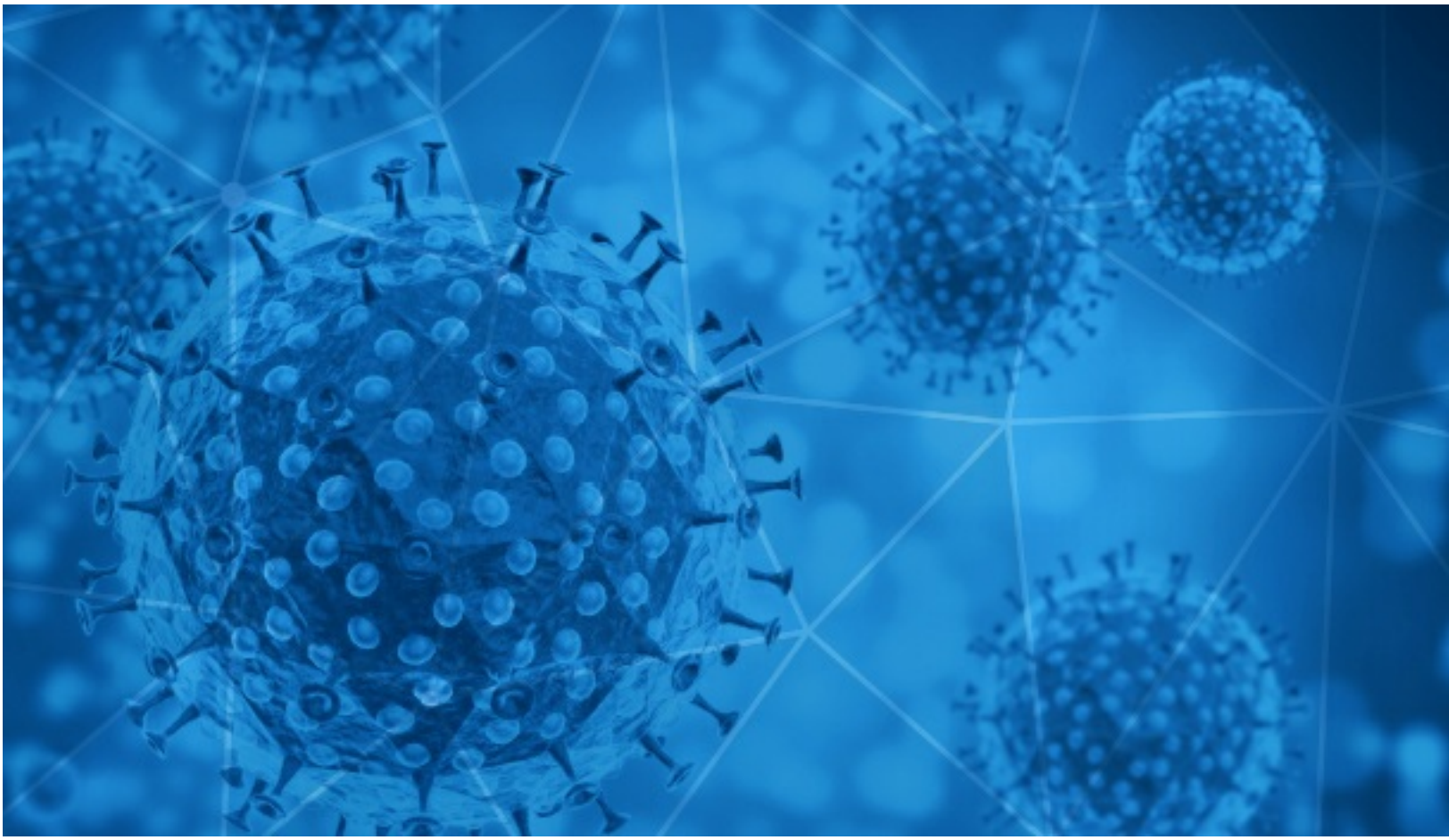
RiskIQ i3:

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

2021-04-07



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 2021-04-06 to 2021-04-07. During this period, RiskIQ analyzed 19,909 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,714 unique subject lines observed during the reporting period. The spam emails originated from 1,132 unique sending email domains and 1,956 unique SMTP IP Addresses. Analysts identified 12 emails which sent an executable file for Windows machines.

