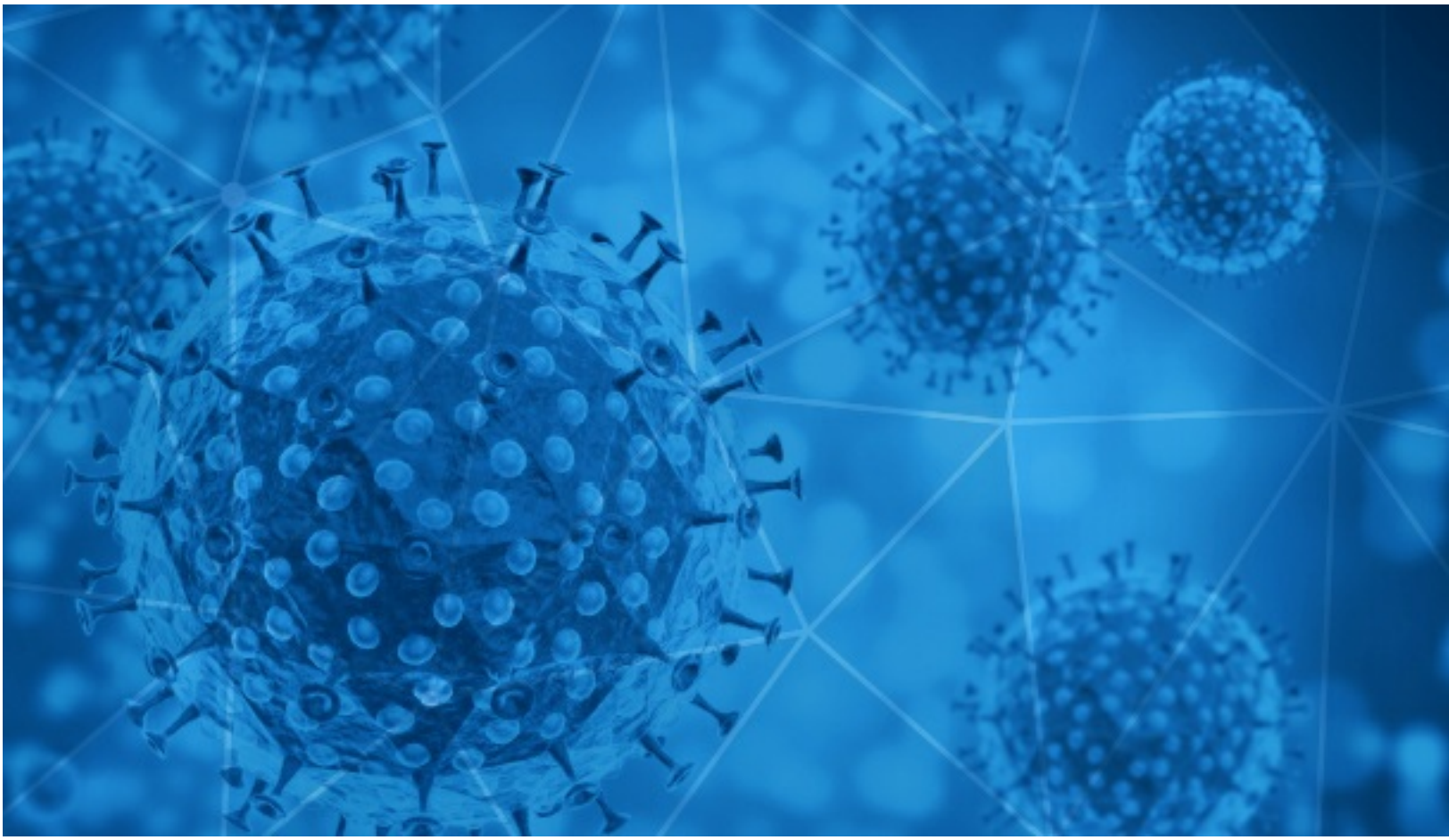
**RiskIQ i3:**

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

2020-07-22



**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 2020-07-21 to 2020-07-22. During this period, RiskIQ analyzed 32,280 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,386 unique subject lines observed during the reporting period. The spam emails originated from 2,133 unique sending email domains and 4,103 unique SMTP IP Addresses. Analysts identified 11 emails which sent an executable file for Windows machines.

