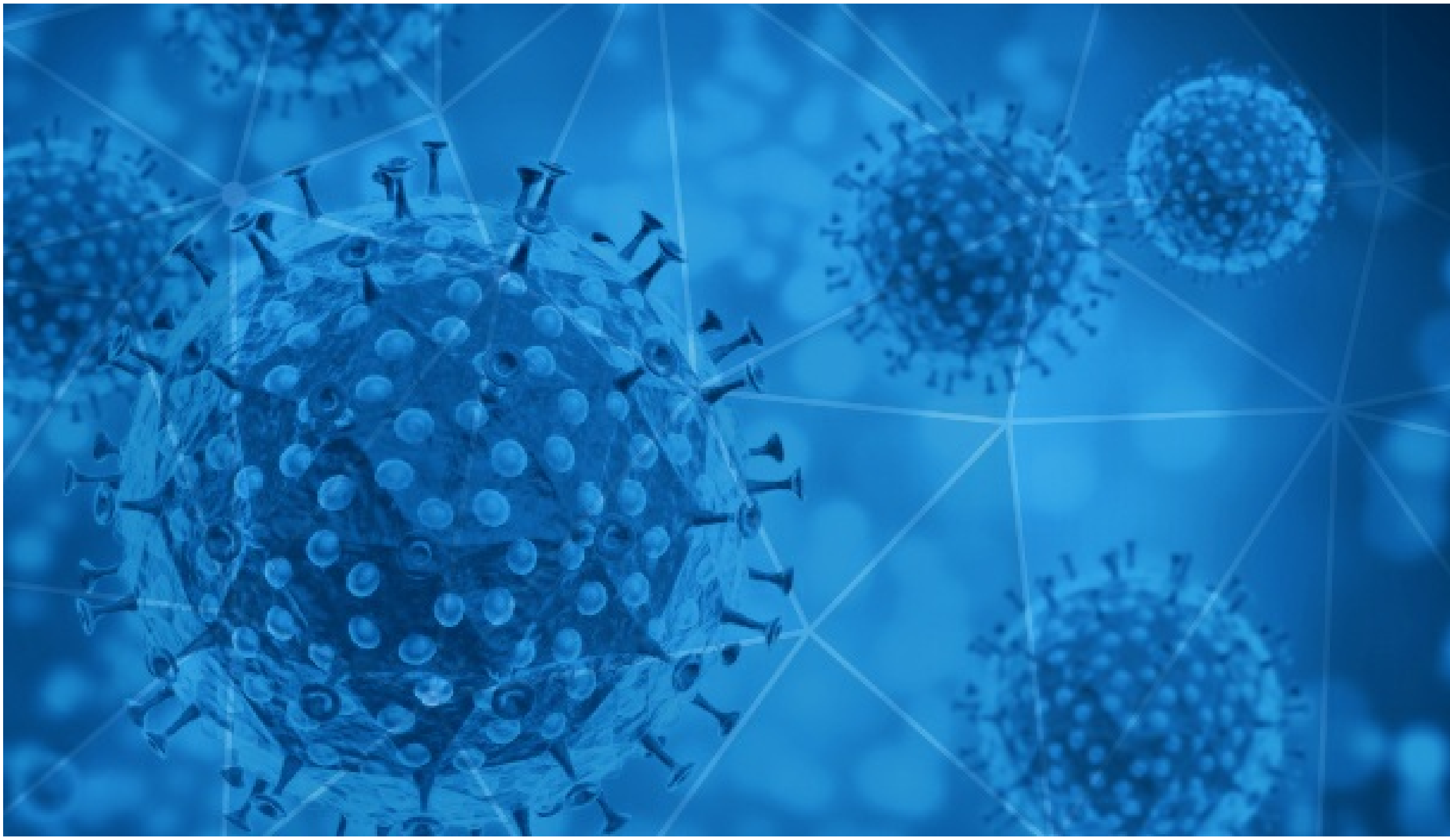
**RiskIQ i3:**

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

2020-07-29



## 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 2020-07-28 to 2020-07-29. During this period, RiskIQ analyzed 28,478 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,889 unique subject lines observed during the reporting period. The spam emails originated from 1,908 unique sending email domains and 3,664 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

