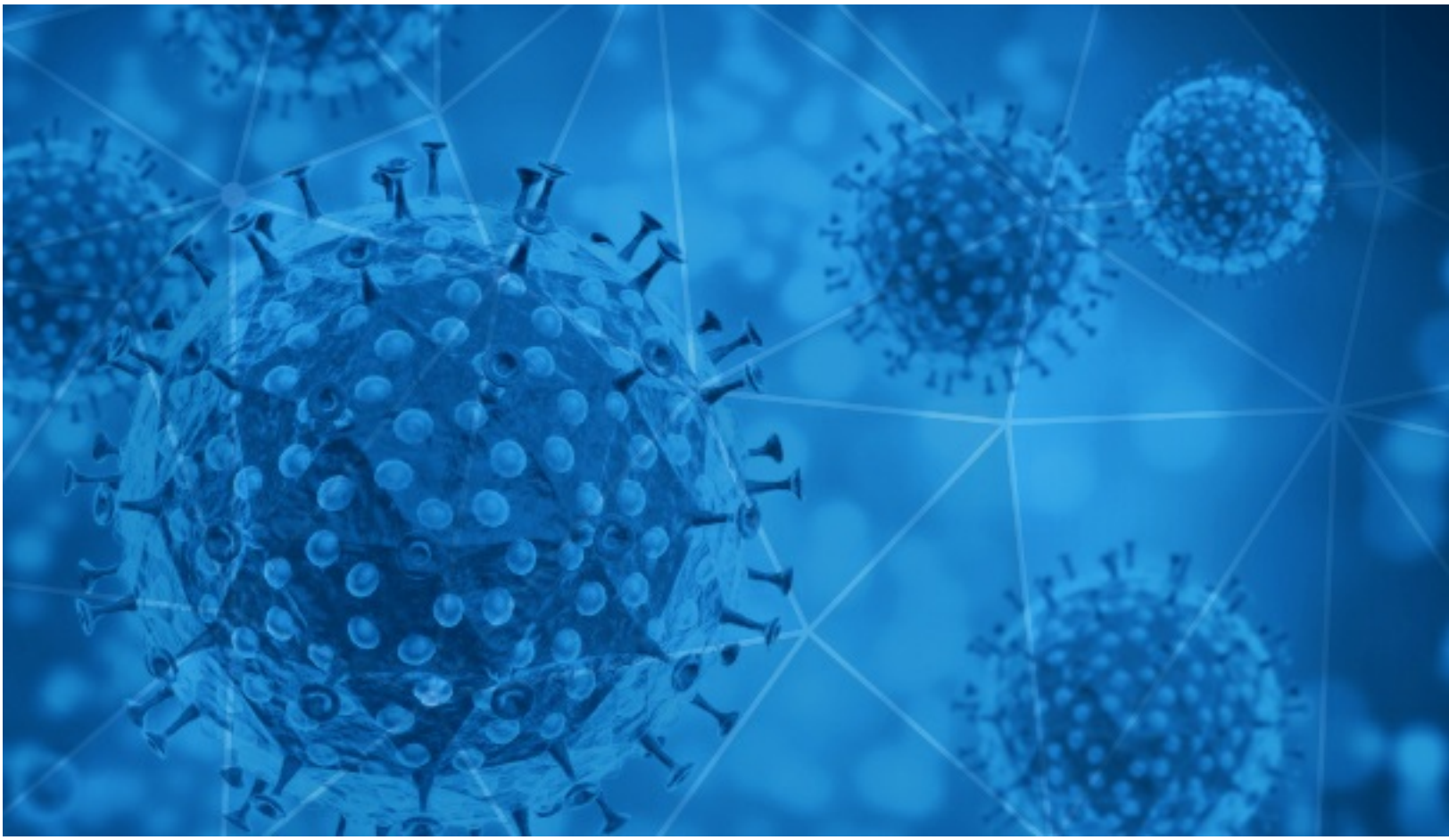
RiskIQ i3:

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

2020-08-19



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 2020-08-18 to 2020-08-19. During this period, RiskIQ analyzed 35,104 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,738 unique subject lines observed during the reporting period. The spam emails originated from 1,881 unique sending email domains and 3,899 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

COVID-19 : Protectores Faciales	3918
The Corona Letter: Shrinking economy, lockdowns are about lives too	1939
IMFCOVID19)	1100
QUIERES LO MEJOR EN BIOSEGURIDAD PARA PROTEGERTE DEL COVID 19.	802
Cuidate del COVID19 con nuestros productos	749
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	571
Desinfeccion covid19 mediante termoniebla	568
Desinfectamos su ambiente de coronavirus	557
Incontri online in Italia (no corona)	546
Desinfeccion Preventiva Covid19	537
Precios Imbatibles / Productos COVID 19	533
Cabinas para la prevencion del coronavirus?	524
Como volver a la actividad post coronavirus?	524
Soluciones para la prevencion del covid19	510
Covid-19: Quality IT Projects | SEO (Results Guaranteed) [REDACTED_DOMAIN]	442
Seminario Taller Fiscalización de La Dirección del Trabajo en Covid 19	432
PRODUCTOS DE PROTECCION COVID 19	428
Artículos Protección COVID-19	425
Re: keep away from Covid-19	402
Fwd:Credito Covid-19 Aprobado.	402
Re: Defeat Coronavirus, non contact fever alarm device	394
Covid-19 Face Mask	392
IFRS Update Actualización IFRS e Impactos por Covid-19	390
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	390
Protección Covid-19	389

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

trendingtopic.cl	3931
gmail.com	3715
countermail.com	3220
timesofindia.com	1939
126.com	1359
focazen.com	802
keyable.net	778
hypedsec.com.ar	749
hotmail.com	573
galanteo.com	546

Top-15 IPs Sending COVID Spam

51.77.33.44	1388
51.77.33.43	1230
45.143.222.167	1100
201.231.83.57	764
201.231.58.244	763
51.38.159.218	703
5.199.131.7	546
201.231.5.61	533
51.38.157.47	453
157.119.122.39	451

Top-15 Countries Sending COVID Spam

US	7811
FR	4787
AR	4267
IN	3793
CN	3476
DE	1857
--	1436
CA	758
CL	737
BE	544

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

CUMPLIMIENTO DE PROTOCOLOS DE BIOSEGURIDAD PARA MANEJO DE PANDEMIA CORONAVIRUS - COVID19	8
Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020	4
Press Release: Europeâs Largest Initiative Launches to Accelerate Therapy Development for COVID-19 and Future Coronavirus Threats - Order# 52268504	3
Cours d'aqua-gym manqués à cause du covid-19	2
ADJUNTO PLAN PARA LA VIGILANCIA, PREVENCIÓN Y CONTROL DE COVID-19 EN EL TRABAJO	2
GF MINING & ASTROTAIL: WEEKLY COVID 19 STATUS REPORT	2
Financial Accounting Impact of COVID-19- An In-depth Look at IFRS	2
Reminder - coronavirus webinar Thursday, Aug 20th - please test your computer ahead of time	2
Covid cases at Hoërskool Roodepoort	2
Beitrag Corona	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: 119,904
Domains with Potential Mail Servers: 2,917
Email-Capable Domains and Hosts: 44,448
Live Hosts and Domains Not Parked: 69,523

Mobile Apps

Apps in Official Stores: 393

by Store

Apple	205
Google	177
WindowsPhone	10
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,149

by Store Type:

Hybrid	698
Secondary	404
Affiliate	47

Blacklisted Mobile Apps: 26

by Store Type:

Secondary	23
Official	2
Hybrid	1