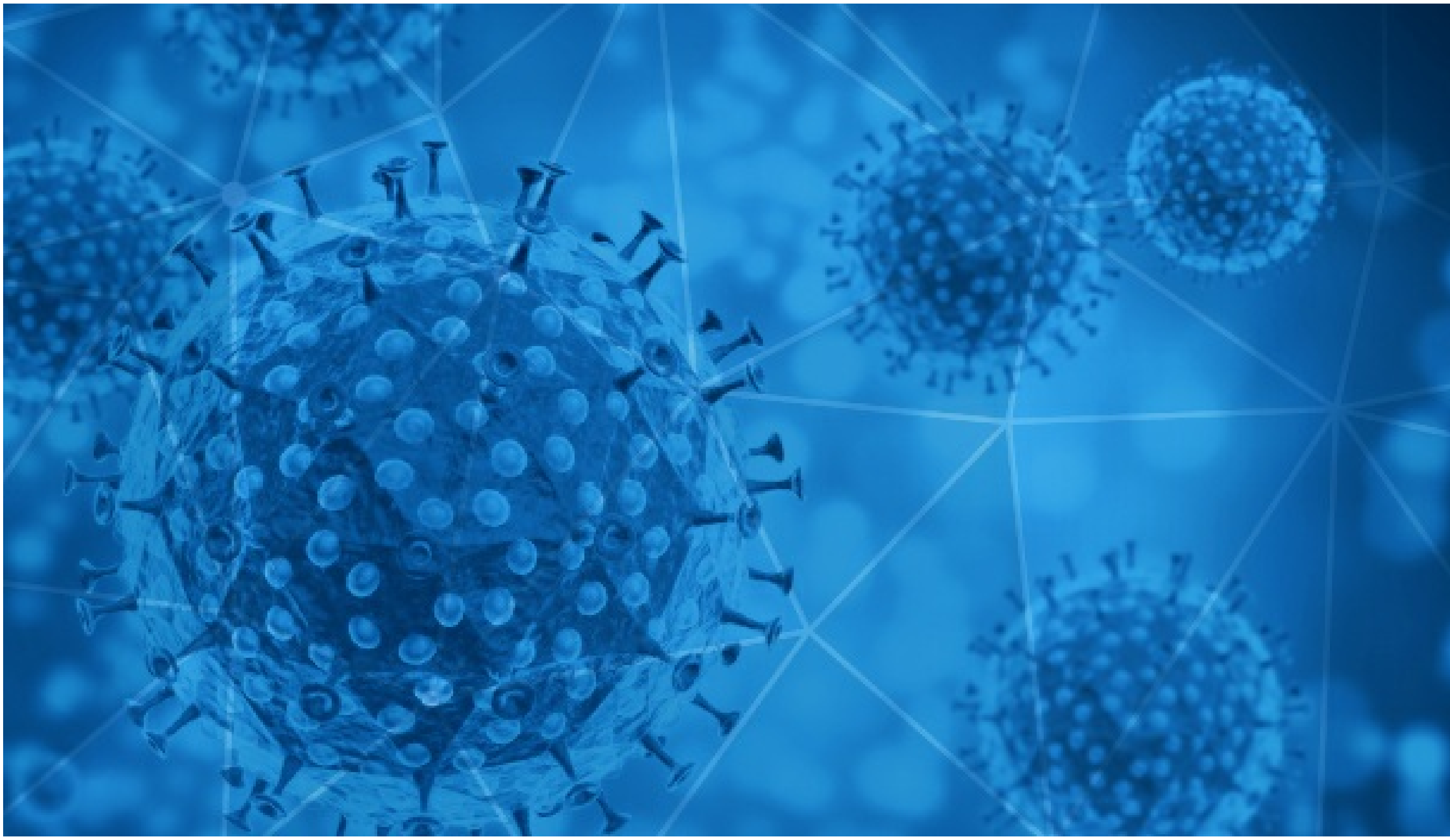
**RiskIQ i3:**

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

2020-09-14



## 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

# COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 2020-09-13 to 2020-09-14. During this period, RiskIQ analyzed 20,186 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,806 unique subject lines observed during the reporting period. The spam emails originated from 761 unique sending email domains and 2,246 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