## Top-25 Subjects

| | |
|---|---|
| **TIMES TOP10: India's Covid map has transformed** | 2995 |
| **The Corona Letter: A lesson from new outbreaks** | 2849 |
| **Covid Victims Compensation** | 1360 |
| **PyMEs contra el COVID19** | 1042 |
| **Super Promociones Julio - Proteccion COVID-19** | 855 |
| **My COVID-19 Donation** | 623 |
| **Importante reportar resultados positivos y negativos COVID-19** | 606 |
| **credito d'imposta sugli acquisti DPI COVID - "ATTIVATO"** | 482 |
| **Covid 19 Wohltätigkeitsfonds** | 480 |
| **2020 COVID-19 Scholarships at University of Minnesota + Fordham University – USA + Others** | 478 |
| **[REDACTED_DOMAIN] Covid 19 Relief Fund Contribution** | 464 |
| **Due to Covid 19 Pandemic , you and your family have been selected to receive (£1,000,000.00 British Pound) charity donation/grant.** | 446 |
| **Incontri online in Italia (no corona)** | 364 |
| **Soluciones para la prevencion del covid19** | 362 |
| **Cabinas para la prevencion del coronavirus?** | 351 |
| **Como volver a la actividad post coronavirus?** | 328 |
| **Oferta !!! Protector Facial Covid-19** | 269 |
| **Test Rapido COVID 19** | 264 |
| **MICROSOFT COVID-19 RELIEF FUND - GLOBALGIVING** | 262 |
| **Let’s fight together to get through the COVID-19** | 253 |
| **Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)** | 252 |
| **Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)** | 228 |
| **ARCO Dual Detector de Temperatura y Metales - Covid-19** | 218 |
| **Join Mayor Muriel Bowser for a Community Leader Telephone Townhall on Coronavirus** | 202 |
| **COVID-19 DONATION FOR YOU! GET BACK TO ME NOW** | 193 |

# COVID-19 Email Spam Statistics (Continued)

## Top-15 Domains Sending COVID Spam

| | |
|---|---|
| **gmail.com** | 3946 |
| **bounce.indiatimes.com** | 2995 |
| **timesofindia.com** | 2849 |
| **countermail.com** | 2083 |
| **126.com** | 1123 |
| **trendingtopic.cl** | 1120 |
| **163.com** | 774 |
| **soft-carpex.com** | 606 |
| **sicurezzanews.it** | 482 |
| **myschool.com.ng** | 478 |

## Top-15 IPs Sending COVID Spam

| | |
|---|---|
| **153.122.116.244** | 1360 |
| **190.247.254.63** | 862 |
| **187.174.101.179** | 623 |
| **190.247.243.11** | 614 |
| **201.134.139.73** | 559 |
| **201.231.4.175** | 504 |
| **64.15.147.126** | 478 |
| **185.222.57.207** | 464 |
| **45.127.62.47** | 446 |
| **119.122.91.162** | 396 |

## Top-15 Countries Sending COVID Spam

| | |
|---|---|
| **US** | 6501 |
| **IN** | 6088 |
| **AR** | 2280 |
| **CN** | 2238 |
| **JP** | 1684 |
| **FR** | 1508 |
| **DE** | 1451 |
| **MX** | 1267 |
| **CA** | 861 |
| **NL** | 754 |

# COVID-19 Email Spam Statistics (Continued)

## Top Subjects Containing exe Files

## Top-15 Subjects Containing doc/xlsx Files

| | |
|---|---|
| **Safety, Security at Work Training(Post Covid 19 Preparedness Course)** | 8 |
| **BHP – obowiązki pracodawcy i pracownika w dobie Covid 19** | 7 |
| **PHHS 7 27 2020 End of Day COVID 19 Report** | 6 |
| **Δελτίο Τύπου - Πιστοποίηση με το COVID Shield της TUV Austria** | 3 |
| **30% DISCOUNT IN DENTAL WORLD, HUNGARY, 8-10 OCT'2020 - COVID-19 COMPLETELY CONTROLLED IN HUNGARY** | 3 |
| **TR: Demande Test COVID 19** | 2 |
| **Fwd: «Մուրացան» համալսարանական հիվանդանոցի վարակաբանների հսկողությամբ 145 երեխա հաղթահարել է Covid 19-ը** | 2 |
| **THÀNH HOÀNG - THÔNG BÁO VỀ CHÍNH SÁCH HỖ TRỢ GIAI ĐOẠN DỊCH BỆNH COVID-19 TẠI ĐÀ NẴNG CỦA CÁC HÃNG** | 2 |
| **Los madrileños cambian de hábitos de consumo por el Covid: adelantaron sus vacaciones a julio y se quedaron en la ciudad** | 2 |
| **R4 COVID-19 Test Sites** | 2 |

# 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: 116,611
Domains with Potential Mail Servers: 2,858
Email-Capable Domains and Hosts: 44,067
Live Hosts and Domains Not Parked: 65,289

## Mobile Apps

### Apps in Official Stores: 359

by Store

| | |
|---|---|
| **Apple** | 190 |
| **Google** | 160 |
| **WindowsPhone** | 8 |
| **Amazon** | 1 |

### Apps in Secondary/Hybrid/Affiliate Stores: 928

by Store Type:

| | |
|---|---|
| **Hybrid** | 596 |
| **Secondary** | 293 |
| **Affiliate** | 39 |

### Blacklisted Mobile Apps: 23

by Store Type:

| | |
|---|---|
| **Secondary** | 20 |
| **Official** | 2 |
| **Hybrid** | 1 |