## Top-25 Subjects

| | |
|---|---|
| **The Corona Letter: Science behind the Oxford vaccine** | 2317 |
| **Re: COVID-19 Give away** | 2045 |
| **re: Productos disponibles COVID** | 1743 |
| **PyMEs contra el COVID19** | 1092 |
| **Alertan nuevos sintomas: 15 minutos para saber si eres positivo o negativo de COVID-19** | 793 |
| **Second Wave of Covid-19** | 693 |
| **COVID-19 - Projects \| Website \| Mobile Application \| E-Commerce \| SEO (Results Guaranteed) [REDACTED_DOMAIN]** | 617 |
| **covid-19 and children - how does it affect them?** | 457 |
| **[REDACTED_DOMAIN] Notification: You Have (9) Pending Incoming Messages for redacted@threatwave.com (COVID-19 IS REAL!! STAY SAFE)** | 431 |
| **Soluciones para la prevencion del covid19** | 401 |
| **Cabinas para la prevencion del coronavirus?** | 394 |
| **My COVID-19 Donation** | 394 |
| **Como volver a la actividad post coronavirus?** | 392 |
| **Join Mayor Muriel Bowser for a Community Leader Telephone Townhall on Coronavirus** | 385 |
| **MICROSOFT CORONAVIRUS RELIEF FUND - GLOBALGIVING** | 372 |
| **COVID-19 - Website Design & Development / Mobile Application / SEO 100%!R(MISSING)esults Guaranteed [REDACTED_DOMAIN]** | 356 |
| **Campaña Curso Autocuidado  Covid-19 Instituto de Capacitación Advance** | 343 |
| **COVID-19 - Website Design & Development / Mobile Application / SEO 100% Results Guaranteed [REDACTED_DOMAIN]** | 329 |
| **Horario especial por covid-19** | 327 |
| **United Nations Covid-19 Palliative/Financial Support/Congratulations.** | 325 |
| **Re : Re: COVID-19 Give away** | 325 |
| **MICROSOFT CORONAVIRUS RELIEF FUND (CRF) GLOBALGIVING** | 322 |
| **Covid- 19 relief payments** | 303 |
| **We Produce Covid-19 (Face Mask,Isolation Gown,Head/Shoe/Sleeve Cover,Vinyl Gloves ,PE Gloves,Apron)** | 300 |
| **Poll: If the Coronavirus vaccine were available tomorrow, would you take it?** | 292 |

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

# COVID-19 Email Spam Statistics (Continued)

## Top-15 Domains Sending COVID Spam

| | |
|---|---|
| **gmail.com** | 5069 |
| **onet.eu** | 2370 |
| **timesofindia.com** | 2317 |
| **countermail.com** | 2279 |
| **163.com** | 1213 |
| **126.com** | 857 |
| **tecnologia-organizacional.com** | 793 |
| **microphilanthropies.com** | 694 |
| **gofundme.com** | 693 |
| **emirates.net.ae** | 466 |

## Top-15 IPs Sending COVID Spam

| | |
|---|---|
| **103.141.137.241** | 2370 |
| **201.223.74.222** | 1743 |
| **201.231.58.168** | 785 |
| **190.247.223.58** | 777 |
| **185.24.233.65** | 693 |
| **157.119.122.135** | 525 |
| **95.211.211.232** | 466 |
| **157.119.122.134** | 443 |
| **223.73.108.112** | 395 |
| **201.231.27.26** | 394 |

## Top-15 Countries Sending COVID Spam

| | |
|---|---|
| **US** | 7876 |
| **IN** | 4326 |
| **--** | 2997 |
| **CN** | 2656 |
| **AR** | 2540 |
| **CL** | 2469 |
| **FR** | 1358 |
| **CA** | 1087 |
| **GB** | 794 |
| **IE** | 760 |

