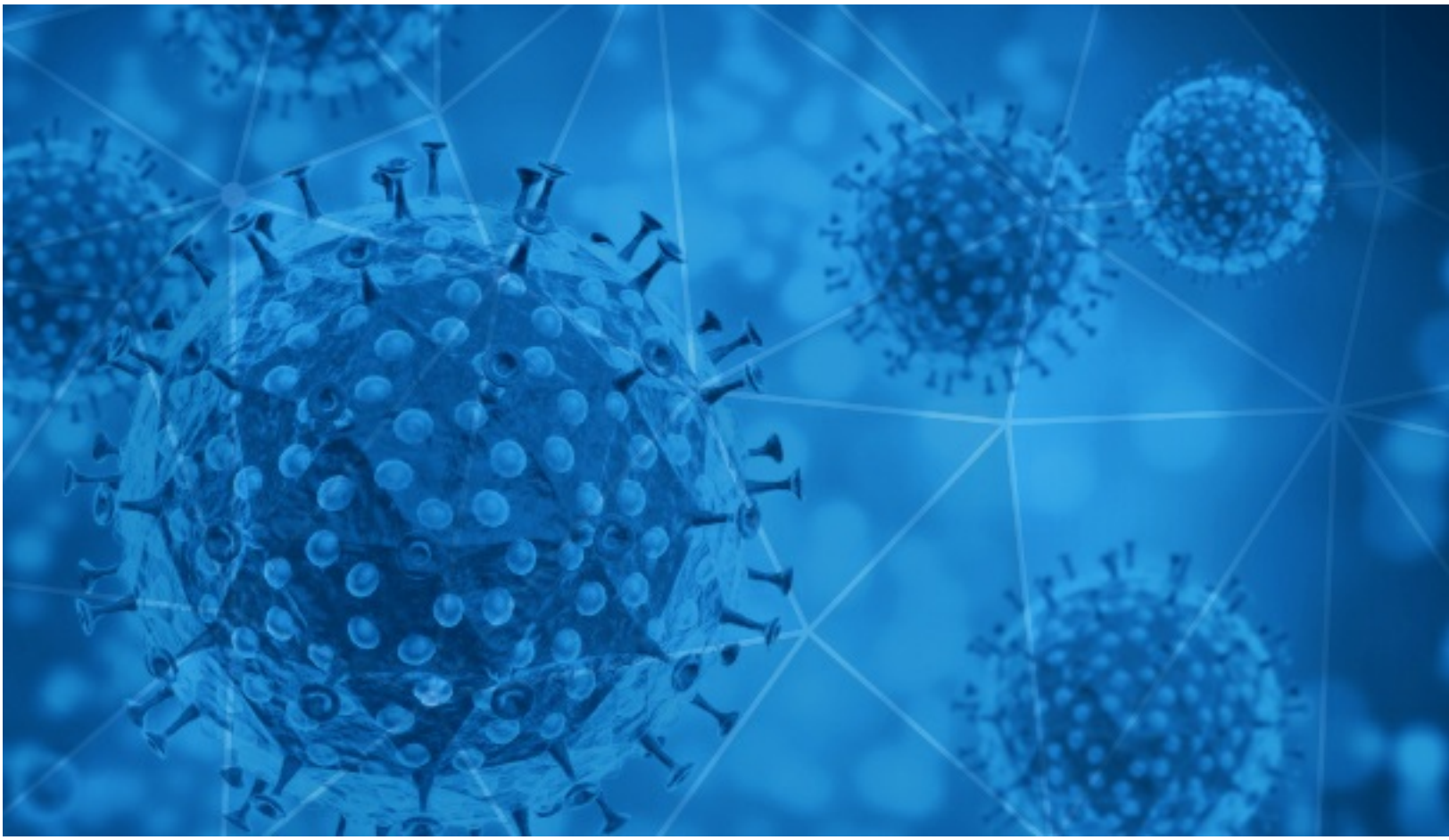
**RiskIQ i3:**

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

2021-01-27



**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 2021-01-26 to 2021-01-27. During this period, RiskIQ analyzed 44,537 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,708 unique subject lines observed during the reporting period. The spam emails originated from 2,290 unique sending email domains and 4,006 unique SMTP IP Addresses. Analysts identified 3 emails which sent an executable file for Windows machines.

