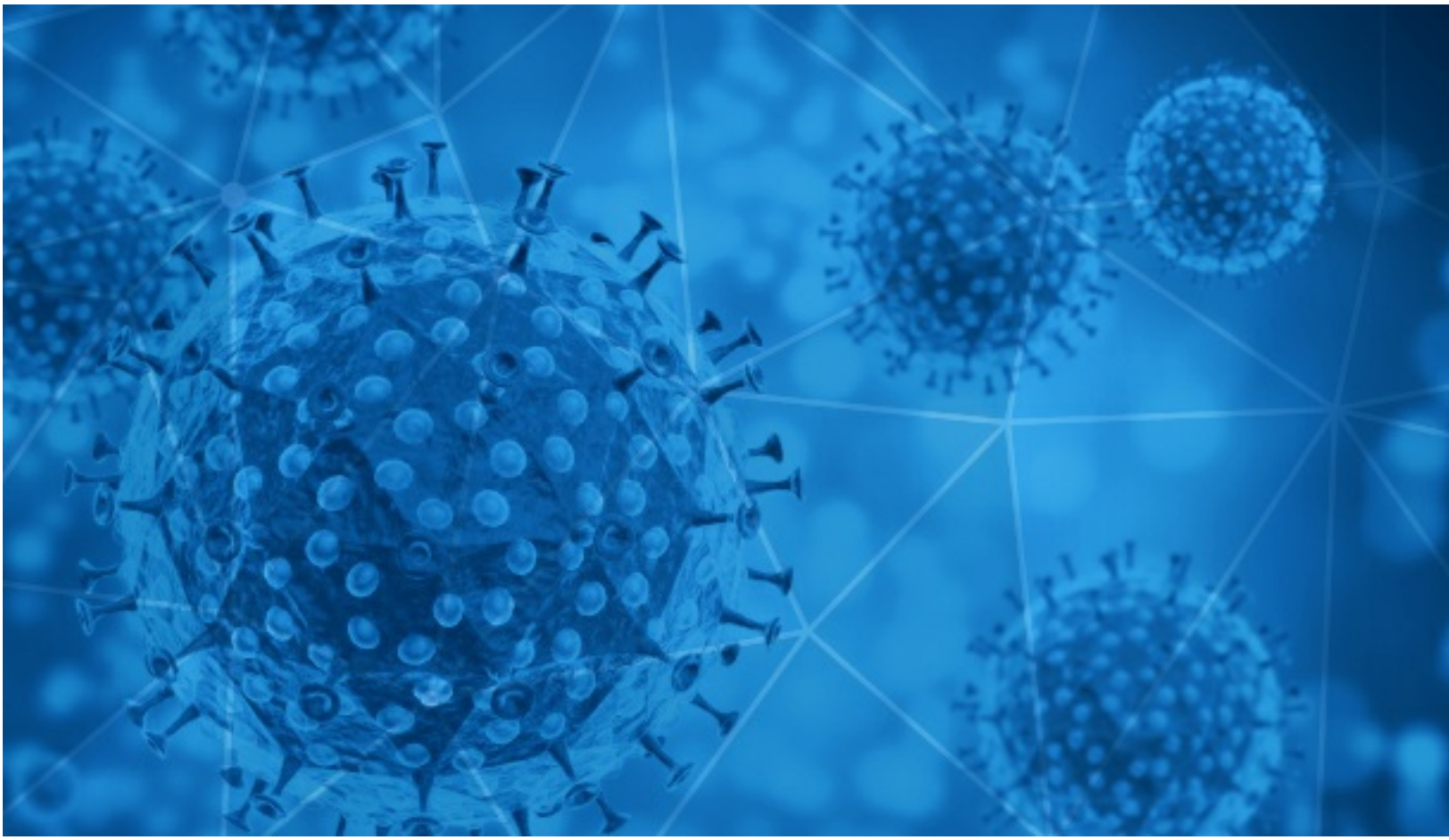
**RiskIQ i3:**

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

2020-11-19



**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 2020-11-18 to 2020-11-19. During this period, RiskIQ analyzed 40,702 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,352 unique subject lines observed during the reporting period. The spam emails originated from 2,923 unique sending email domains and 5,047 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