Top-25 Subjects

Coronaschnelltest jetzt bestellen. 5,90 bzw. 3,90 EUR (SARS-Cov-2-Test)	3815
Corona-Test 25-Päckchen sofort lieferbar	3249
25er Pakete Covid Schnelltest lieferbar (Realy-Saliva-Test)	2064
You cant ignore Advertising& Marketing in corona.	1984
The Corona Letter: Before India opens up vaccination for all…	1523
Recuperacion en Tiempos de Covid19 - Subsidios Laborales	635
Domowe testy COVID-19 już od 25 zł.	467
-$ Covid Relief Donation	234
Curso Gestión de los Riesgos Psicolaborales + Nuevo Módulo Covid 19	232
Descontaminación COVID: Oficinas, Domicilios, Bodegas, Talleres…	143
COVID19 LOAN / BOND INVESTMENT OFFER	138
Reducción de costos salariales: reestructurando la remuneración en el Contexto COVID	138
Don't delay getting checked for COVID IgG Antibody in your body at just Rs 449/-.	129
SEMANA SANTA Y PASCUA: AplicaciÃ³n Prueba COVID-19	128
Seguro COVID19 para la construccion	128
protective supplies for corona	124
Fight Corona with the help of experts	120
Covid19 Relief Fund	112
Re:Your Covid vaccine is approved for vacination	104
Re: Personal, SME & Business Relief (COVID-19).	89
Re: COVID -19 NUTZENFONDS	81
Coronavirus briefing: A new weapon in the UK's vaccine arsenal?	79
Conferir "DATA LIMITE (2019) de CHICO XAVIER e a PANDEMIA do CORONAVÍRUS: Existe alguma relação entre elas ?" em Espirit book	71
En vivo: Rehabilitación para pacientes post covid-19.	61
Apply For A Covid19 Unsecured Loan!! Low Interest Rate	60

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	9129
rkinfomedia.in	1984
timesofindia.com	1527
peruleadership.com	635
gmail.com	494
off-send.pl	268
tie.cl	232
24promo.pl	199
163.com	199
usiad.org	169

Top-15 IPs Sending COVID Spam

185.224.129.236	5102
78.142.61.109	2345
104.236.5.95	1984
188.166.14.210	1537
51.68.142.11	268
201.189.174.238	232
146.59.3.64	199
220.128.102.163	169
157.245.42.150	161
107.175.137.136	143

Top-15 Countries Sending COVID Spam

NL	6829
US	5469
BG	2348
IN	1654
FR	465
CN	328
DE	287
CL	236
GB	227
NO	199

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

DHL Global Forwarding Customer Advisory – COVID-19 ECRS Update 5	11

Top-15 Subjects Containing doc/xlsx Files

UN Covid 19 Relief fund.	3
Covid-19 : Activité partielle : prolongation des taux actuels de prise en charge et précisions sur les règles applicables pour la garde d'enfant.	2
[sections] TTU COVID-19 : accueil des enfants de personnels indispensables à la gestion de la crise sanitaire	1
DECLARACIÓN DE CONDICIONES DE SALUD FRENTE AL COVID-19	1
INCAPACIDADES COVID19, MARZO 04 2021	1
COVID 19 CASE REPORT | MAC | Sebastian | Family Member	1
RV: Evidencia de enrolamiento de personal en plaraforma Vacunas COVID	1
COVID REPORT	1
Δελτίο Τύπου Ηλεκτρονικές Υπηρεσίες του Δήμου Βέροιας στην Covid εποχή	1
Coronavirus Update	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: 154,650
Domains with Potential Mail Servers: 2,549
Email-Capable Domains and Hosts: 50,123
Live Hosts and Domains Not Parked: 44,289

Mobile Apps

Apps in Official Stores: 525

by Store

Apple	262
Google	246
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,279

by Store Type:

Hybrid	1165
Secondary	1047
Affiliate	67

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1