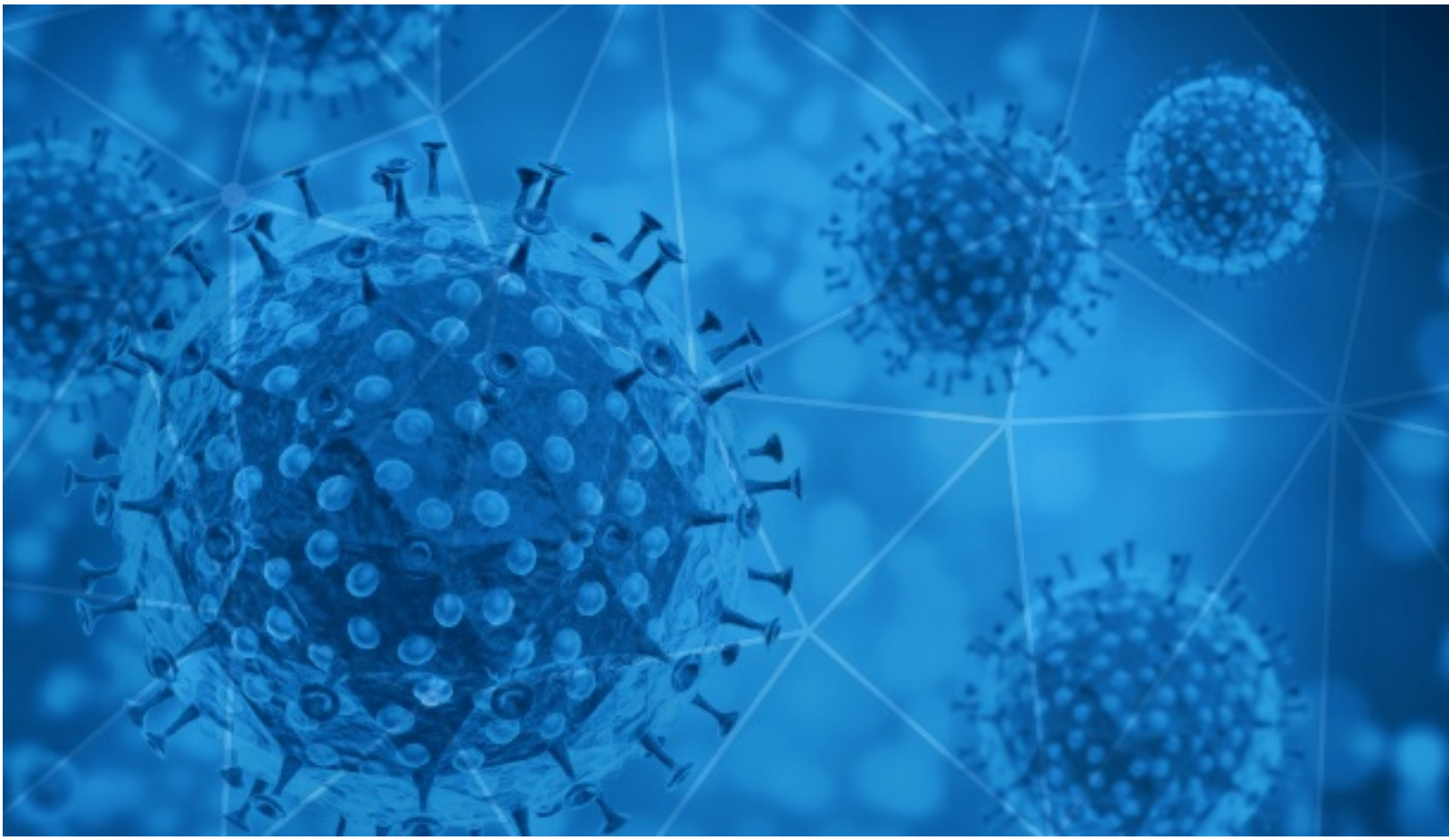
**RiskIQ i3:**

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

2021-04-06



**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 2021-04-05 to 2021-04-06. During this period, RiskIQ analyzed 19,765 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,227 unique subject lines observed during the reporting period. The spam emails originated from 831 unique sending email domains and 1,765 unique SMTP IP Addresses. Analysts identified 14 emails which sent an executable file for Windows machines.

