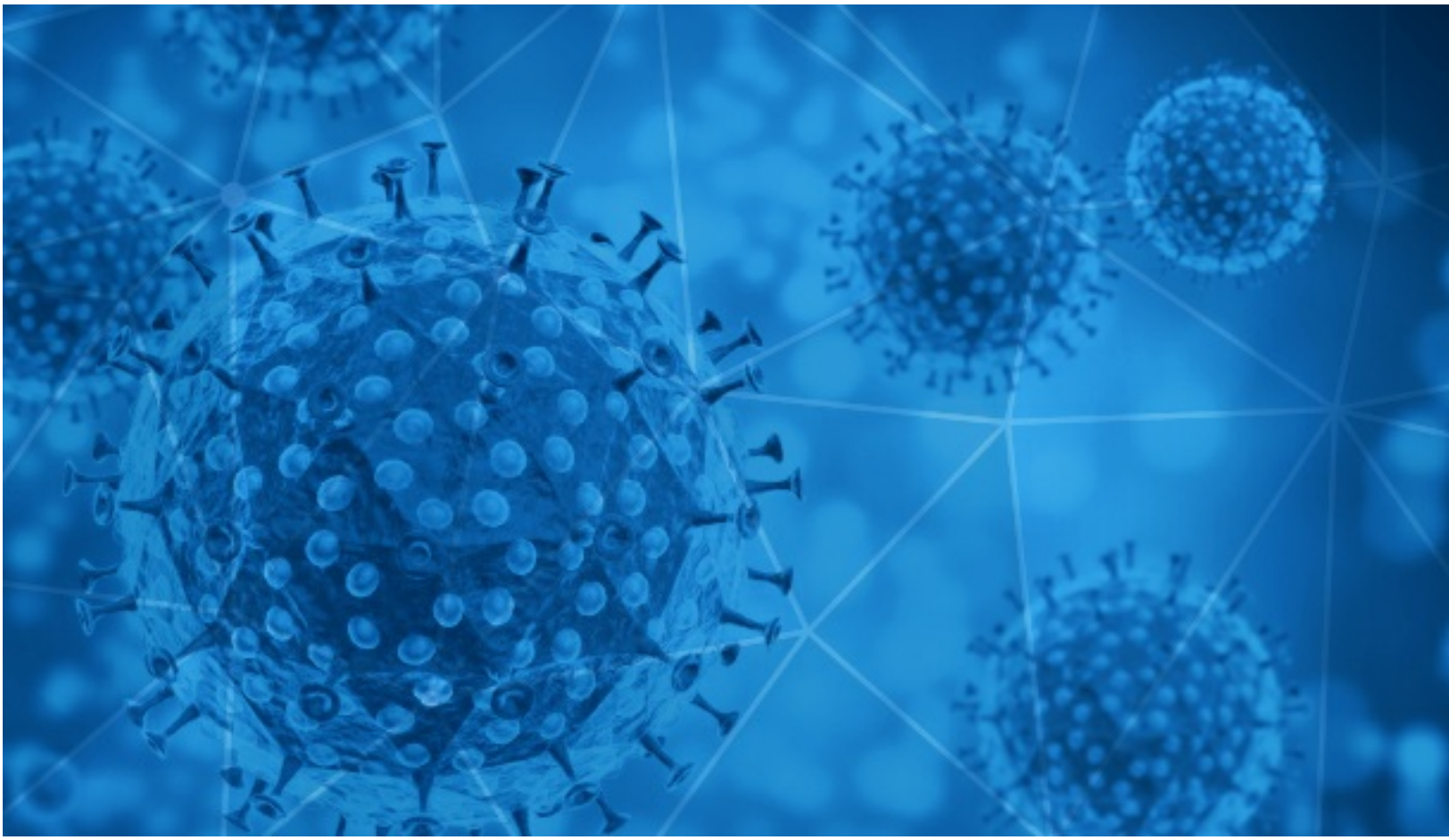
RiskIQ i3:

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

2021-01-04



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 2021-01-03 to 2021-01-04. During this period, RiskIQ analyzed 42,508 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 800 unique subject lines observed during the reporting period. The spam emails originated from 524 unique sending email domains and 2,060 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	24163
COVID-19 Update: We are open and now offering Free Virtual Consultations	1706
Detect COVID19 From A Distance Using Heat Scan IR Thermometer	1352
The Ultimate COVID19 Fighting Tool- All New Heat Scan Infrared Thermometer	1323
Detecting COVID19 From A Distance Using Heat Scan IR No Touch Thermometer	1321
At Home COVID19 Detecting Made Easy- Just Point And Shoot	1135
Point And Shoot- That Easy To Detect COVID19 Temperate Readings At Home	1131
Checking For COVID19 Temperature Readings Using Infrared Heat Scan Thermometer	1104
Check COVID19 Temperature Readings At Home, Just Point And Shoot	1096
ANTI-COVID "Touchless" Thermometer Laser Tech Lets You Take Their Temp From A Distance	1076
Heat Scan IR Thermometer Lets You Check An Individual For COVID19 High Temperature	968
Safely Check For COVID19 Symptoms Using All New Infrared Heat Scan Thermometer	889
Check Early Signs Of COVID19 Using Revolutionary Infrared Heat Scan Thermometer	824
Detecting Early Signs Of COVID19 Using All New Infrared Heat Scan Thermometer	819
Covid-19 Donation	360
COVID-19 PANDEMIC COMPENSATION FUND	190
Todo En Insumos Covid 19	137
Coronavirus au Maroc: 1.005 nouveaux cas, 33 décès	131
Covid-19 Financial Relief Donation	125
Coronavirus updates: Bharat Biotechâs Covaxin can be used as backup, says AIIMS Director Dr Randeep Guleria	109
Re:□coronavirus civil mask / Chinese qualified manufacturer	99
Re:covid-19 touch monitor	95
To combat the wild spread of Corona virus Pandemic	80
Corona-uitbraak net voor vaccinatie: acht bewoners en vier medewerkers besmet in Pelts rusthuis | Zwembadbouwers hebben nu al bomvolle agenda | Jeugdliefdes vinden elkaar bijna zestig jaar later terug	71
Coronavirus au Maroc: 1.171 nouveaux cas en 24h, 27 décès	70

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	24166
elavatehealthclinics.com	3997
garnerresrouces.com	3362
daginnzeemorgun.com	2532
bowhantersuperstore.com	2180
akhirawahdnshaamolananjibobih.com	983
bzfereshchow.com	968
gmail.com	636
akhirawahdanshaamolananjibobih.com	624
163.com	238

Top-15 IPs Sending COVID Spam

72.19.15.143	3957
72.19.15.208	3329
72.19.15.137	2519
72.19.15.170	2154
72.19.15.159	968
103.225.55.104	626
103.225.55.100	566
103.225.52.82	561
103.225.52.143	520
103.225.55.138	508

Top-15 Countries Sending COVID Spam

JP	24470
--	12991
US	1972
CN	487
FR	389
BG	363
GB	323
NL	150
AU	148
SI	124

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

IMSS Boletín 004.- Mantiene IMSS atención de enfermedades crónico degenerativas durante pandemia por COVID-19	2
Tratamento inadequado de cadáveres de doentes falecidos com COVID-19 no Centro Hospitalar de Lisboa Central	2
CCS/11000 Suman 4 mil 300 defunciones por COVID-19 en Chihuahua	2
CENSO COVID-19 HGAV	1
FW: Covid Vaccine Staff Update	1
Welcome back! Covid Update and more :)	1
IMSS Boletín 005- La vitamina D actúa como protector de enfermedades respiratorias como la influenza y, probablemente, contra COVID-19 (FOTOS)	1
COVID 19 RT PCR REPORTS DAILY STAT 03.01.2021	1
Fwd: MATERIAL COVID A. SALUDABLE	1
COVIDSafe Venues - Stopping the Complacency Creep	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: 138,349
Domains with Potential Mail Servers: 2,551
Email-Capable Domains and Hosts: 52,678
Live Hosts and Domains Not Parked: 47,563

Mobile Apps

Apps in Official Stores: 496

by Store

Apple	241
Google	239
WindowsPhone	15
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,986

by Store Type:

Hybrid	1021
Secondary	905
Affiliate	60

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1