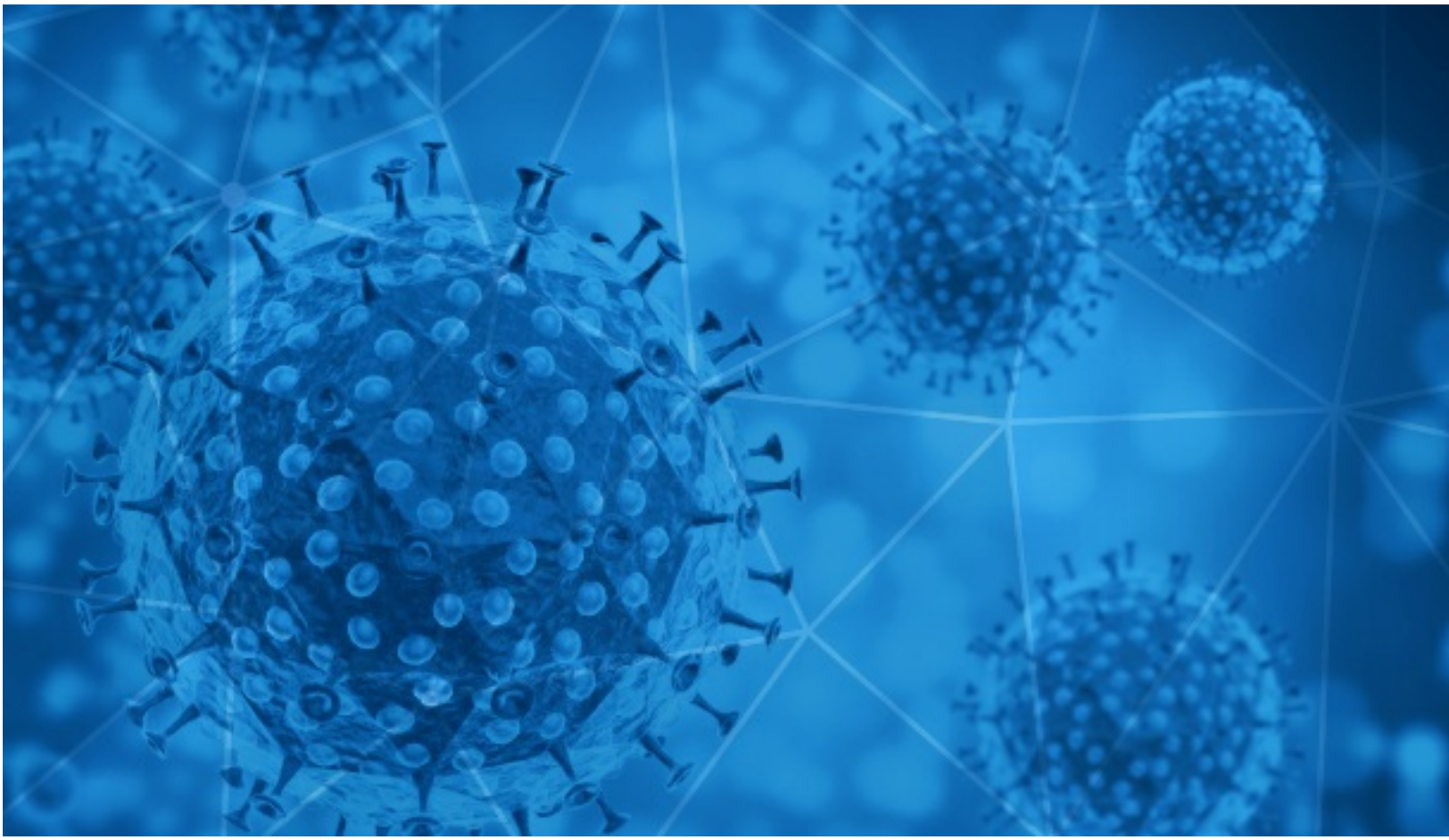
RISKIQ®

RiskIQ i3:

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

2021-04-12



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 2021-04-11 to 2021-04-12. During this period, RiskIQ analyzed 11,507 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 862 unique subject lines observed during the reporting period. The spam emails originated from 432 unique sending email domains and 960 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	4110
The Corona Letter: You can stop deep cleaning now?	1272
Your Opinion is Important! Take This Survey to Claim Your $50 Moderna COVID Vaccine Survey Reward	566
Shopper, You can qualify to get a $50 Moderna COVID Vaccine Survey gift card!"	553
30 Seconds Will Reward You With $50 in Exclusive Moderna COVID Vaccine Survey Rewards	518
You're Invited: To Redeem Your $50 Moderna COVID Vaccine Survey reward	504
Fwd: COVID Behaviour change campaign - regarding	279
Better than COVID Vaccine…	247
Infórmate sobre la población excluida del Plan Nacional de Vacunación contra COVID19	225
All you need to know about “Double Mutant” COVID-19	184
Toma de prueba Covid19 11 y 12 de abril	177
Retrogen is now performing diagnostic testing for COVID-19	137
redacted@threatwave.com : COVID 19 RELIEF FUND / LOAN (INVESTMENT)	125
Covid19 Relief Fund	102
□ Nově zlevněné testy na COVID-19 a až 40%! (MISSING)sleva na zdravotnické přístroje	92
Seguro COVID19 para la construccion	76
BENEFITS PAYMENT SUPPORT FOR COVID-19	72
Tweede prik van AstraZeneca vóór 5 mei? Dat kan, op eigen risico - Jongeman maakt fatale val uit raam bij politiecontrole lockdownfeestje in hotel - Coronavaccin zou ‘Trumpcine’ moeten heten (vindt Trump) - Dag wordt nacht in Barbados door…	71
Conferir "A desobediência a Gaia e a COVID-19, artigo de Eloy F. Casagrande Jr." em Espirit book	59
После решения мэра дому в Челябинской области задним числом начислили 5 миллионов долга за капремонт. Поздно спохватились? Новые штаммы COVID-19 в Россию завозят из Турции. Успеем ли остановить третью волну.	53
COVID-19 DONATION FOR YOU! GET BACK TO ME	42
(□□)□□□□19(COVID-19)□ □□ □ □□□□□□ □□ □□□□□ □□ □□□	41
Re: Personal, SME & Business Relief (COVID-19).	39
Payment of all outstanding Covid-19 palliatives	39
Re: COVID -19 NUTZENFONDS	38

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

giant-pw.com	4110
savagehut.us	2141
timesofindia.com	1275
saludtotal.com.co	402
bcrec.ac.in	278
gmail.com	265
immunboosts.co	247
faceonpro.com	184
loanme.com	143
retrogenmail.com	137

Top-15 IPs Sending COVID Spam

185.239.242.81	2141
200.31.17.85	402
101.79.49.106	247
206.214.77.98	247
103.225.55.239	213
103.225.53.66	212
192.99.34.104	184
103.225.52.211	183
103.225.52.92	168
103.225.55.218	159

Top-15 Countries Sending COVID Spam

JP	4118
MD	2141
US	1624
IN	1287
AR	484
KR	297
CA	222
--	170
CN	129
DE	122

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

ANC Weekly COVID-19 Reports	9
Document COVID-19 Self declaration form.docx has been completed	4
FW: MEDIA RELEASE: Samoa receives 24,000 doses of COVID-19 vaccines through the COVAX facility	2
INVENTARIO DE COVID-19 11/abril/2021	1
Fw: Marija potvrda alergija i covid	1
NOTA DE PRENSA - Huánuco: Más de 600 miembros del Ejército vacunados contra la COVID -19	1
Comunicato stampa del 11 aprile 2021 - Vaccini anti Covid-19. Alla Ugl prosegue il servizio di supporto per la prenotazione delle vaccinazioni per la fascia di età over 65 e soggetti fragili.	1
HERE ATTACHED WITH 10th APRIL 2021 COVID REPORT	1
Fwd: Olympian Maurice Smith losses mom to COVID-19	1
COVID 19 Natore(11.04.2021)	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: 155,522
Domains with Potential Mail Servers: 2,542
Email-Capable Domains and Hosts: 49,862
Live Hosts and Domains Not Parked: 43,200

Mobile Apps

Apps in Official Stores: 525

by Store

Apple	262
Google	246
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,290

by Store Type:

Hybrid	1174
Secondary	1048
Affiliate	68

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1