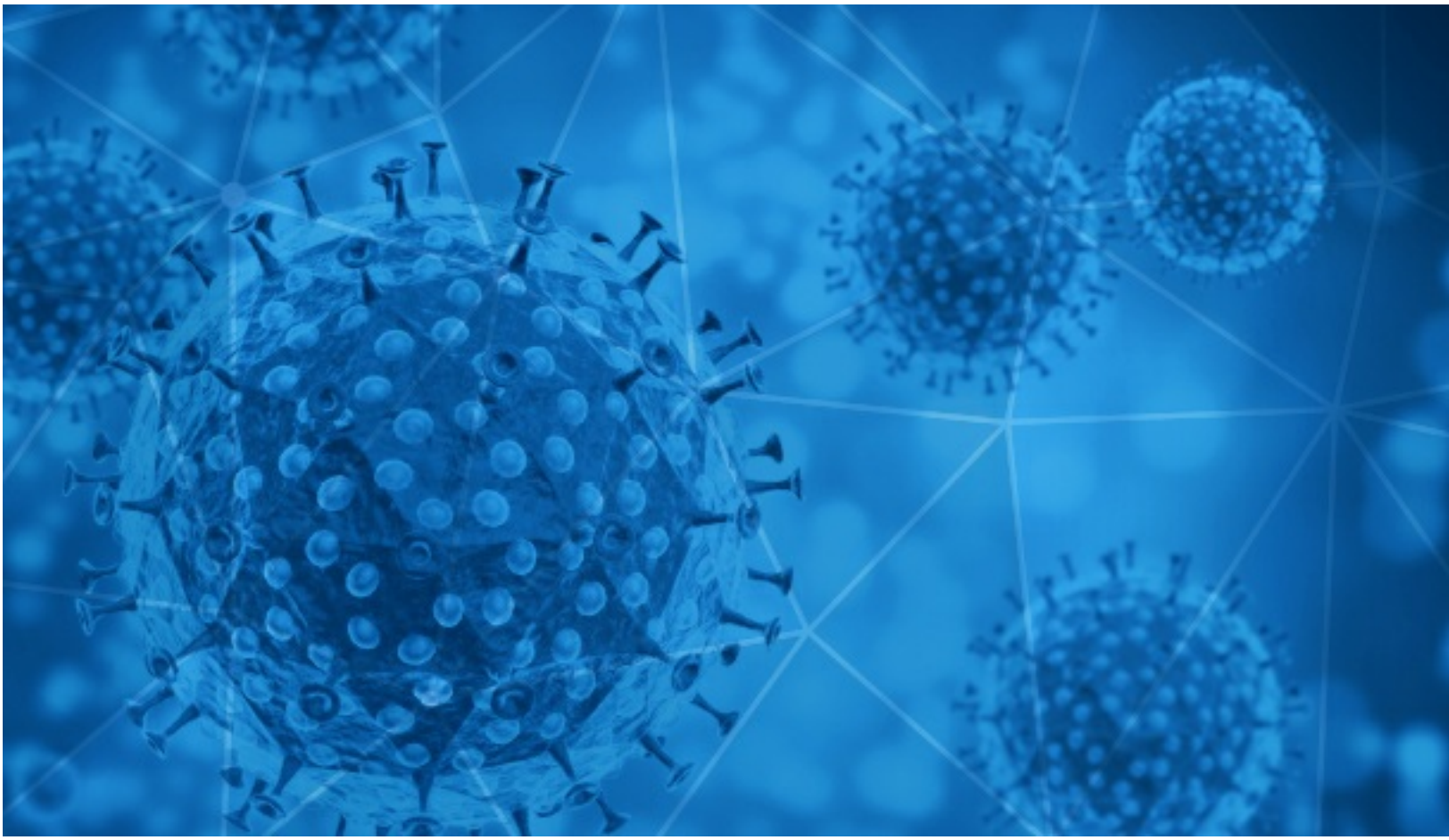
RISKIQ®

RiskIQ i3:

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

2020-12-24



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 2020-12-23 to 2020-12-24. During this period, RiskIQ analyzed 49,141 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,567 unique subject lines observed during the reporting period. The spam emails originated from 1,878 unique sending email domains and 4,029 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	15266
Trump issues a wave of pardons, the mysterious link between COVID-19 and sleep, and more from Apple News	4706
TIMES TOP10: New Covid strain not in India, for now	4399
The Corona Letter: Vaccines easiest to tweak for a new virus strain	3727
Watch out for COVID-19 vaccine scams	1658
Opportunity Knocks: How You Can Make Money From VideoTours 360 During Covid-19	1003
Contactless infrared body temperature thermometer defeat Coronavirus	747
Re: Defeat Coronavirus, non contact fever alarm device	712
Ingresaron TEST COVID19 de deteccion rapida	560
LJC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation.	463
La solution anti covid pour votre entreprise	403
Freelancer Coronavirus Survey #4	315
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	258
Covid shot is Ã¢ÂÂmorally acceptableÃ¢ÂÂ	249
Test Rápido Covid-19 Segunda Generación	230
Dieses Covid-Spezialpaket wird geliefert	222
Jailed Covid Student Calls on Trump For Assistance	221
Trabajo Seguro Covid-19 Serprom Spa	194
Let’s fight together to get through the COVID-19	189
PACK DESINFECCIÓN COVID-19 CON DESPACHO GRATIS	183
Covid-19 Spende	180
COVID-19 Vaccine Update	168
COVID ALLEVIATION STIMULUS PROGRAM [IMF]	156
Covid-19 Disbursement ,	156
NCJ Daily - 12 New COVID Cases. Snowy Weather. Food for People Fundraiser. Vaccines Roll Out.	155

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	15268
insideapple.apple.com	4707
bounce.indiatimes.com	4399
timesofindia.com	3730
subscriptions.cms.hhs.gov	1665
keyable.net	1459
gmail.com	964
quzdilwy.club	737
herculist.com	623
aol.com	597

Top-15 IPs Sending COVID Spam

113.116.207.145	1458
103.225.54.40	760
188.227.86.37	737
103.225.54.95	735
216.87.190.232	643
190.247.254.103	560
69.94.152.247	510
103.225.52.213	496
103.225.52.62	464
131.0.103.220	463

Top-15 Countries Sending COVID Spam

JP	15340
US	14895
IN	8457
CN	2592
RU	943
GB	861
DE	715
AR	708
BR	554
FR	445

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Fwd: Signalement Covid positif	1

Top-15 Subjects Containing doc/xlsx Files

Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	12
Precizări de presă privind modificarea condițiilor de intrare pe teritoriul Regatului Belgiei, în contextul pandemiei de COVID-19	4
Δελτίο Τύπου: ΥπΑΑΤ, Μ. Βορίδης: Πάνω από 33 εκατομμύρια ευρώ σε πληγέντες παραγωγούς λόγω Covid-19 - Ολοκληρώθηκε η πληρωμή των δικαιούχων	3
Buletin de presa 23.12.2020 + comunicat actiuni COVID19	2
COVID: CRISI ECONOMICA DA RECESSIONE, ITALEXIT ABRUZZO AFFIANCO DELLE PICCOLE E MEDIE IMPRESE	2
Excel Covid-19 Residencia Antequera San Juan de Dios 24/12/2020	1
Anpassungen CoronaSchVO	1
Vacinação Covid - 19 ERPIs - Cooperativa Mista de Ensino do Laranjeiro - Centro Sócio-Cultural de Apoio à Terceira Idade	1
Plan de desinfección frente COVID	1
FW: [redacted] COVID-19 ([redacted] QR Code [redacted] MKD1 [redacted] MKD2)	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: 137,363
Domains with Potential Mail Servers: 2,597
Email-Capable Domains and Hosts: 52,337
Live Hosts and Domains Not Parked: 47,544

Mobile Apps

Apps in Official Stores: 494

by Store

Apple	245
Google	234
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,934

by Store Type:

Hybrid	989
Secondary	886
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1