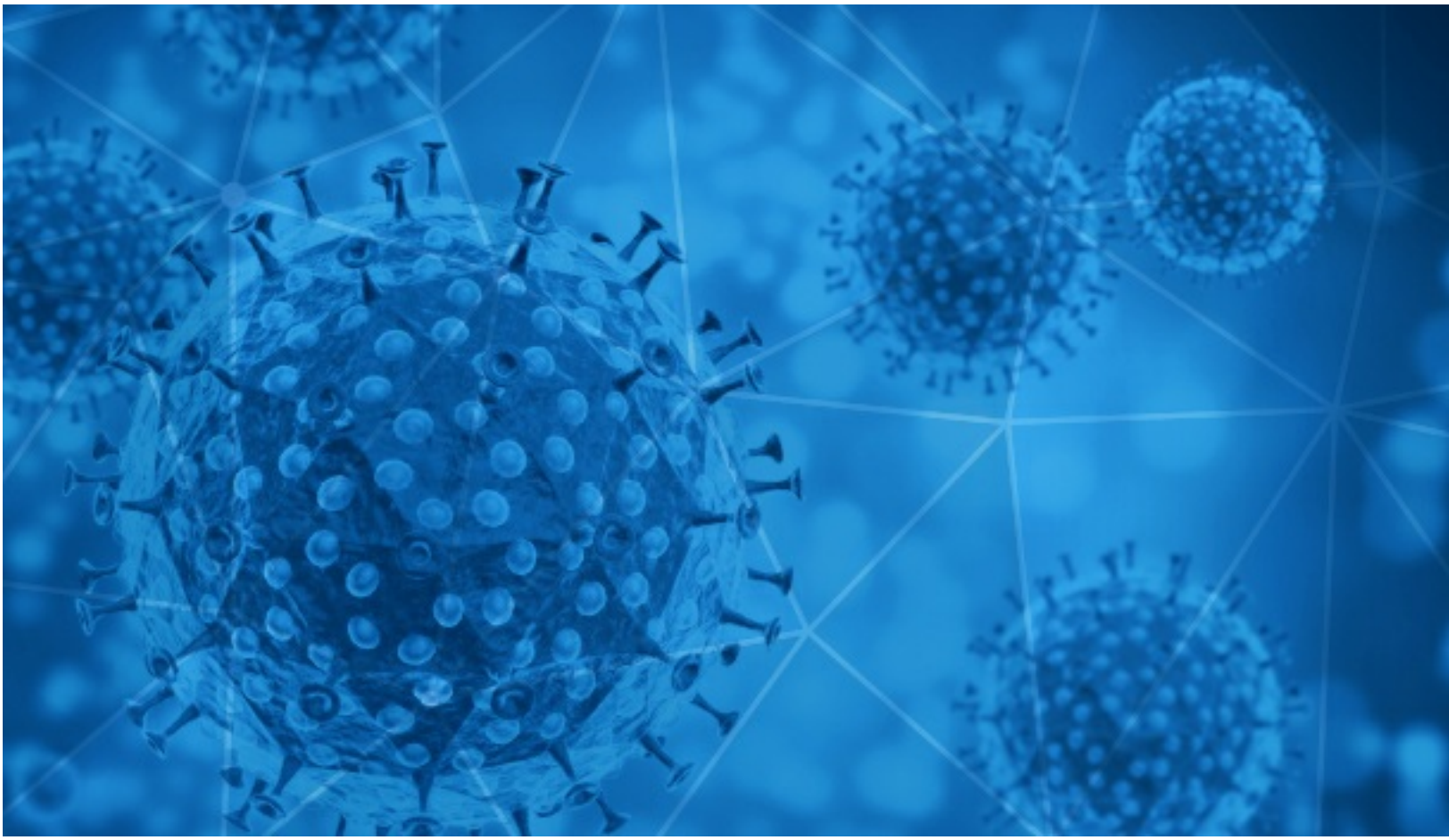
RiskIQ i3:

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

2021-04-02



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 2021-04-01 to 2021-04-02. During this period, RiskIQ analyzed 18,349 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,173 unique subject lines observed during the reporting period. The spam emails originated from 1,105 unique sending email domains and 2,253 unique SMTP IP Addresses. Analysts identified 6 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	4709
The Corona Letter: Good news for animals!	1595
UNITED NATIONS COVID-19 RESPONSE AND RECOVERY FUND	1277
COVID-19 BENEFIT CASH GRANT!!!	706
Recuperacion Efectiva de los Subsidios Laborales ante Essalud Post Covid19	556
UN Covid-19 Winning Notification me	488
Starmer: Covid passports un-British	456
Scale of long Covid revealed	391
COVID19 LOAN / BOND INVESTMENT OFFER	372
'Covid vaccine passports would be un-British'	307
Recuperacion Efectiva de los Subsidios Laborales ante Essalud Post Covid19 -8 y 9 de Abril	303
Additional Coronavirus Information and Resources	250
COVID19 LOAN/ INVESTMENT OFFER	227
No April Fool's Joke: We want 1 Million Americans Dry Practicing. We'll give YOU and every one of them $100. See our NEW Special Coronavirus Reality Check Video. Watch, learn and FORWARD…	227
Liquidación de Productos Covid -19	205
UN Covid-19 Winning Notification	162
COVID-19 BENEFIT!!!	161
Covid-19 Vaccination Awareness	133
protective supplies for corona	105
Formati per la trasformazione digitale post Covid	102
COVID-19 Relief Fund, Please Send all Replies to benduke111@hotmail.com	99
COVID-19: Employer support – live webinars	92
UN Covid-19 Winning Notification	92
Believe on us, we gives 100% accurate report of Covid Antibody test @just Rs 449/-	89
Covid19 Relief Fund	79

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	4709
gmail.com	2663
timesofindia.com	1599
email3.telegraph.co.uk	1209
msn.com	869
euroavisos.com	556
mladvocaciamjassociados.com.br	435
protonmail.ch	401
paisperu.com	303
163.com	245

Top-15 IPs Sending COVID Spam

83.12.212.149	1277
192.163.208.148	903
157.245.42.150	794
221.123.163.87	488
103.225.54.190	348
103.18.244.112	345
130.248.205.97	344
103.225.55.242	336
178.128.82.194	301
130.248.205.96	297

Top-15 Countries Sending COVID Spam

US	6538
JP	4716
IN	1706
PL	1315
CN	816
MY	493
GR	331
GB	258
FR	250
DE	218

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

REMINDER: INVITATION: Inter-parliamentary Dialogue on Gender-responsive recovery post COVID-19 (April 2021) // RAPPEL : Dialogue interparlementaire sur la reprise post-COVID-19 respectueuse de l'égalité des sexes (Avril 2021°	1

Top-15 Subjects Containing doc/xlsx Files

szczepienia p/covid-19	4
MaryFrances new admit negative for COVID	3
Constance Altemose new admit negative for COVID	3
ENTRADAS Y SALIDAS VACUNAS COVID_.xlsx	1
BACC Covid-19 Vaccination Providers	1
Covid-19 : mesures sanitaires au 1er avril 2021	1
Fwd: IESS RIOBAMBA - UCI COVID RODRIGUEZ ANDRADE NELSON	1
COVID & APS Death Case MONTHLY REPORT MARCH 2021	1
REMITO ACTUALIZACION DE REGISTRO DE PRUEBAS RAPIDAS COVID Y CASOS NUEVOS	1
Covid letter with signature	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: 154,291
Domains with Potential Mail Servers: 2,542
Email-Capable Domains and Hosts: 50,638
Live Hosts and Domains Not Parked: 45,555

Mobile Apps

Apps in Official Stores: 519

by Store

Apple	256
Google	246
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,265

by Store Type:

Hybrid	1158
Secondary	1040
Affiliate	67

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1