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

# COVID-19 Email Spam Statistics (Continued)

## Top Subjects Containing exe Files

| | |
|---|---|
| **RE: Payment delayed due to situation COVID-19** | 7 |
| **Fwd: Authorization for landing and departure of a chartered flight and exemption from Covid-19 test** | 1 |
| **Raccomandazioni congiunte su luoghi di lavoro sani e sicuri nei settori chimico, farmaceutico, della plastica e della gomma in tempi di COVID-19** | 1 |

## Top-15 Subjects Containing doc/xlsx Files

| | |
|---|---|
| **PPE items against Covid-19** | 4 |
| **CORONAVIRUS, POSITIVO IL 5,5% DELLE PERSONE SOTTOPOSTE AL TEST SIEROLOGICO EFFETTUATO DALLA SQUADRA B-LIFE** | 3 |
| **CUMPLIMIENTO DE PROTOCOLOS DE BIOSEGURIDAD PARA MANEJO DE PANDEMIA CORONAVIRUS - COVID19** | 3 |
| **NdP - El empleo TIC crece un 1,58% en el último año, pero el negocio cae por el coronavirus** | 2 |
| **DECLARACION JURADA CORONAVIRUS** | 2 |
| **27 JULIO ACTUALIZACIÓN TRIBUTARIA 2020 Y REFORMAS TRIBUTARIAS EN LA LEY ORGANICA DE APOYO HUMANITARIO (COVID-19) CURSO ON LINE 100 % PRACTICO** | 2 |
| **Press Release: Everbridge Announces Two New Countrywide Public Warning Deployments in The Middle East and in Africa to Mitigate COVID-19 and Other Critical Events - ENG - Order# 52252570** | 2 |
| **COVID-19 COMMODITY DISTRIBUTION STATUS AS AT 20TH JULY 2020.** | 2 |
| **COVID Report** | 1 |
| **Tran, Mayor of City of Milpitas, has used all resources available to him including Police Force, to keep HA Kang Silent. Tran is has been in office by support of Chinese ??? and Vietnamese ??? Immegrants.. SIR KEEP ON IGNORING HS KANG SIR TILL THESE TERRORISTS FINALLY KILL HS KANG ( 600,000 DEAD BODIES IN THE NAME OF CORONA VIRUS IS NOT GOOD ENOUGH, THEY WOULD KILL PLENTY PLENTY MORE HUMENS. BEFORE SOME BODY TELLS THEM IT IS GOOD ENOUGH NOW YOU STOP) MODI / TRUMP, I DO NOT NEED THESE CRIMINALS INDIANS AROUND ME, WHY THEY HAVE TO BE AROUND ME, TO JUST KILL HS KANG, KILL HS KANG. ???? HS Kang is a USA Citizen, and lives in USA. IF any Indian or any person with Indian Origin , has any issue at any place , He can file complaint in USA or in USA Courts, BUT All Indians, and persons with Indian Origin , Including Modi Should get Off HS Kangs Back. White Skin Terrorists (Religion NOT ISLAM) (These are NOT White Skin Supermists, These Are White Skin Terrorists and ARE REAL TERRORISTS WORST THAN ISCS) Indian Terrorists religion is not Islam, They are real Terrorists worst than ICSC.** | 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: 115,507
Domains with Potential Mail Servers: 2,826
Email-Capable Domains and Hosts: 43,680
Live Hosts and Domains Not Parked: 64,977

## Mobile Apps

### Apps in Official Stores: 354

by Store

| | |
|---|---|
| **Apple** | 190 |
| **Google** | 155 |
| **WindowsPhone** | 8 |
| **Amazon** | 1 |

### Apps in Secondary/Hybrid/Affiliate Stores: 903

by Store Type:

| | |
|---|---|
| **Hybrid** | 576 |
| **Secondary** | 289 |
| **Affiliate** | 38 |

### Blacklisted Mobile Apps: 22

by Store Type:

| | |
|---|---|
| **Secondary** | 19 |
| **Official** | 2 |
| **Hybrid** | 1 |