## Top-25 Subjects

| | |
|---|---|
| **{COVID-19} □□□□□□□□□□□□□□□□□□** | 19298 |
| **The Corona Letter: Vaccines versus the variants** | 3439 |
| **Covid19- Fund Compensation Notice** | 1950 |
| **Public Relation Facebook Covid-19 Lottery Department** | 1823 |
| **YOU ARE COVID-19 REWARD BENEFICIARY.** | 1087 |
| **Snake oil salesman injecting patients with unproven COVID-19 vaccine for 1K a shot'+BOY, shot 6 DEAD** | 983 |
| **COVID-19 Pantallas Protectoras** | 587 |
| **COVID-19 Compensation Claim** | 558 |
| **COVID-19 What youâre not being told!** | 514 |
| **Your Ultimate Protection against COVID-19. US FDA Registered** | 458 |
| **Re: Personal, SME & Business Relief (COVID-19).** | 336 |
| **_Step_Closer_To_FDA_ Approval_ 20 People_Take COVID19_ PILL!** | 300 |
| **Productos Covid 19, entrega inmediata !!** | 273 |
| **Re: Digital signage solution for Covid-19** | 261 |
| **_Step_Closer_To_ FDA_ Approval_ 20_ people_ Take_ COVID19_PILL !** | 238 |
| **Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.** | 227 |
| **Equipamentos de Proteção Individual (EPI's COVID 19)** | 223 |
| **COVID-19 PANDEMIC COMPENSATION FUND** | 215 |
| **NCJ Daily - Two More COVID Deaths, 132 New Cases. Sign up for a Vaccination. Winter Storm Coming. Warm Line Offers Helping Hand.** | 165 |
| **Sanitizadores Anti Covid en aire y superficie** | 153 |
| **Marché de l'emploi : les seniors moins impactés par le Covid \| Tous les jobs en CDI \| Formez-vous au marketing avec Facebook** | 150 |
| **En vivo: Mitos y verdades de la nueva cepa y variantes de la COVID-19** | 146 |
| **Managing the Remote Workforce During Covid-19: Policies, Procedures, and Practices** | 137 |
| **Ofertas Test Rapido Covid 19** | 130 |
| **Toma de prueba COVID19** | 128 |

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

# COVID-19 Email Spam Statistics (Continued)

## Top-15 Domains Sending COVID Spam

| | |
|---|---|
| **epc-store.com** | 19301 |
| **yahoo.com** | 3821 |
| **timesofindia.com** | 3439 |
| **gmail.com** | 1775 |
| **caribbeanfever.com** | 983 |
| **herculist.com** | 571 |
| **aliyun.com** | 558 |
| **mailinator.cl** | 514 |
| **host2.herculist.com** | 457 |
| **163.com** | 403 |

## Top-15 IPs Sending COVID Spam

| | |
|---|---|
| **153.19.70.33** | 1949 |
| **59.152.229.114** | 1823 |
| **185.24.233.19** | 1015 |
| **103.225.54.136** | 642 |
| **216.87.190.231** | 606 |
| **103.225.54.223** | 589 |
| **45.133.203.109** | 557 |
| **103.225.53.8** | 493 |
| **216.87.190.229** | 421 |
| **103.225.52.177** | 420 |

## Top-15 Countries Sending COVID Spam

| | |
|---|---|
| **JP** | 19601 |
| **US** | 7384 |
| **IN** | 3794 |
| **PL** | 2187 |
| **HK** | 1906 |
| **FR** | 1187 |
| **CN** | 1108 |
| **IE** | 1080 |
| **--** | 656 |
| **DE** | 634 |

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

# COVID-19 Email Spam Statistics (Continued)

## Top Subjects Containing exe Files

| | |
|---|---|
| **Campagne de test Antgénique COVID** | 1 |

## Top-15 Subjects Containing doc/xlsx Files

| | |
|---|---|
| **WEB OnLine COVID 19 Organizzazione lavoro PA e Spa pubbliche: remote working, contenuti POLA, sicurezza, responsabilità 16/2/21** | 9 |
| **Las enfermeras piden a Carolina Darias que cuente de verdad con los profesionales para trazar estrategias contra el COVID-19** | 3 |
| **Come affrontare la PMA ai tempi del Covid-19? Il prof. La Marca illustra lo stato dell'arte ai colleghi europei di ESHRE** | 2 |
| **La Covid-19 dispara el uso de la firma electrónica** | 2 |
| **Covid 19 £500 Bonus Payment** | 2 |
| **Covid-19-20-21-22 etc., vaccins, mondkapjes, lockdowns, avondklok en wat ons verder nog te wachten staat..** | 1 |
| **DVE 005/2021 Estudio de caso ESAVI por Vacuna contra COVID-19** | 1 |
| **Free COVID-19 Policy - in case you missed it!** | 1 |
| **Fwd: Comunicato 3131/CAV - emergenza Coronavirus 2019 - aggiornamento numero Volontari impiegati** | 1 |
| **COVID 19 test results negative 211016945 Cameron Giorgianni Incident date 1/13/21 Emp ID 00170161** | 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: 140,778
Domains with Potential Mail Servers: 2,566
Email-Capable Domains and Hosts: 51,072
Live Hosts and Domains Not Parked: 43,888

## Mobile Apps

### Apps in Official Stores: 506

by Store

| | |
|---|---|
| **Apple** | 249 |
| **Google** | 240 |
| **WindowsPhone** | 16 |
| **Amazon** | 1 |

### Apps in Secondary/Hybrid/Affiliate Stores: 2,053

by Store Type:

| | |
|---|---|
| **Hybrid** | 1053 |
| **Secondary** | 933 |
| **Affiliate** | 67 |

### Blacklisted Mobile Apps: 28

by Store Type:

| | |
|---|---|
| **Secondary** | 25 |
| **Official** | 2 |
| **Hybrid** | 1 |