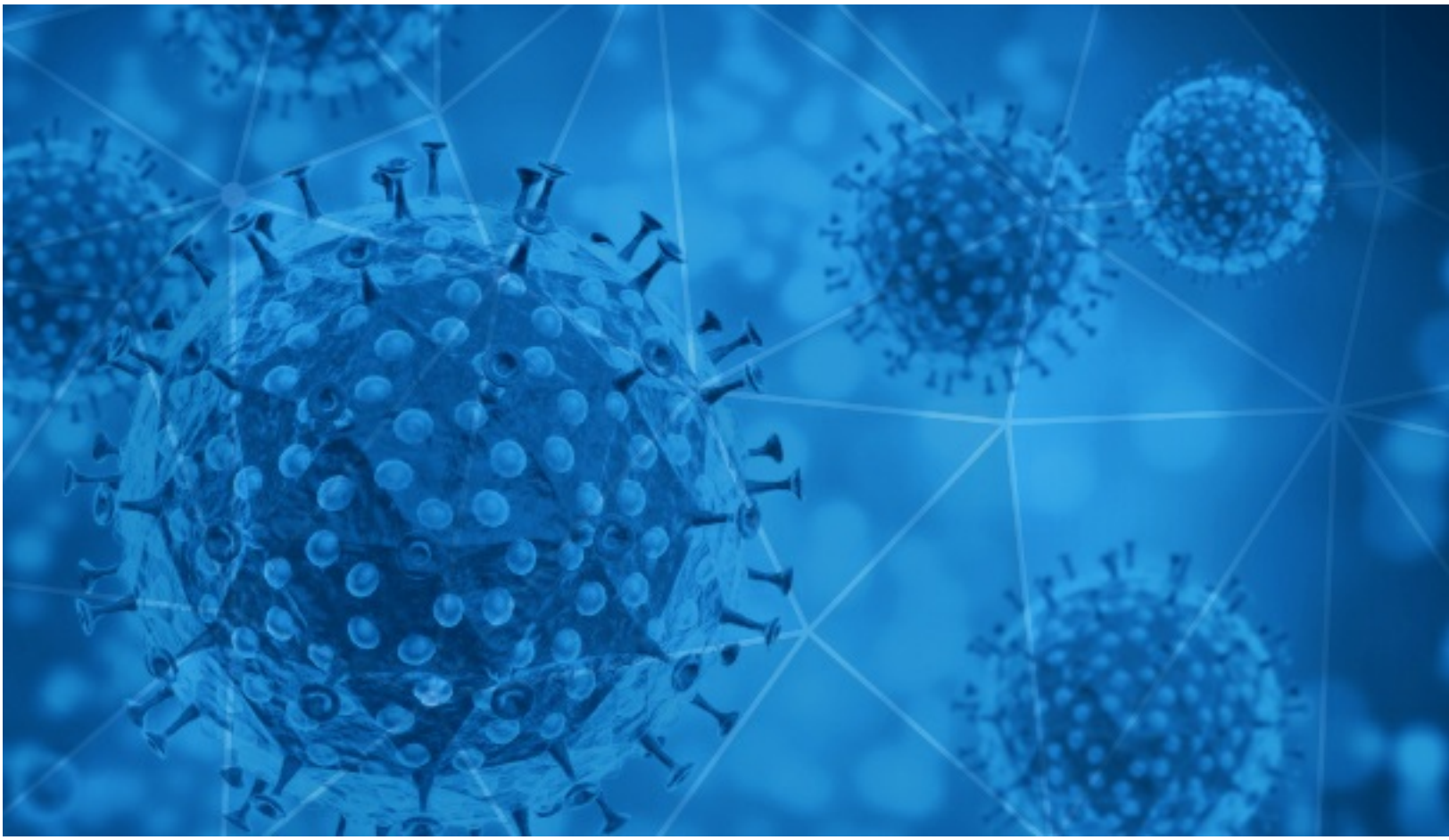
RiskIQ i3:

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

2020-07-01



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 2020-06-30 to 2020-07-01. During this period, RiskIQ analyzed 55,601 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,524 unique subject lines observed during the reporting period. The spam emails originated from 2,379 unique sending email domains and 4,874 unique SMTP IP Addresses. Analysts identified 727 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	14336
Govt approves far reaching reforms in India's space sector; 'Made in India' ventilators to combat COVID-19...Read more in the newsletter!	3826
Covid-19 Credit Facility Business Owners	3283
Due to Coronavirus I lost 50lb in 61 Days. What about you?	2378
The Corona Letter: Did we unlock too much too soon?	1981
COVID 19 RELIEF PROGRAME AND BUSINESS FUNDING SCHEME	1835
My COVID-19 Donation.	1531
Test Rapido COVID 19	783
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	764
Minimice el Riesgo de contagio del Coronavirus - Validacion Biometrica	706
Diederik Health and Safety Consultant - Covid-19 Safety Plan Package Invoice	687
APLICACIÃN PRUEBAS RÃPIDAS COVID-19: CÃ³mo funcionan y cÃ³mo se aplican	671
COVID-19 - Mobile App Development/ PHP, Magento, Drupal, E-Commerce -etc texelglobal.com	623
Test Rápido COVID-19	612
COVID-19 Protection Products	532
[Possible Spam] Covid 19 Wohltätigkeitsfonds	524
Oferta Test RÃ¡pidos COVID-19	461
Implacable contra el COVID-19 AMONIOX	427
Extra editie: Best practices tegen corona	401
COVID-19 - Custom Projects | Mobile Application | SEO !! -etc [REDACTED_DOMAIN]	367
COVID-19 EMERGENCY DELIVERY OF YOUR CONSIGNMENT BOX TODAY.	365
Productos Prevención Covid-19	359
Extra édition: Les bonnes pratiques contre le Covid-19	341
Insumos de Protección COVID-19	335
Long Lasting and Eco-Friendly Disinfectant to Fight Covid19...	307

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

toyotacarrr.com	14338
gmail.com	7511
sampark.gov.in	3826
timesofindia.com	1981
sendgrid.net	1881
coldaninvestmentcompany.online	1836
126.com	1291
trendingtopic.cl	1266
163.com	1184
expobase.be	957

Top-15 IPs Sending COVID Spam

187.174.101.179	4814
45.147.231.51	1833
81.95.112.26	957
119.122.91.11	762
142.24.50.246	739
167.99.191.76	706
95.211.208.50	687
51.77.33.44	677
103.225.52.14	657
95.211.208.25	532

Top-15 Countries Sending COVID Spam

JP	14624
US	8351
IN	7033
MX	4870
--	4715
CN	2961
FR	2474
CA	1901
NL	1647
DE	1261

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Diederik Health and Safety Consultant - Covid-19 Safety Plan Package Invoice	687
FW: APPOINTMENT FOR PERIODIC COVID-19 SWAB TESTS IN PREPARATION FOR SAFE AND CONTROLLED RESTART OF CONSTRUCTION SECTOR	2

Top-15 Subjects Containing doc/xlsx Files

CII Online Programme on 'Workplace Precautions during COVID 19' 9 July 2020 : 11.00 am to 1.00 pm	5
NdP 8 de cada 10 españoles han cambiado su percepción sobre los profesionales que trabajaron durante la crisis del COVID-19	3
Image : COVID-19 and Type 2 diabetes: regional experts shed light on the latest scientific updates and clinical practices in disease management for patient education	2
RE: Corona Virus Cancellation (OSA)	2
SICUR ESPECIAL COVID inaugura mañana su actividad	2
Gacetilla de prensa panel: "Desafíos de las negociaciones internacionales en tiempos de COVID 19"	2
[adherents] Covid - Evolution du chômage partiel au 1er octobre et dispositif longue durée au 1er juillet	2
An initiative bringing together India Inc and Entertainment to promote behavioural-change to fight COVID-19 - #EKDeshEkJung	2
IMSS Boletín 439.-Con lectura de libros pacientes COVID-19 se ayudan en su recuperación (FOTOS)	2
RV: Matriz de seguimiento 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: 111,124
Domains with Potential Mail Servers: 2,812
Email-Capable Domains and Hosts: 42,138
Live Hosts and Domains Not Parked: 53,097

Mobile Apps

Apps in Official Stores: 311

by Store

Apple	174
Google	129
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 815

by Store Type:

Hybrid	505
Secondary	274
Affiliate	36

Blacklisted Mobile Apps: 20

by Store Type:

Secondary	19
Official	1