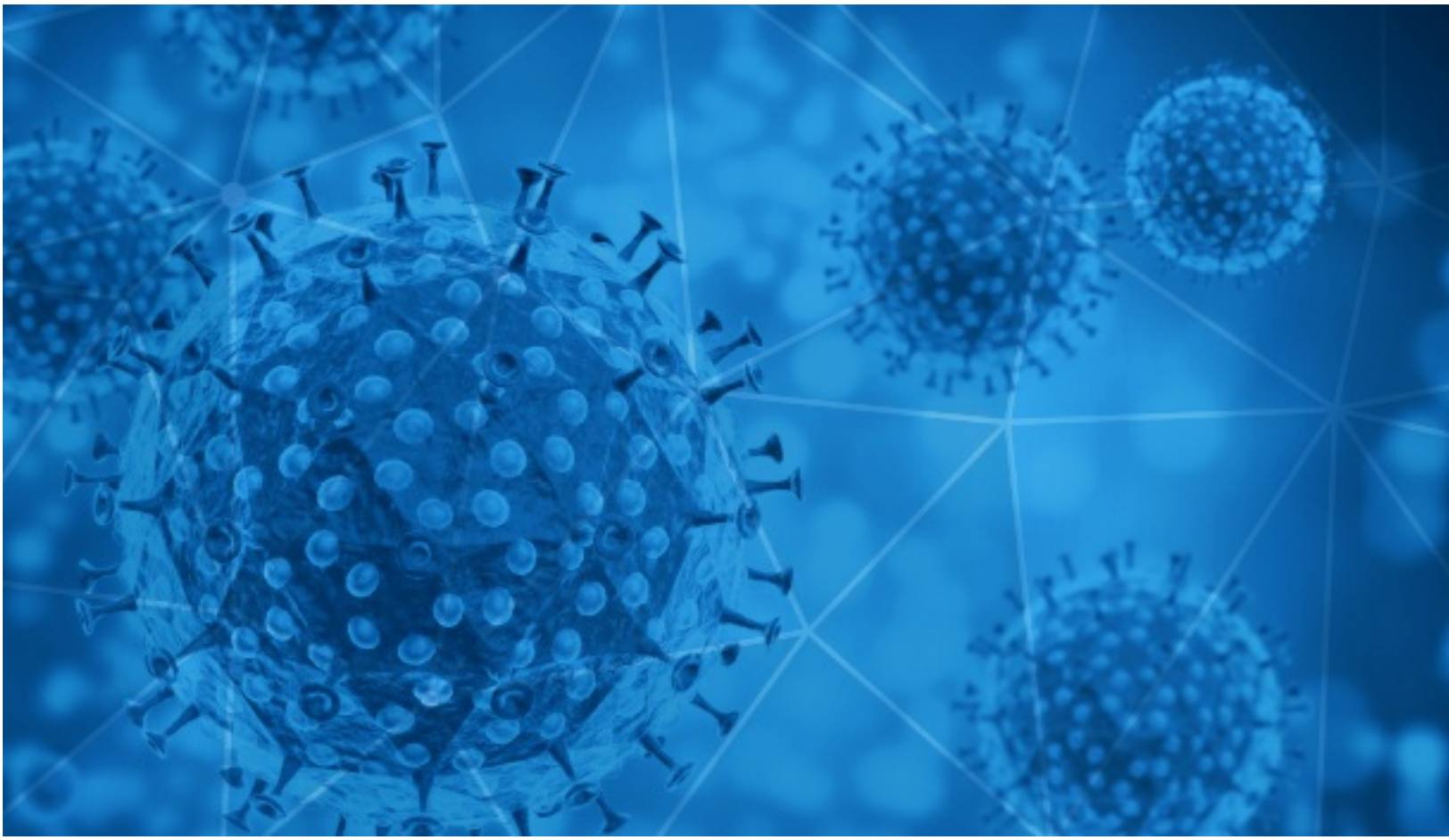
RiskIQ i3:

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

2020-08-06



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 2020-08-05 to 2020-08-06. During this period, RiskIQ analyzed 32,250 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,650 unique subject lines observed during the reporting period. The spam emails originated from 1,825 unique sending email domains and 4,331 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Something about our innate immune system	2759
Customer Information – Krispy Kreme Coronavirus Update	2279
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	1025
5 simple ways to grow during COVID-19	900
SBSA COVID-19 Financial Relief to receive your R15000 redacted@threatwave.com,	823
PyMEs contra el COVID19	819
Solución contra Covid-19: Medición de temperatura sin contacto	695
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	611
United Nations Covid-19 Palliative/Financial Support/Congratulations.	553
Precios Imbatibles/Productos Covid 19	508
Test Rápido Covid-19 Mascarillas Guantes e Insumos	455
Covid-19	445
Test Rápido Covid-19 Mascarillas e Insumos	423
Register Now | Importance of upskilling amid COVID -19	422
Surgical & Medical Mask for Coronaviruse / China Qualified Manufacturer	364
Mascarilla Desechable 3 Pliegues - Especial Covid-19	362
Let’s fight together to get through the COVID-19	317
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	312
Desinfeccion covid19 mediante termoniebla	310
Re: keep away from Covid-19	305
Desinfectamos su ambiente de coronavirus	297
Re: Defeat Coronavirus, non contact fever alarm device	293
Contactless infrared body temperature thermometer defeat Coronavirus	290
ATALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID -19	283
Mascarillas Protectoras AntiCOVID	271

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	2759
krispykreme.co.uk	2279
gmail.com	1959
126.com	1733
countermail.com	1692
163.com	1048
lulalend.co.za	900
standardbank.co.za	824
hotmail.com	800
keyable.net	583

Top-15 IPs Sending COVID Spam

192.174.92.52	2278
201.231.6.191	1176
181.46.136.168	1025
80.66.193.60	823
145.131.225.161	553
113.89.42.144	520
119.122.91.97	462
206.189.231.202	407
219.65.84.186	339
69.63.146.164	298

Top-15 Countries Sending COVID Spam

US	10834
CN	3843
IN	3355
AR	2964
DE	2267
FR	1014
--	925
CL	792
NL	788
BR	749

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

BHP – obowiązki pracodawcy i pracownika w dobie Covid 19	11
Re: Nirathanka (www.mhrspl.com) Covid-19 seal-down area	6
Comunicato stampa::Inps: Misure Covid-19. I dati al 3 agosto 2020	2
NP_Lilly inicia la fase 3 del ensayo clínico para la prevención de COVID-19 en colaboración con el NIAID	2
1001 BAY- A MAXIMUM OF 10 PEOPLE ARE ALLOWED AT ONE TIME IN THE BBQ PATIO AREA & COVID App	2
Precizări de presă privind modificarea condițiilor de intrare pe teritoriul Confederației Elvețiene și al Principatului Liechtenstein în contextul pandemiei de COVID-19	2
Melatonina, mientras llega la vacuna contra la COVID-19	2
Adult Social Care - Covid-19 update - 5 August 2020	1
Hoe verder na Corona?	1
FW: Protocolo Pruebas rápidas COVID -19 Cast&Crew Backdoor T2	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: 118,240
Domains with Potential Mail Servers: 2,869
Email-Capable Domains and Hosts: 44,343
Live Hosts and Domains Not Parked: 66,561

Mobile Apps

Apps in Official Stores: 371

by Store

Apple	195
Google	167
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 960

by Store Type:

Hybrid	618
Secondary	301
Affiliate	41

Blacklisted Mobile Apps: 23

by Store Type:

Secondary	20
Official	2
Hybrid	1