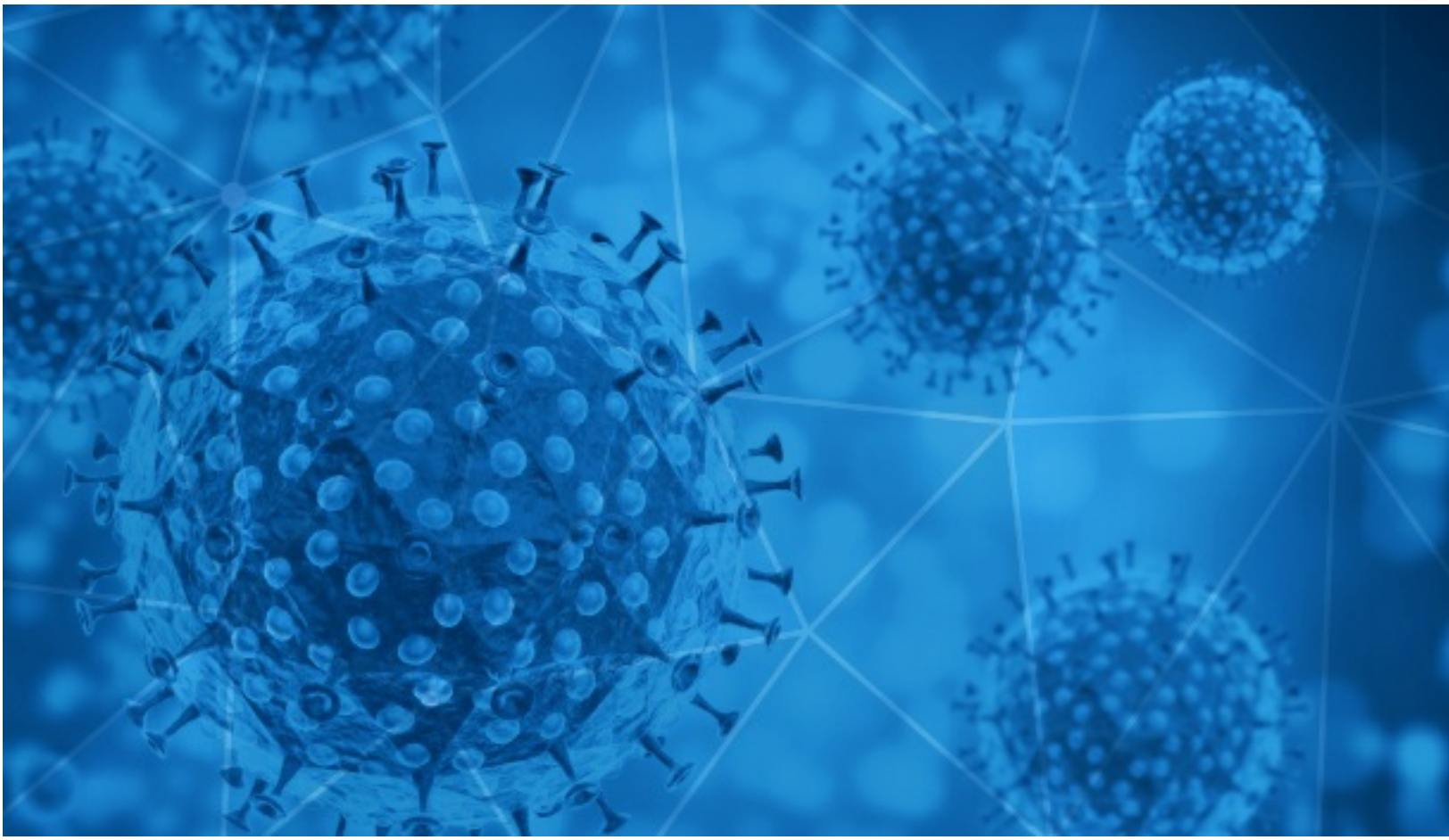
RiskIQ i3:

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

2021-04-14



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 2021-04-13 to 2021-04-14. During this period, RiskIQ analyzed 23,729 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,659 unique subject lines observed during the reporting period. The spam emails originated from 1,225 unique sending email domains and 2,288 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	5497
Corona Tests werden verpflichtend	3393
Corona Test werden eventuell Pflicht (BfArM-AT088-21)	2307
The Corona Letter: Drugs to beat back the Covid surge	1639
Limpieza Preventiva COVID19	688
CONGRATS! You Can Get $50 Pfizer COVID Vaccine Survey Rewards	461
Congrats! You've Been Selected For $50 Pfizer COVID Vaccine Survey Reward	454
Your Fifty Dollar Pfizer COVID Vaccine Survey Offer Is Waiting	424
Confirmed: Your Fifty Dollar Pfizer COVID Vaccine Survey Reward	416
Why Feds suspend Johnson & Johnson COVID vaccine + Police Say Daunte Wright Shooting was an Accident	411
Double mutant COVID19	387
COVID-19 Update: We are open and now offering Free Virtual Consultations	256
Mandatory Covid-19 vaccination/Link is below	252
Fino allï¿½ultimo paziente Covid-19	252
Infórmate sobre la población excluida del Plan Nacional de Vacunación contra COVID19	241
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!!!	231
COVID 19 - Deteccion de Brotes y Control	226
IMF COVID-19 FINANCIAL ASSISTANCE[2]	185
Re:Your Covid vaccine is approved confirm date and time	174
Polizza sanitaria con copertura COVID-19.	157
Covid19 Relief Fund	142
Donation of one million dollar to you regarding this Corona Virus	131
Liquidación de Productos Covid -19	115
COVID-19 DONATION FOR YOU! GET BACK TO ME	111
Test Antígeno Covid 19-Resultado en 30 minuto	98

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	5700
giant-pw.com	5498
electricmind.us	1755
timesofindia.com	1651
walla.co.il	712
gmail.com	486
caribbeanfever.com	411
faceonpro.com	394
saludtotal.com.co	295
ediscomspa.com	256

Top-15 IPs Sending COVID Spam

195.62.32.160	1755
149.3.170.90	1649
185.53.168.37	1018
5.253.176.41	975
206.189.13.88	791
104.129.11.178	786
201.231.27.51	559
103.225.53.104	551
77.73.68.109	474
192.99.34.104	394

Top-15 Countries Sending COVID Spam

JP	5513
US	4611
RU	2488
IN	1783
SA	1649
DE	1553
AR	1058
--	1004
FR	686
IT	677

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

Document COVID-19 Self declaration form.docx has been completed	20
UN Covid 19 Relief fund.	6
El CGE y ANENVAC explican las claves de la vacuna de Janssen y recuerdan a la población que todas son seguras y eficaces contra el COVID-19	3
Comunicado: 'SEFAC respalda el uso de las vacunas para la protección de la salud frente a la COVID-19'	2
BLANK covid neg	2
Confirmed COVID case; Caso confirmado de COVID-19	1
20210413 encuestas covid y mascarillas	1
Comparto 'JEFA PERLA COVID' con usted	1
Fwd: Protocolo Geral: Senado Federal, Câmara dos Deputados e Supremo Tribunal Federal a solicitação de protocolo urgente das Ilustres Lideranças e Bancadas para acordo de Créditos Extraordinários do Senado Federal para aquisição de vacinas a custo reduzido, doações e cestas básicas para os Brasileiros em isolamento social e existência de pedaladas fiscais durante Orçamento do Estado de Calamidade Pública, pandemia em exponencial de ascensão horizontal de alto risco e Brasileiros estão a 3 três meses sem receber o Auxílio Emergencial que é desumano e causa genocídio. Protocolo da Poder Judiciário Supremo Tribunal Federal Liminar para autorização do Poder Legislativo Senado Federal e Poder Executivo Ministério da Economia. Anexo Lockdown Nacional Social, Empresarial, Bairros, Mutirão de Limpeza Comunitária e Prevenção Covid. O Auxílio Emergencial de 150.00 cento e cinquenta reais é desumano e causa genocídio, porque 150.00 é 90% do salário.	1
COVID-`19 EN PUERTO RICO	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: 155,925
Domains with Potential Mail Servers: 2,537
Email-Capable Domains and Hosts: 49,676
Live Hosts and Domains Not Parked: 42,831

Mobile Apps

Apps in Official Stores: 525

by Store

Apple	262
Google	246
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,296

by Store Type:

Hybrid	1177
Secondary	1051
Affiliate	68

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1