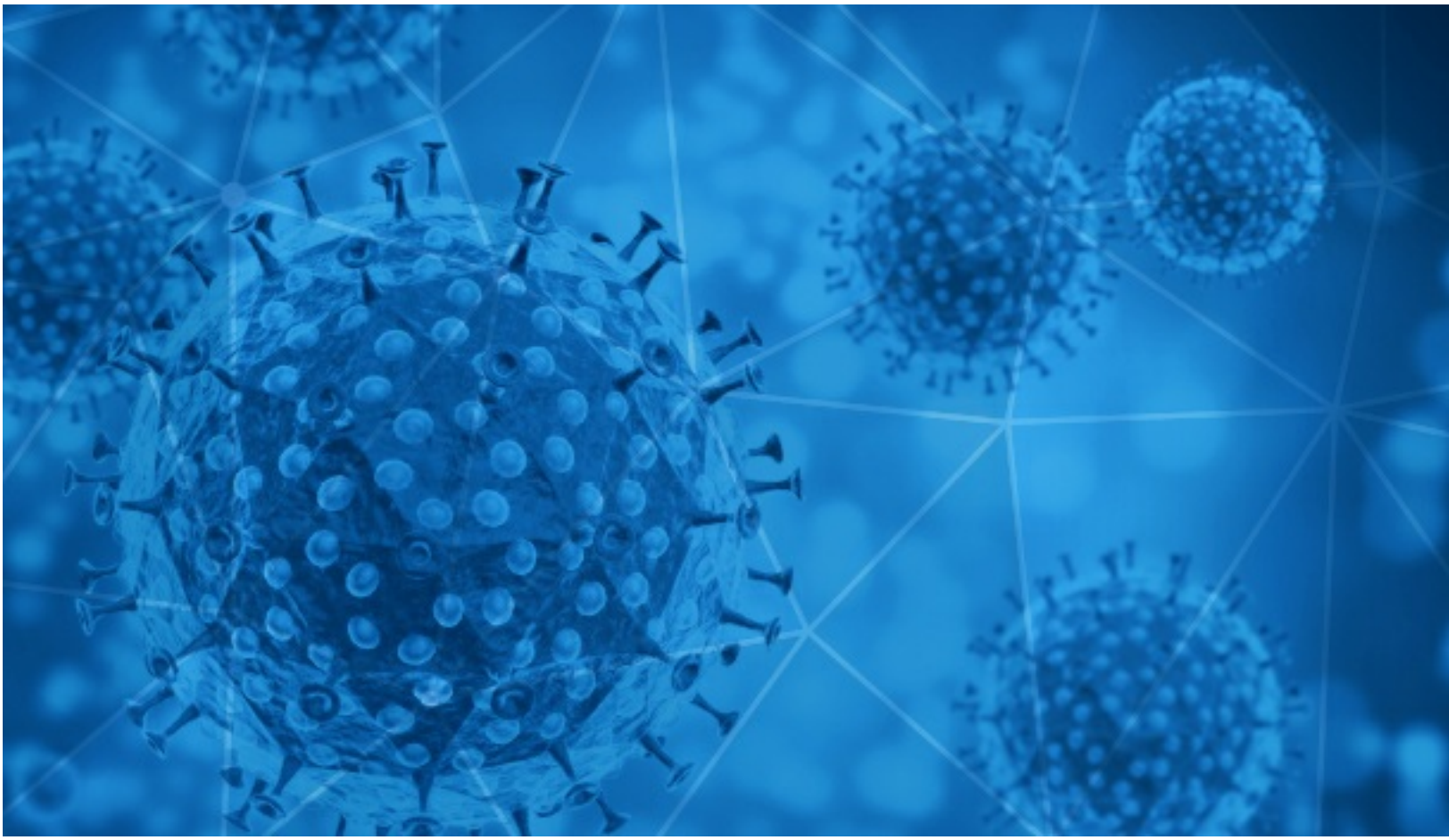
RiskIQ i3:

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

2020-08-21



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 2020-08-20 to 2020-08-21. During this period, RiskIQ analyzed 42,040 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,355 unique subject lines observed during the reporting period. The spam emails originated from 2,425 unique sending email domains and 3,814 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	5492
Re:Covid 19 Loan Relief	2577
Charter Air Service/Fast Air service/Mask /Covid-19 test/Medical equipment	2179
The Corona Letter: A rare Covid-19 complication in children	1967
Will COVID-19 Impact Your Credit Scores?	1689
Protect Scores During Coronavirus	1684
COVID-19 And Your Credit Health	1627
Ayúdanos a frenar que el COVID-19 llegue a los campos de refugiados. ¡Firma ahora!	791
QUIERES LO MEJOR EN BIOSEGURIDAD PARA PROTEGERTE DEL COVID 19.	752
Check out "BWL Ep16: Sean Price Tribute: Covid, RZA VS, Trump Stealing Mailboxs, Cardi B, DMX, Boosie Begging ?" on Wane Enterprises	741
Como volver a la actividad post coronavirus?	602
Soluciones para la prevencion del covid19	550
Cuidate del COVID19 con nuestros productos	534
Cabinas para la prevencion del coronavirus?	522
e-Conference on Accelerating New Business Model In Covid-19	457
Mega-funds find success despite COVID-19	434
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	420
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	410
Precios Imbatibles / Productos COVID 19	387
Desinfectamos su ambiente de coronavirus	373
SA's Leader in Covid 19 Protection!	366
Desinfeccion covid19 mediante termoniebla	354
Desinfeccion Preventiva Covid19	349
Re: keep away from Covid-19	346
Re: Defeat Coronavirus, non contact fever alarm device	341

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

web4youonline.xyz	5492
gmail.com	3865
countermail.com	2750
memodecruit.cyou	2618
memodecruit.icu	2382
oceanbridgecargo.com	2179
timesofindia.com	1967
126.com	1312
offerly.eu	791
focazen.com	756

Top-15 IPs Sending COVID Spam

167.99.227.36	5491
170.130.213.120	2617
211.241.209.104	2577
170.130.213.121	2381
203.86.233.195	2179
190.247.241.96	780
201.231.5.143	758
190.247.240.154	713
113.89.41.139	661
119.139.136.219	530

Top-15 Countries Sending COVID Spam

US	19031
AR	3857
IN	2894
CN	2719
KR	2666
HK	2264
DE	1086
PL	1041
FR	1036
CL	658

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	10
Covid-19 Humanitarian Food Relief Programme	7
COVID-19 - JAK ZORGANIZOWAĆ PRACĘ W PLACÓWCE OŚWIATOWEJ W CZASIE PANDEMII 190zł./os - 25 VIII 2020 r	5
Fwd: Coronatransporte Frankreich	2
"PRUEBA" de anticuerpos de Covid-19, para su personal, !Rápida y Segura" Sin hacer citas en laboratorios	2
COVID-19 Update August 20	2
considerar esse email - planilha monitoramento covid19	1
ENC: material do trabalho em casa da COVID-19 Educação Infantil	1
programmazione sopralluoghi SPSAL per vigilanza COVID - 24/28 agosto	1
Informasjonsskriv til søkere covid 19 11204016	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: 120,123
Domains with Potential Mail Servers: 2,923
Email-Capable Domains and Hosts: 44,799
Live Hosts and Domains Not Parked: 68,127

Mobile Apps

Apps in Official Stores: 394

by Store

Apple	206
Google	177
WindowsPhone	10
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,180

by Store Type:

Hybrid	706
Secondary	424
Affiliate	50

Blacklisted Mobile Apps: 26

by Store Type:

Secondary	23
Official	2
Hybrid	1