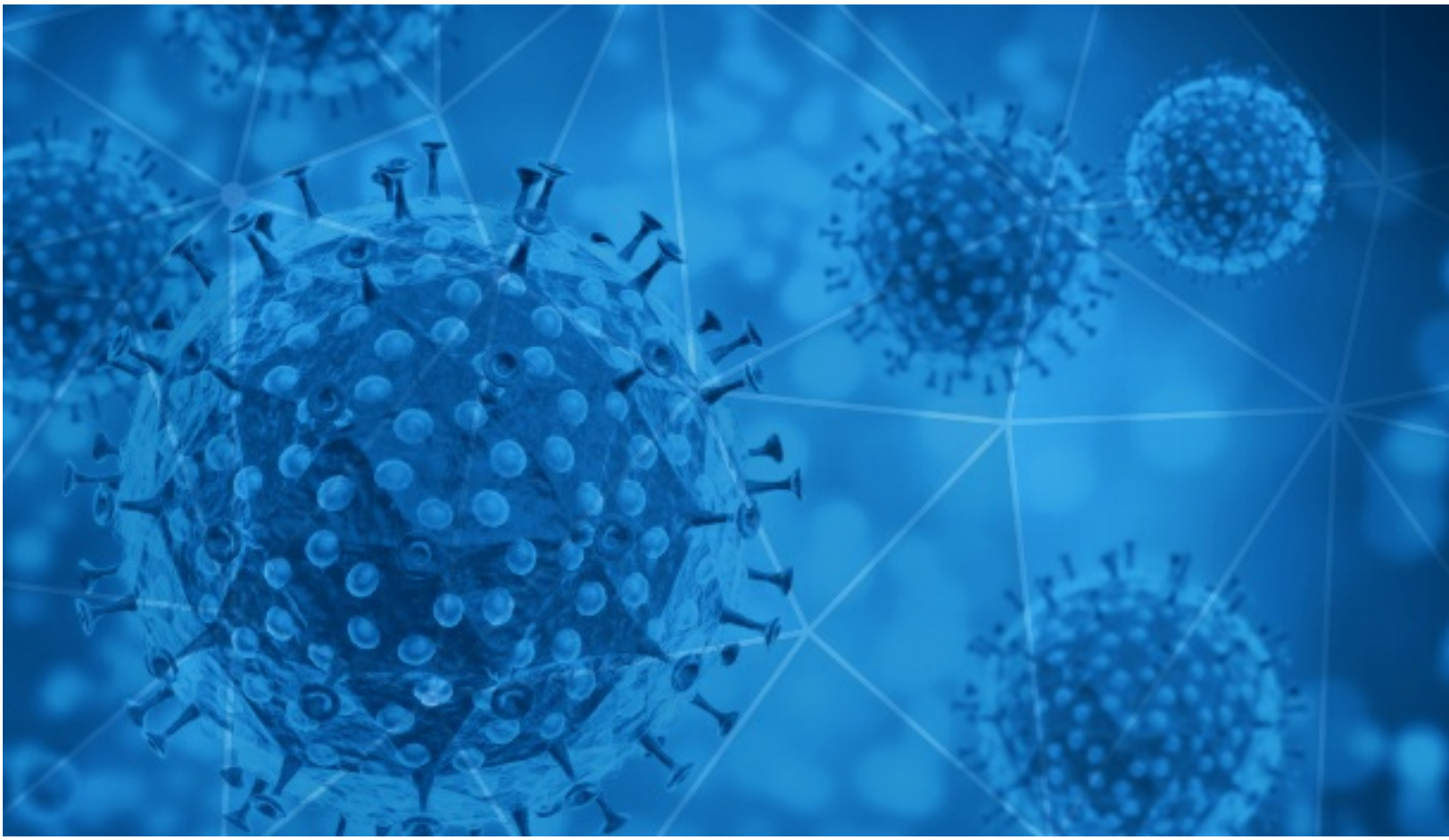
RISKIQ®

RiskIQ i3:

