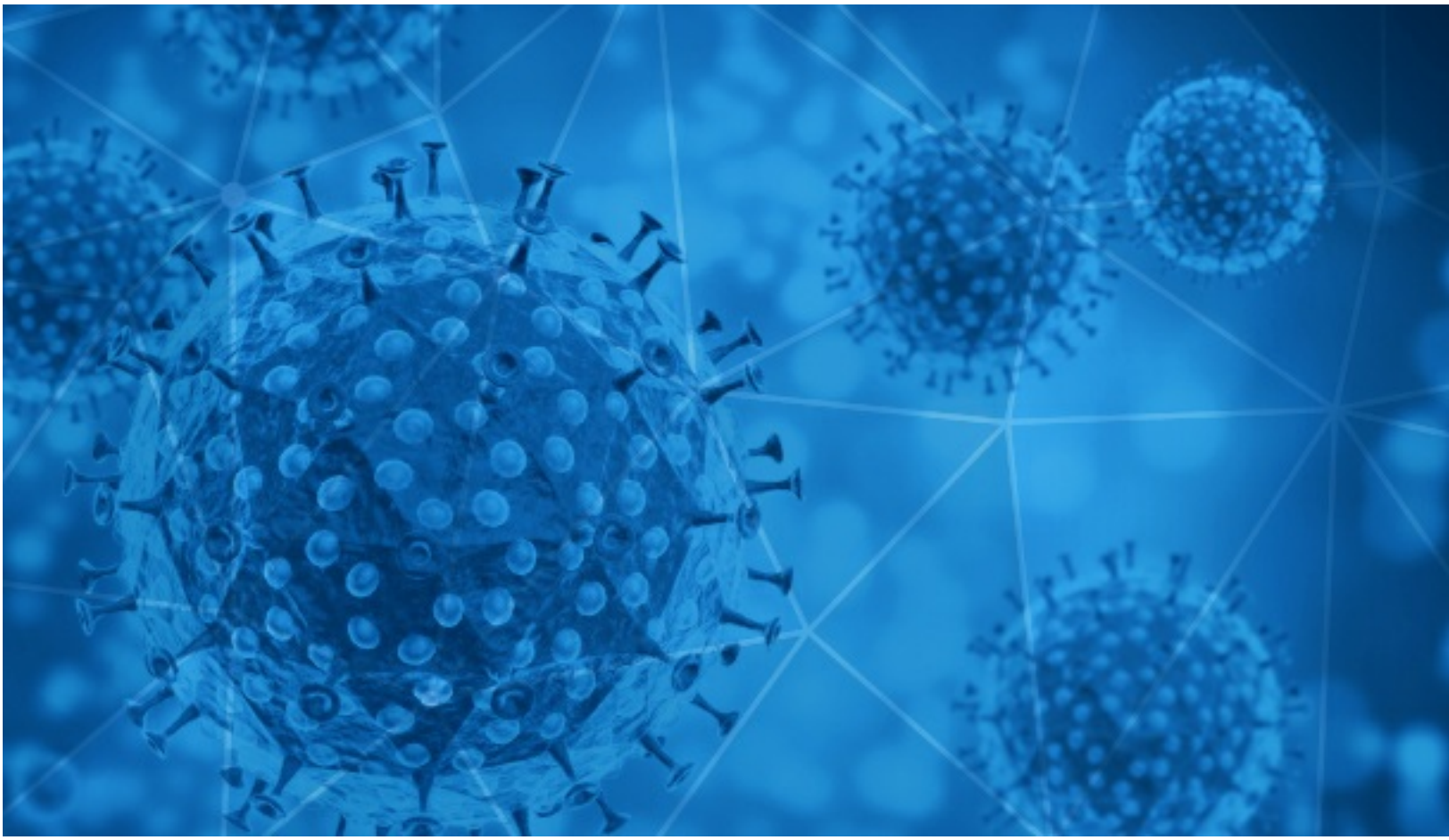
RiskIQ i3:

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

2021-01-01



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 2020-12-31 to 2021-01-01. During this period, RiskIQ analyzed 4,147 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 758 unique subject lines observed during the reporting period. The spam emails originated from 400 unique sending email domains and 975 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

Todo En Insumos Covid 19	495
Puricador y Sanitizador de Aire, Estirilización contra Coronavirus	291
Good Morning, SA | SA diplomats sue over Covid, B&B owners beaten by massive losses	169
Let’s fight together to get through the COVID-19	151
And the Startup of the Year is…, Covid Haves & Have Nots, and more	119
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	92
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	86
WATCH: What's Going on With California's Covid Numbers?	85
UK approves Oxford vaccine | India split into 6 regions in hunt for UK strain |Â US Nurse testsÂ +ve over a week after receiving Pfizer Covid-19Â vaccine	80
Formati per la trasformazione digitale post Covid	79
Your daily news fix: Year-end cheer: India closer to Covid-19 vaccine after UKâs Oxford nod	64
Las compañías farmacéuticas han mantenido su investigación más allá del Covid-19	60
How You Can Stop COVID Lies From Spreading	57
Re: covid-19 touch monitor	56
"Op laatste nippertje aan ramp ontsnapt" - Tientallen vermisten door corona in tweede lockdown - Gert Verhulst verliest zijn papa	56
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	56
Re: Comment on Los Angeles County coronavirus deaths reach 10, 000 total	55
Your COVID-19 Test Results	53
ENTRUST COVID Test!	52
Re:coronavirus civil mask / Chinese qualified manufacturer	44
Re: Digital signage solution for Covid-19	43
Hay 519 casos nuevos y seis fallecidos por COVID-19	42
Sustaining Customer Experience Amidst the Coronavirus Threat	36
Coronavirus Relief Update - What You Need To Know	33
COVID-19 Chinese protective products	31

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

grupocorreomasivo.com	495
mailinator.cl	291
163.com	226
news24.com	169
nieuwsblad.be	164
gmail.com	152
ettech.com	119
126.com	99
disqus.net	96
hcprintery.com	92

Top-15 IPs Sending COVID Spam

51.83.246.190	176
51.83.246.189	163
175.44.33.22	122
69.63.146.169	92
180.165.115.217	92
120.229.72.10	90
51.83.246.191	89
192.146.0.93	82
51.83.246.184	80
51.83.246.188	79

Top-15 Countries Sending COVID Spam

US	1398
FR	871
CN	532
AU	211
BE	166
IN	160
GB	156
SG	92
IE	66
JP	63

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

Comunicat actiuni COVID 19	2
COVID 19 UPDATE - Shared facilities	2
FW: COVID VACCINE INFORMATION	2
MD COVID News Hour 123020	1
COVID Vaccine Update	1
Inf. Prevention Test Revised for Covid	1
IMSS Boletín 870.- Avanza inmunización contra COVID-19 para personal médico y de enfermería de la Operación Chapultepec (FOTOS)	1
RV: Altas pacientes covid imss	1
RV: AUTORIZACION PACINTE COVID ENRIQUE GONZALEZ MUÑIZ	1
covid	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: 138,043
Domains with Potential Mail Servers: 2,564
Email-Capable Domains and Hosts: 52,584
Live Hosts and Domains Not Parked: 49,006

Mobile Apps

Apps in Official Stores: 496

by Store

Apple	241
Google	239
WindowsPhone	15
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,973

by Store Type:

Hybrid	1012
Secondary	901
Affiliate	60

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1