## Top-25 Subjects

| | |
|---|---|
| **{COVID-19} □□□□□□□□□□□□□□□□□□** | 4353 |
| **U.S. sets record for daily COVID-vaccine doses, inside the world of hot-chili eaters, and more from Apple News** | 3277 |
| **The Corona Letter: Burden on babies & moms worsens** | 1600 |
| **Your Fifty Dollar Pfizer COVID Vaccine Survey Offer Is Waiting** | 1596 |
| **Claim Your Fifty Dollar Pfizer COVID Vaccine Survey Offer** | 1532 |
| **You cant ignore Advertising& Marketing in corona.** | 576 |
| **SEMANA SANTA Y PASCUA: AplicaciÃ³n Prueba COVID-19** | 516 |
| **Covid tests twice a week** | 451 |
| **Seguro COVID19 para la construccion** | 393 |
| **Descontaminación COVID: Oficinas, Domicilios, Bodegas, Talleres…** | 378 |
| **(covid19) compensation** | 335 |
| **UN Covid-19 Winning Notification lv** | 310 |
| **UN Covid-19 Winning Notification** | 211 |
| **Re: Mashalat Capital Relief (COVID-19).** | 142 |
| **Re:Your Covid vaccine is approved for vacination** | 132 |
| **UN Covid-19 Winning Notification obi** | 119 |
| **UN Covid-19 Winning Notification** | 101 |
| **Covid19 Relief Fund** | 83 |
| **Re: COVID -19 NUTZENFONDS** | 80 |
| **Fight Corona with the help of experts** | 74 |
| **CUIDADO DE ADULTOS MAYORES /// PROTOCOLO ANTE EL COVID19** | 72 |
| **Book your COVID-19 RT-PCR test from SpiceHealth for as low as ₹299!** | 68 |
| **Get tested! Book your COVID-19 RT-PCR test on SpiceHealth starting at just ₹299.** | 61 |
| **Re: Mashalat Capital Funding & Relief (COVID-19).** | 60 |
| **Ofertas Test Rapido Covid 19** | 59 |

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** | 4353 |
| **insideapple.apple.com** | 3278 |
| **cleanwork.guru** | 3128 |
| **timesofindia.com** | 1600 |
| **gmail.com** | 1382 |
| **rkinfomedia.in** | 576 |
| **soft-carpex.com** | 516 |
| **email3.telegraph.co.uk** | 451 |
| **walla.co.il** | 393 |
| **flowja.com** | 335 |

## Top-15 IPs Sending COVID Spam

| | |
|---|---|
| **104.140.80.102** | 3127 |
| **104.236.5.95** | 576 |
| **221.123.163.87** | 449 |
| **107.175.137.136** | 378 |
| **201.231.83.45** | 346 |
| **195.62.15.242** | 335 |
| **103.18.244.112** | 333 |
| **103.225.55.67** | 310 |
| **103.225.55.236** | 294 |
| **103.225.55.83** | 233 |

## Top-15 Countries Sending COVID Spam

| | |
|---|---|
| **US** | 10345 |
| **JP** | 4368 |
| **IN** | 1664 |
| **CN** | 605 |
| **AR** | 501 |
| **MY** | 337 |
| **UA** | 335 |
| **PH** | 203 |
| **--** | 150 |
| **BE** | 137 |

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** | 14 |

## Top-15 Subjects Containing doc/xlsx Files

| | |
|---|---|
| **MERCHANDISERS COVID ATTENDANCE MONITORING AS OF APRIL 5, 2021** | 1 |
| **situación covid** | 1 |
| **ATTESTATION COVID à remplir avant de venir au cabinet** | 1 |
| **RE: Caso Positivo Covid Jacqueline Flores y Lorena Rebolledo** | 1 |
| **Press Release \| India becoming a leading global hub for nutraceuticals post-Covid** | 1 |
| **Tableau des mesures pour faire face à l'épidémie de COVID-19** | 1 |
| **RE: Patricia Mata - Covid Test** | 1 |
| **DECLARACIÓN JURADA-COVID-19** | 1 |
| **Boletim Epidemiológico Covid-19 - 332 05 de Abril de 2021** | 1 |
| **PARTE COVID-19 DEL DIA 05ABRIL2021** | 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: 154,435
Domains with Potential Mail Servers: 2,544
Email-Capable Domains and Hosts: 50,208
Live Hosts and Domains Not Parked: 45,374

## Mobile Apps

### Apps in Official Stores: 525

by Store

| | |
|---|---|
| **Apple** | 262 |
| **Google** | 246 |
| **WindowsPhone** | 16 |
| **Amazon** | 1 |

### Apps in Secondary/Hybrid/Affiliate Stores: 2,274

by Store Type:

| | |
|---|---|
| **Hybrid** | 1164 |
| **Secondary** | 1043 |
| **Affiliate** | 67 |

### Blacklisted Mobile Apps: 30

by Store Type:

| | |
|---|---|
| **Secondary** | 27 |
| **Official** | 2 |
| **Hybrid** | 1 |