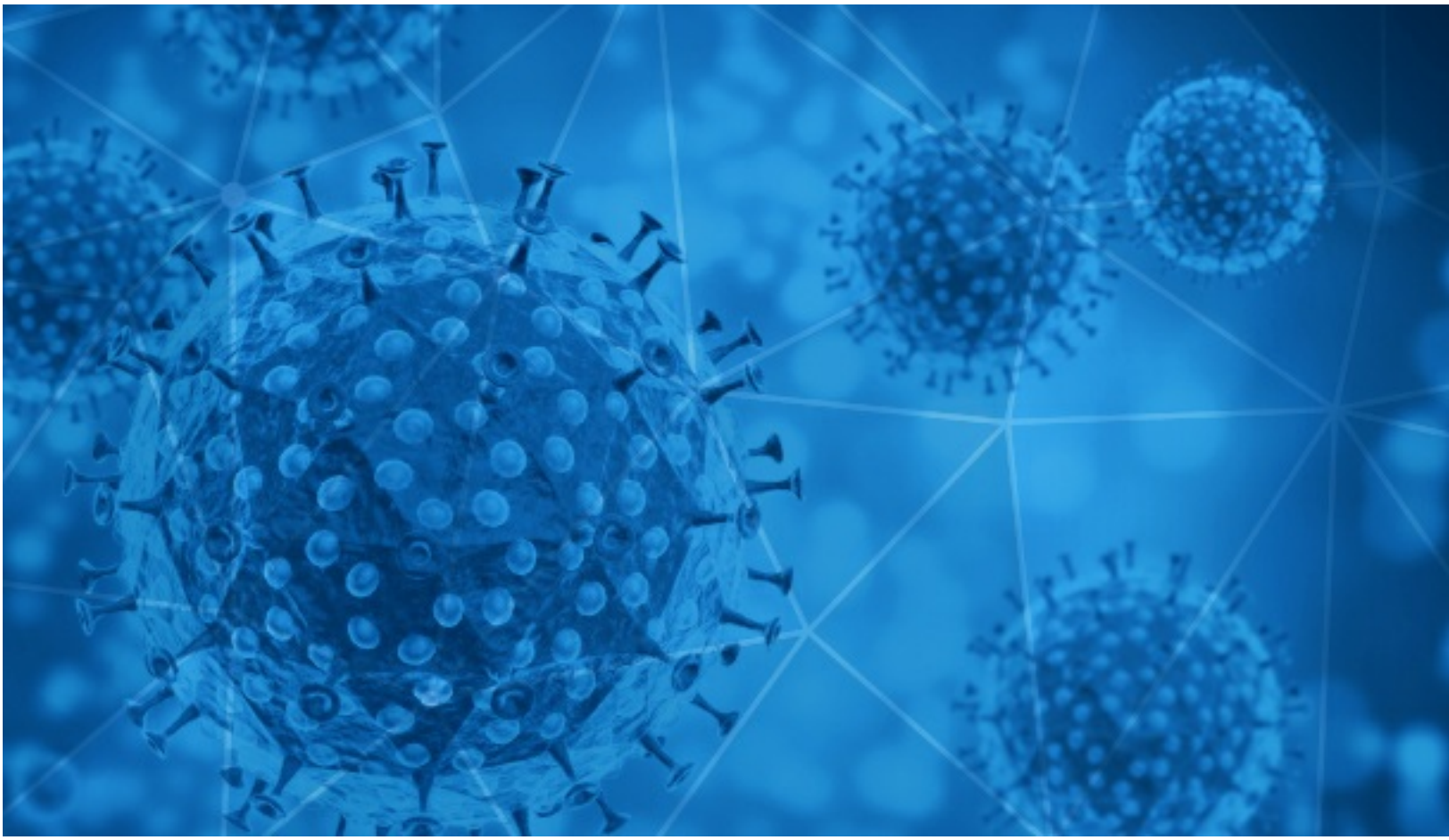
RiskIQ i3:

