.com	3139
clevisor.com	1524
163.com	608
mailinator.cl	568
126.com	478
xcontrol.it	342
hongchengco.com	339

Top-15 IPs Sending COVID Spam

51.81.24.158	12589
219.65.84.187	5556
194.146.44.135	1662
69.94.152.252	1523
142.4.14.219	806
136.243.29.110	774
93.174.10.25	405
150.136.130.23	342
175.44.33.22	327
219.65.85.33	319

Top-15 Countries Sending COVID Spam

FR	14060
IN	10728
US	9434
--	1942
DE	1777
CN	1715
GB	634
BE	504
JP	324
IT	320

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

Emergenza COVID 19 WEB ON LINE Società a partecipazione pubblica: governo societario e equilibrio finanziario 17/2/21	11
POSITION PAPER AD INTERIM VACCINAZIONE ANTI-COVID19 E GRAVIDANZA	3
PONUDA ZA TESTIRANJE NA COVID 19 ANTIGEN	3
Consent form – Rapid COVID-19 Testing	3
URGENT Due 11am on Jan. 5 NF COVID19 Vaccination Data	3
Ampas survey COVID-19 impacted	2
Buletin de presa 04.01.2020 + comunicat actiuni COVID	2
FW: [listserve@cosaslc.org] FW: COVID-19 - Situation Report #41	2
Re: Actualización de Directorio para vacuna COVID-19	2
Fwd: COVID 19 Support Group at VCS Inc.	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: 138,398
Domains with Potential Mail Servers: 2,576
Email-Capable Domains and Hosts: 52,716
Live Hosts and Domains Not Parked: 49,942

Mobile Apps

Apps in Official Stores: 496

by Store

Apple	241
Google	239
WindowsPhone	15
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,987

by Store Type:

Hybrid	1021
Secondary	905
Affiliate	61

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1