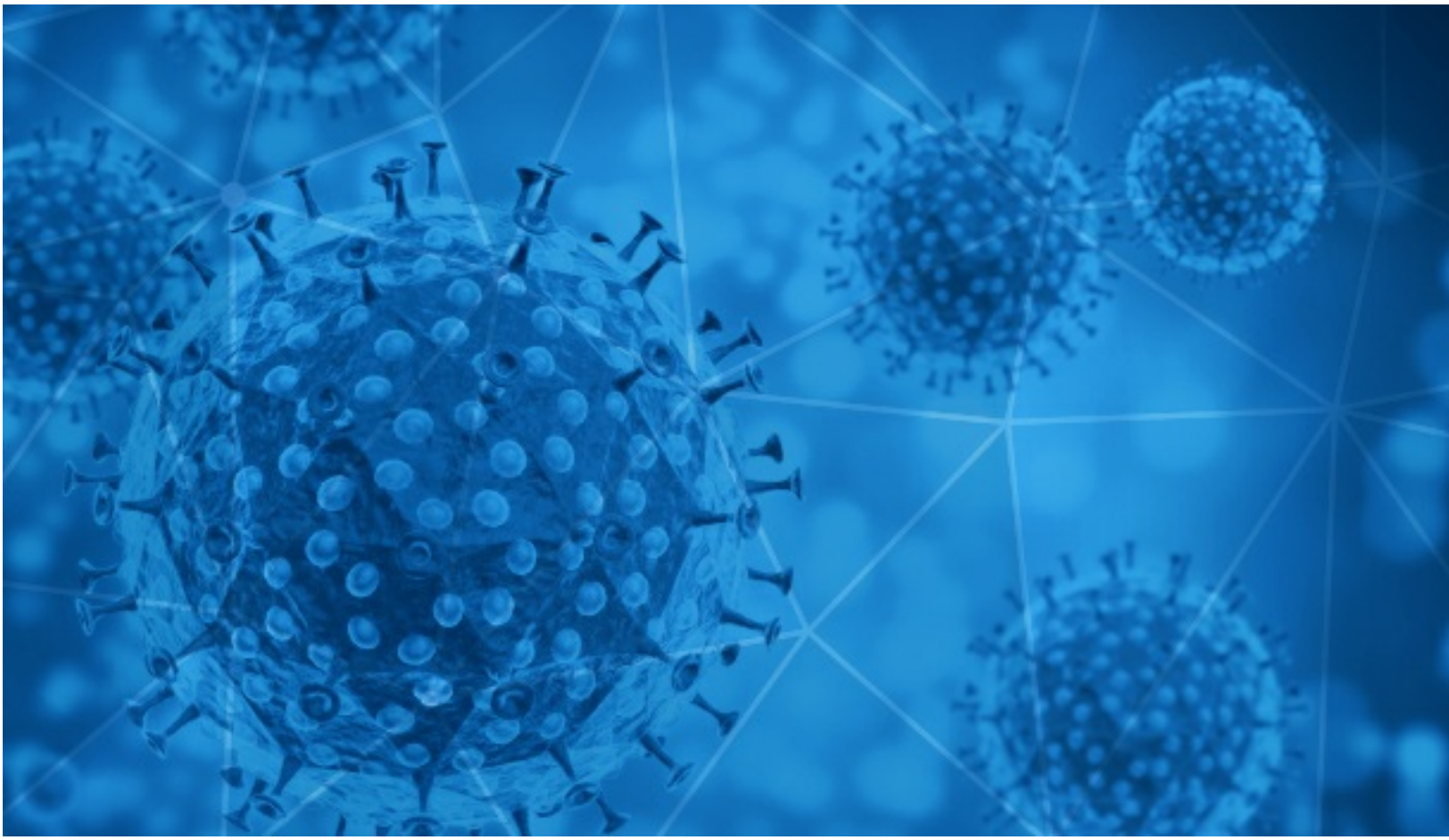
RiskIQ i3:

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

2021-02-15



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 2021-02-14 to 2021-02-15. During this period, RiskIQ analyzed 23,385 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,627 unique subject lines observed during the reporting period. The spam emails originated from 957 unique sending email domains and 2,016 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Vaccines for kids are coming but…	4782
[UK 000] Now with covid-19 you need this more than ever!	4479
{COVID-19} □□□□□□□□□□□□□□□□□	2892
UN Covid-19 Winning Notificationw	1471
[OL] Updated for Covid-19 times.	1300
TermoScanner e strumenti DPI Anti-Covid in pronta consegna con sconti oltre il 70% e prezzi a partire da Euro 39,00 + spedizione gratuita. Non Abbassiamo la guardia!!!	595
Better than COVID Vaccine…	559
Direct weten of u Corona hebt?	360
Covid-19 Relief Payment Approval.	318
COVID-19 RELIFE FUND NOTIFICATION.REF/ 88.28.108.25	291
This Mask Is Being Called "The Anti COVID19"- Shop Here For Incredible Rates And Discounted Shipping	270
Public Relation Facebook Covid-19 Lottery Department	262
Preventing COVID19 Starts With KN-95 Masks, Shop Here For Discounted Rates And Shipping Waived	225
COVID-19 RELIFE FUND NOTIFICATION.REF/MX 303583	219
Your Ultimate Protection against COVID-19. US FDA Registered	165
Re: covid-19 touch monitor	145
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	136
The 3 plants you need to throw in your shopping cart to fight coronavirus	121
Re: COVID 19 GIFT	112
✓ Odmor na Brijunima | Testiranje na COVID-19 | Jahanje 2 sata -58% Jastrebarsko | Medicinska ili sportska masaža -41% | Uklanjanje bradavice -83% Maksimir | UZV dojki -43% Centar | Čišćenje zubnog kamenca -78%	107
Beat The Market With AI: 10 Stocks to Buy This Week ★ Algorithmic Trading With I Know First Versus HFT ★ Low PE Stocks Beat S&P 500 4 Times Amid COVID-19 ★ The New Cryptocurrency Package ★ Apple To Offer Bitcoin on Wallet App ★	107
Re: 2021 COVID-19 RELIEF GRANT.	97
COVID-19 Notice: Stores now closed - Phone orders and Click & Collect will be available	81
World Covid-19 Support Program (WCSP).	63
Re: 2020/2021 COVID-19 EMPOWERMENT	57

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	4783
bizuk01.com	4479
giant-pw.com	2893
gmail.com	2621
1treebridge.com	1301
livejob.it	608
carbofixx.cyou	555
offerly.com.pl	360
ggnet.nl	270
proposalforward.club	270

Top-15 IPs Sending COVID Spam

65.175.68.191	4478
65.175.68.7	1301
103.225.54.123	1282
47.112.227.11	742
221.123.163.87	729
185.221.173.42	608
72.19.13.91	555
88.218.108.25	511
103.225.53.31	387
211.136.178.66	318

Top-15 Countries Sending COVID Spam

US	7701
IN	4811
JP	2946
CN	2271
--	1186
IT	823
ES	567
NL	425
PL	412
FR	314

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	34
UN Covid 19 Relief fund.	3
[medios.sevilla.csalud] Comunicado Coronavirus	2
SOPs for Library during Covid-19	2
15 February 2021 Comms - Compass Group NZ: Re-unite against COVID19	2
[Press Release] International Webinar by Asian and African Media Diagnosed COVID-19 and Social Change with the Focus of Peacebuilding	1
INVENTARIO DE COVID-19 14/febrero/2021	1
Бланк анкеты пациента, желающего пройти обследование на определение РНК вируса SARS-COV-2 или антител к COVID 19	1
COMUNICADO ARRIBO DE VACUNAS DE ASTRAZENECA CONTRA COVID	1
COVID 19 LEVEL 3 UPDATE LETTER	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: 143,663
Domains with Potential Mail Servers: 2,578
Email-Capable Domains and Hosts: 52,164
Live Hosts and Domains Not Parked: 44,865

Mobile Apps

Apps in Official Stores: 513

by Store

Apple	254
Google	242
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,090

by Store Type:

Hybrid	1068
Secondary	955
Affiliate	67

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1