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

2020-08-28



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 2020-08-27 to 2020-08-28. During this period, RiskIQ analyzed 43,196 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,973 unique subject lines observed during the reporting period. The spam emails originated from 2,712 unique sending email domains and 3,925 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

United Nations Covid-19 Palliative/Financial Support/Congratulations.	4986
Safety Essential PPE For Covid19	4633
{COVID-19} □□□□□□□□□□□□□□□□□	3746
The Corona Letter: Why men may be more prone to Covid	2005
Soluciones para la prevencion del covid19	1862
Como volver a la actividad post coronavirus?	1818
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	1573
Cabinas para la prevencion del coronavirus	1377
covid-19 and children - how does it affect them?	816
TermoScanner Anti-Covid. Sconti fino al 50 % e pronta consegna. Non abbassiamo la guardia!!!	586
Reife Frauen zu Corona-Zeiten treffen	584
COVID-19 Products Nitrile-Vinyl-Latex Gloves and PPE with Best Price - Fast Shipping - Order NOW!	489
Incontri online in Italia (no corona)	489
Cuidate del COVID19 con nuestros productos	487
Evite contagios, no al Covid19, Accese, Asistencia biométricos	478
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	405
PRODUCTOS DE PROTECCION COVID 19	403
Desinfeccion Preventiva Covid19	374
Oferta Reingreso Laboral Covid19	373
Cabinas para la prevencion del coronavirus?	356
Desinfeccion covid19 mediante termoniebla	340
Totem Covid-19 Test Rápido, Mascarillas, Guantes e Insumos	326
Desinfectamos su ambiente de coronavirus	307
Re: keep away from Covid-19	295
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	245

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

countermail.com	6922
rediffmail.com	4988
medicproduction.com	4633
toyotacarrr.com	3746
gmail.com	2385
timesofindia.com	2008
126.com	1568
emailmarketingservices.us	816
livejob.info	618
data2web.de	584

Top-15 IPs Sending COVID Spam

80.118.240.244	4986
139.99.133.125	4632
190.247.226.214	3666
201.231.27.27	1874
181.46.136.168	1573
201.231.6.237	798
151.22.250.164	616
46.20.37.30	584
190.247.255.229	564
103.225.55.155	527

Top-15 Countries Sending COVID Spam

AR	8540
US	5445
FR	5272
AU	4694
JP	4032
IN	2452
DE	2387
CN	2372
--	1783
IT	1099

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

Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020	18
Webinar On "COVID-19 LIVE LIFE"	11
ΕΧΕΙΣ UVAIR-60? ΔΕΝ ΕΧΕΙΣ COVID 19!!!	7
NdP FAMMA pone en marcha inCOVID19 por la bajada en un 46, 52%!d(MISSING)el empleo para personas con discapacidad	3
CP- Cooperativas eléctricas realizan donaciones e iniciativas de apoyo a familias afectadas por Covid-19	2
First-of-its-kind co-browsing service during COVID Times - Media Release: Bajaj Allianz Life launches Smart Assist	2
REPORTE CASO POSITIVO COVID -19 ORIGEN COMUN	2
Siaran Pers XL Axiata_Di Tengah Pandemi Covid-19 dan Kompetisi Makin Ketat, XL Axiata Berhasil Jaga Pertumbuhan Kinerja_27Agustus2020	2
COVID 19 Line List	2
Thema der Woche: Covid-19 stellt die duale Berufsausbildung im Ausland vor neue Herausforderungen	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: 120,922
Domains with Potential Mail Servers: 2,944
Email-Capable Domains and Hosts: 45,198
Live Hosts and Domains Not Parked: 68,907

Mobile Apps

Apps in Official Stores: 408

by Store

Apple	211
Google	182
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,246

by Store Type:

Hybrid	722
Secondary	472
Affiliate	52

Blacklisted Mobile Apps: 26

by Store Type:

Secondary	23
Official	2
Hybrid	1