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

2021-04-08



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 2021-04-07 to 2021-04-08. During this period, RiskIQ analyzed 29,593 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,540 unique subject lines observed during the reporting period. The spam emails originated from 1,103 unique sending email domains and 2,250 unique SMTP IP Addresses. Analysts identified 6 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	5268
Sofort lieferbare Covid-Schnelltets. (3,90)	4439
All U.S. adults to be eligible for COVID vaccines by April 19, a groundbreaking transplant surgery, and more from Apple News	2940
Covid-Schnelltets keine Pflicht aber sinnvoll. (3,90)	2250
Covid-Schnelltets in Firmen werden zu wenig angeboten. (3,90)	2205
The Corona Letter: India's syringe heft	1556
Recuperacion en Tiempos de Covid19 - Subsidios Laborales	1144
Domowe testy COVID-19 już od 25 zł.	929
COVID19 LOAN / BOND INVESTMENT OFFER	598
$: Donation For Covid Relief	489
Recuperacion Efectiva de los Subsidios Laborales ante Essalud Post Covid19	390
DISPONIBILI PER L'IMPRESA I NUOVI TEST "COVID19" SALIVARI	306
You cant ignore Advertising& Marketing in corona.	273
Additional Coronavirus Information and Resources	258
REF: PANDEMIC "COVID19" GLOBAL MANDATORY AID	223
Re:Your Covid vaccine is approved for vacination	215
Seguro COVID19 para la construccion	170
Curso Gestión de los Riesgos Psicolaborales + Nuevo Módulo Covid 19	154
Retrogen is now performing diagnostic testing for COVID-19	153
COVID-19 DONATION FOR YOU! GET BACK TO ME	144
Re: COVID -19 BENEFIT FUNDS	105
redacted@threatwave.com : COVID 19 RELIEF FUND / LOAN (INVESTMENT)	104
BENEFITS PAYMENT SUPPORT FOR COVID-19	104
UN Covid-19 Winning Notification se	96
Action required – submit your March claims for the Coronavirus Job Retention Scheme	88

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmx.net	8896
giant-pw.com	5268
insideapple.apple.com	2941
timesofindia.com	1557
peruleadership.com	1145
0nline.media.pl	929
gmail.com	716
loanme.com	702
aiusm.com	489
mailingperu2020.com	390

Top-15 IPs Sending COVID Spam

45.89.127.226	4191
103.194.171.113	3636
157.245.42.150	702
64.32.22.161	541
188.72.187.72	506
202.143.97.88	489
165.227.58.99	390
103.225.55.70	380
103.225.55.124	349
94.152.193.45	291

Top-15 Countries Sending COVID Spam

US	8781
JP	5504
--	4340
NL	3880
IN	2207
PL	954
CN	578
AZ	506
DE	506
AR	274

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Media Invite: Latest research / findings at the Clinic regarding homeopathic prevention & management of COVID-19, Hypothyroidism and Chronic Kidney Disease	5
MEETING TODAY-OFFICIAL LINK: IPU-UN Women Dialogue on Gender-responsive recovery post COVID-19 (First meeting of the series - 7 April) //LIEN OFFICIEL : Dialogue sur la reprise post-COVID-19 respectueuse de l'égalité des sexes (1er meeting - 7avril)	1

Top-15 Subjects Containing doc/xlsx Files

BHP – obowiązki pracodawcy i pracownika w dobie covid-19	3
UN Covid 19 Relief fund.	2
comunicato stampa_ Da medico a paziente: l'esperienza del Dottor Francesco Tursi, responsabile del reparto di Pneumologia del Maggiore di Codogno e l'efficacia del trattamento della Sindrome Post Covid con L-Arginina e Vitamina C Liposomiale.	2
Please join us for the VCHIP VDH CHAMP COVID-19 update, on Friday, 4/9/21 (12:15-12:45)	2
Fwd: CVASU COVID-19 Testing Lab report on 07/04/21	2
Schedule for COVID-19 Vaccination @ Jindal Sanjeevani Hospital	1
RE: REPORTE COVID PEDREGAL	1
AdobCovid. FFP2 25db=90Ft, Pulzoxy készleten, KN95=67Ft, színes gyerek 3R. 21.04.07.	1
CUADRO COVID.19-COM. JESUS MARIA	1
Fwd: RHL COVID Center Admit Patient Detail 06-Apr-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: 154,654
Domains with Potential Mail Servers: 2,549
Email-Capable Domains and Hosts: 49,995
Live Hosts and Domains Not Parked: 44,079

Mobile Apps

Apps in Official Stores: 525

by Store

Apple	262
Google	246
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,284

by Store Type:

Hybrid	1170
Secondary	1047
Affiliate	67

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1