## Top-25 Subjects

| | |
|---|---|
| **The Corona Letter: Can a mask be a crude vaccine?** | 3969 |
| **My COVID-19 Donation** | 1181 |
| **Reife Frauen zu Corona-Zeiten treffen** | 1032 |
| **ICO Covid Inversión** | 967 |
| **Prevencion de covid19** | 666 |
| **Cuidate del COVID19 con nuestros productos** | 657 |
| **Videos para la prevencion de Covid** | 652 |
| **Frente al Coronavirus nos Cuidamos Todos !** | 552 |
| **Re: Defeat Coronavirus, non contact fever alarm device** | 477 |
| **Contactless infrared body temperature thermometer defeat Coronavirus** | 453 |
| **Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)** | 447 |
| **Congratulations! your Covid Antibody IgG + IgM appointment is confirmed at Rs 750 only.** | 416 |
| **CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19** | 405 |
| **Incontri online in Italia (no corona)** | 382 |
| **COVID-19 - Federal Funding Programs** | 316 |
| **Chinese Virologist Shatters COVID Narrative with Bombshell Discovery** | 229 |
| **Check the appointment for Covid Antibody IgG + IgM test starting at Rs 750 and confirm soon.** | 197 |
| **Van Ranst haalt uit naar critici en politici die coronamaatregelen in vraag stellen - Toekomst van de liefde: ‘Vreemdgaan houdt monogamie in stand’ - Amerikaans studentenfeestje waar iedereen besmet is, stilgelegd - De strakke teugels van Von der Leyen** | 192 |
| **Re: Covid-19 acrylic protect shield** | 182 |
| **Let’s fight together to get through the COVID-19** | 181 |
| **TEST ANTÍGENO COVID-19 TIPO PCR** | 137 |
| **Covid-19 Rapid Test Kits** | 126 |
| **Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products).** | 122 |
| **Re:□coronavirus civil mask / Chinese qualified manufacturer** | 121 |
| **Re: Covid-19 Protective acrylic sneeze guards** | 110 |

# COVID-19 Email Spam Statistics (Continued)

## Top-15 Domains Sending COVID Spam

| | |
|---|---|
| **timesofindia.com** | 3969 |
| **gmail.com** | 2514 |
| **countermail.com** | 1975 |
| **126.com** | 1700 |
| **data2web.de** | 1032 |
| **keyable.net** | 930 |
| **sabaziusvi.com** | 865 |
| **seajin.chtah.com** | 613 |
| **grupocorreomasivo.com** | 552 |
| **galanteo.com** | 382 |

## Top-15 IPs Sending COVID Spam

| | |
|---|---|
| **190.247.255.194** | 1262 |
| **43.239.110.184** | 1181 |
| **46.20.37.30** | 1032 |
| **113.116.207.111** | 864 |
| **201.231.6.4** | 713 |
| **181.46.136.168** | 405 |
| **5.199.131.7** | 381 |
| **219.65.85.30** | 204 |
| **219.65.85.34** | 204 |
| **219.65.85.25** | 201 |

## Top-15 Countries Sending COVID Spam

| | |
|---|---|
| **IN** | 5271 |
| **CN** | 3164 |
| **US** | 2830 |
| **AR** | 2452 |
| **DE** | 1726 |
| **ES** | 1065 |
| **FR** | 1009 |
| **BE** | 427 |
| **GB** | 260 |
| **CA** | 224 |

# COVID-19 Email Spam Statistics (Continued)

## Top Subjects Containing exe Files

## Top-15 Subjects Containing doc/xlsx Files

| | |
|---|---|
| **ANC Weekly COVID-19 Reports** | 29 |
| **Covid-19 compensation fund** | 8 |
| **COVID-19 RELIEF FUNDING** | 2 |
| **Corona-Wochenbericht1308** | 2 |
| **COVID -19 DUTY SCHEDULE OF DNB/CPS RESIDENTS** | 2 |
| **PARTE COVID-19 DEL 13SET2020 EESTP PNP TRUJILLO** | 1 |
| **Line List Form COVID-19 9-1** | 1 |
| **Fwd: COVID-19 - September 12, 2020** | 1 |
| **[Spzg-Newsletter] CORONA: Update Freischaltung System für finanzielle Unterstützung von Mitgliedsvereinen** | 1 |
| **CONSOLIDADO DE LLAMADA CASO COVID-19** | 1 |

# 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: 123,954
Domains with Potential Mail Servers: 2,967
Email-Capable Domains and Hosts: 45,918
Live Hosts and Domains Not Parked: 69,819

## Mobile Apps

### Apps in Official Stores: 415

by Store

| | |
|---|---|
| **Apple** | 211 |
| **Google** | 189 |
| **WindowsPhone** | 14 |
| **Amazon** | 1 |

### Apps in Secondary/Hybrid/Affiliate Stores: 1,313

by Store Type:

| | |
|---|---|
| **Hybrid** | 761 |
| **Secondary** | 497 |
| **Affiliate** | 55 |

### Blacklisted Mobile Apps: 29

by Store Type:

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