## Top-25 Subjects

| | |
|---|---|
| **{COVID-19} □□□□□□□□□□□□□□□□□** | 11572 |
| **COVID 19 LOCK DOWN COMPENSATION FUND** | 3236 |
| **The Corona Letter: Immunity may last years, even decades** | 2488 |
| **COVID 19 LOCK DOWN COMPENSATION FUND** | 1118 |
| **Coronavirus (Covid19) Bailout Fund** | 864 |
| **MASK-GLASSES la NOVITA’ per la protezione COVID-19 (VISO - OCCHI)** | 862 |
| **COVID-19 DONATION FOR YOU! GET BACK TO ME NOW** | 593 |
| **Fight COVID-19□ With $100 at Walmart Gift Card!** | 464 |
| **Re: Digital signage solution for Covid-19** | 419 |
| **Re:::Your Covid-19 Fund Benefit** | 412 |
| **Desinfección Covid-19 y aseo industrial para empresas. Santiago, Rancagua y Calama** | 395 |
| **Atencion covid Estudio Contable Legal e Impositivo para tu negocio** | 349 |
| **Re: Corona virus Protection Pills.Order confirmation** | 332 |
| **Reserve Your Seat . Thriving not just surviving post-COVID** | 331 |
| **COVID-19 SUPPORT DONATION** | 300 |
| **BATCH REF: NOV/COVID/2020/836278215** | 285 |
| **Wat het goede nieuws over de vaccins betekent voor ons normale leven - Miljardenverlies hangt boven ziekenhuizen door covid-19 - Waarom Trump in Iran en elders geen rare bokkensprongen kan maken - Welk recept vrolijkt uw coronadagen op?** | 280 |
| **COVID-19 Vaccine for Veterans, Free Customer Experience Certificate, Changes to Patient Billing** | 259 |
| **Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)** | 243 |
| **Help Curving COVID-19, KN95 Masks Are Suggested** | 236 |
| **Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove...etc.** | 229 |
| **Aprovecha Productos COVID en Oferta!** | 205 |
| **Second Potential COVID-19 Wave May Hit, Stock Up On KN95 Masks** | 197 |
| **Fight COVID-19□ With $100 at Amazon Gift Card!** | 196 |
| **Let’s fight together to get through the COVID-19** | 186 |

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** | 11574 |
| **aol.com** | 4373 |
| **timesofindia.com** | 2489 |
| **gmail.com** | 1634 |
| **sicurezzanews.it** | 862 |
| **126.com** | 828 |
| **yeah.net** | 715 |
| **protonmail.com** | 593 |
| **daum.net** | 482 |
| **walla.co.il** | 349 |

## Top-15 IPs Sending COVID Spam

| | |
|---|---|
| **121.135.150.159** | 4150 |
| **45.5.200.6** | 864 |
| **103.225.54.169** | 714 |
| **82.135.19.130** | 486 |
| **103.225.53.45** | 479 |
| **103.225.52.109** | 452 |
| **207.166.95.11** | 422 |
| **103.225.54.173** | 405 |
| **82.135.19.131** | 376 |
| **203.174.90.33** | 362 |

## Top-15 Countries Sending COVID Spam

| | |
|---|---|
| **JP** | 12053 |
| **US** | 8035 |
| **KR** | 4313 |
| **IN** | 2851 |
| **CN** | 2440 |
| **DE** | 2111 |
| **BR** | 1273 |
| **FR** | 910 |
| **GB** | 844 |
| **--** | 763 |

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

| | |
|---|---|
| **COVID 19 WEB DIR. STREAM CYBERSECURITY, COMPLIANCE, GDPR: perimetro nazionale sicurezza (in vigore dal 5/11/20), rischi 15/12/20** | 14 |
| **NUEVA FORMACION COVID PARA EMPRESAS** | 7 |
| **OSCE: Misija OSCE-a u BiH predstavila izvještaj o odgovoru na krizu uzrokovanu pandemijom COVID-19** | 4 |
| **COVID 19 WEB DIRETTA STREAM GESTIONE RISCHIO IMPRESA: obbligatorietà adeguati assetti e MOG 231, equilibrio finanziario 2/12/20** | 4 |
| **RE; COVID19 suspect- placed in isolation** | 3 |
| **PARTE COVID-19 DEL 18NOV2020 EESTP PNP TRUJILLO** | 2 |
| **[Arabic Press Release] اجتماع صلاة عبر الإنترنت للمتدينين من جميع أنحاء العالم لإنهاء COVID-19** | 2 |
| **Re: Invitación al Programa Nacional de Formación para la Vacunación contra la COVID -19** | 2 |
| **Каждый месяц Тульский филиал «АльфаСтрахование» организует тестирование сотрудников ООО «423 Завод» в Богородицке на COVID-19** | 2 |
| **Foro de París sobre la Paz - Proyecto mexicano seleccionado para construir el mundo poscovid** | 2 |

**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: 132,971
Domains with Potential Mail Servers: 2,635
Email-Capable Domains and Hosts: 50,514
Live Hosts and Domains Not Parked: 45,783

## Mobile Apps

### Apps in Official Stores: 474

by Store

| | |
|---|---|
| **Apple** | 238 |
| **Google** | 221 |
| **WindowsPhone** | 14 |
| **Amazon** | 1 |

### Apps in Secondary/Hybrid/Affiliate Stores: 1,756

by Store Type:

| | |
|---|---|
| **Hybrid** | 922 |
| **Secondary** | 775 |
| **Affiliate** | 59 |

### Blacklisted Mobile Apps: 28

by Store Type:

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