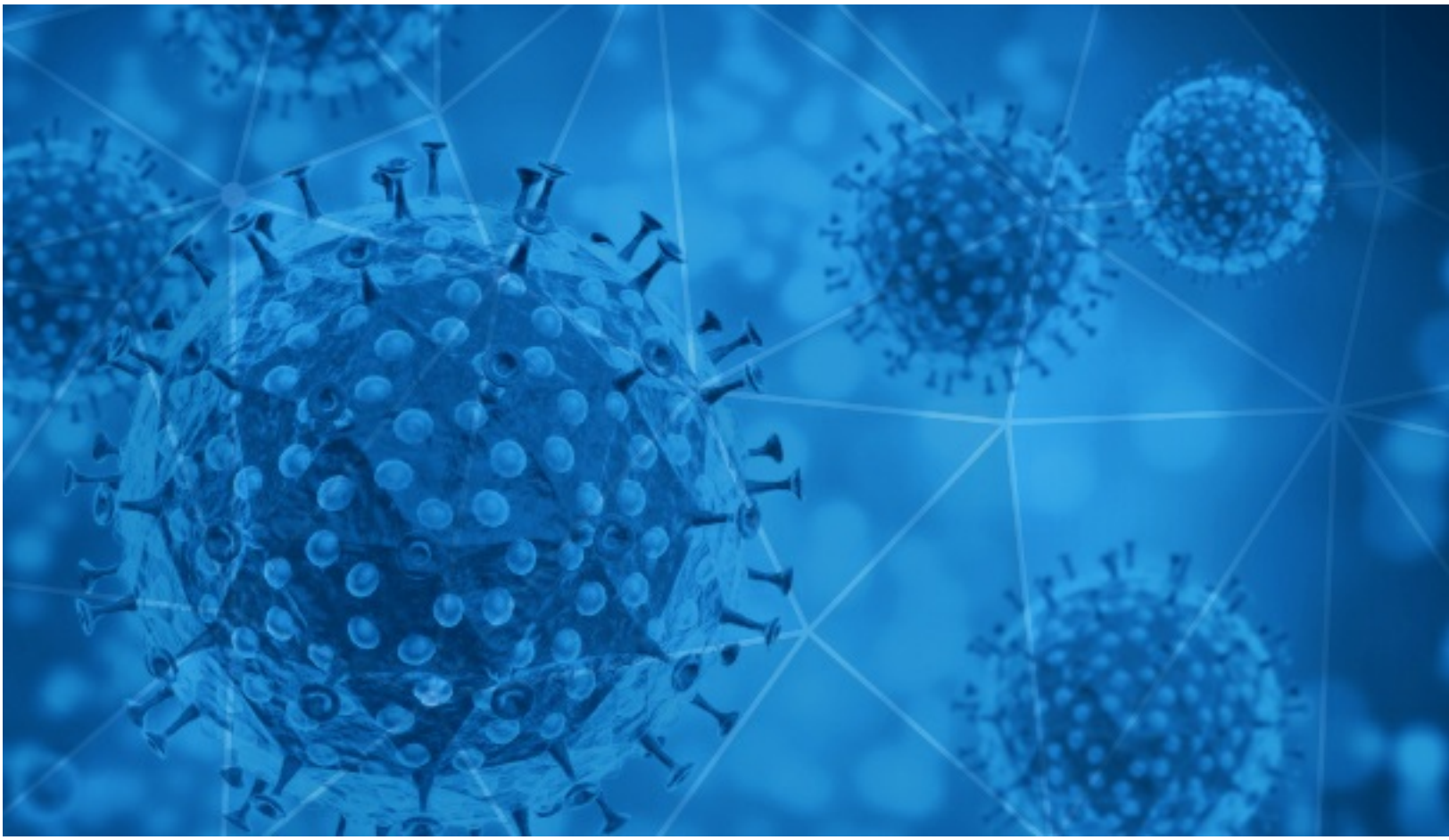
RISKIQ®

RiskIQ i3:

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

2020-08-20



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 2020-08-19 to 2020-08-20. During this period, RiskIQ analyzed 40,482 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,314 unique subject lines observed during the reporting period. The spam emails originated from 2,460 unique sending email domains and 4,088 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

COVID-19 And Your Credit Health	3161
Will COVID-19 Impact Your Credit Scores?	3055
Protect Scores During Coronavirus	3030
The Corona Letter: We need to know why we die	1905
Termómetro infrarrojo de pared especial COVID-19	1361
QUIERES LO MEJOR EN BIOSEGURIDAD PARA PROTEGERTE DEL COVID 19.	1173
Cuidate del COVID19 con nuestros productos	689
Desinfeccion covid19 mediante termoniebla	633
Desinfectamos su ambiente de coronavirus	579
Desinfeccion Preventiva Covid19	578
Japanese Band FLOW's Guitarist Take Contracts the Coronavirus - Sankaku News	572
Cabinas para la prevencion del coronavirus?	497
Form 941X COVID-19 Edition	493
Soluciones para la prevencion del covid19	489
Como volver a la actividad post coronavirus?	485
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	484
Llavero Anticovid metálico	464
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	461
Re: Personal & Business Funding (COVID-19 Relief).	436
Precios Imbatibles / Productos COVID 19	406
Covid-19 Face Mask	372
Re: Defeat Coronavirus, non contact fever alarm device	352
Contactless infrared body temperature thermometer defeat Coronavirus	345
Re:Covid 19 Loan Relief	325
Re: keep away from Covid-19	315

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

chaness.monster	3471
derpenording.casa	3264
countermail.com	3261
dickstonyx.cyou	2511
timesofindia.com	1905
gmail.com	1753
brandmed.cl	1413
126.com	1359
focazen.com	1175
keyable.net	697

Top-15 IPs Sending COVID Spam

170.130.213.22	3465
170.130.213.23	3263
170.130.213.4	2509
201.231.6.152	1256
201.231.83.196	1256
5.56.22.141	717
5.56.22.142	701
113.89.41.139	696
190.247.240.134	604
208.100.24.254	572

Top-15 Countries Sending COVID Spam

US	18413
AR	4465
CN	3516
IN	2685
DE	2077
FR	965
JP	866
GB	766
CL	739
BE	704

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

PHHS 8 18 2020 End of Day Summary for COVID 19	13
COVID-19 - JAK ZORGANIZOWAĆ PRACĘ W SZKOLE PRZEDSZKOLU W CZASIE PANDEMII 190zł./os - 25 VIII 2020 r	9
PHHS 8 19 2020 End of Day COVID 19 Response Report	7
NOTA DE PRENSA - LEGADO INSTALA DESDE ESTE JUEVES DOS ESTACIONES DE OXÍGENO PARA PACIENTES COVID - 19 EN AMAZONAS - ENLACES DE VIDEOS Y GALERÍA DE FOTOS	4
Press-release: "Rosoboronexport renders humanitarian aid to Venezuela to fight COVID-19"	2
NP Rastreadores coronavirus	2
[DIV20-Announce] Professional Development Webinar: Navigating the Job Market amidst COVID19	2
ADJUNTO, PLAN PARA LA VIGILANCIA, PREVENCIÓN Y CONTROL DE COVID-19 EN EL TRABAJO	2
Press Release_ UV-C devices, launched by NCR-based Company, to destroy Corona Virus within Seconds	2
Fw: COVID- 19 August 19, 2020	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: 119,995
Domains with Potential Mail Servers: 2,917
Email-Capable Domains and Hosts: 44,543
Live Hosts and Domains Not Parked: 68,652

Mobile Apps

Apps in Official Stores: 392

by Store

Apple	204
Google	177
WindowsPhone	10
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,170

by Store Type:

Hybrid	704
Secondary	417
Affiliate	49

Blacklisted Mobile Apps: 26

by Store Type:

Secondary	23
Official	2
Hybrid	1