



**RiskIQ i3:**

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

2020-09-01



## 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, phishing, malware, or malicious code. This data is delivered "AS-IS".

[https://covid-public-domains.s3-us-west-1.amazonaws.com/covid19\\_blacklist.html](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 2020-08-31 to 2020-09-01. During this period, RiskIQ analyzed 32,331 spam emails containing either “\*corona\*” or “\*COVID\*” in the subject line. There were 2,750 unique subject lines observed during the reporting period. The spam emails originated from 2,040 unique sending email domains and 3,756 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

### Top-25 Subjects

<b>Cuidate del COVID19 con nuestros productos</b>	2751
<b>Essential Safety PPE For Covid19</b>	2579
<b>{COVID-19} ████████████████████</b>	2244
<b>The Corona Letter: A case against RT-PCR tests</b>	1996
<b>Reife Frauen zu Corona-Zeiten treffen</b>	1861
<b>CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19</b>	1276
<b>Evite contagios, no al Covid19, Accese, Asistencia biométricos</b>	662
<b>Desinfectamos su ambiente de coronavirus</b>	645
<b>Desinfeccion Preventiva Covid19</b>	641
<b>Desinfeccion covid19 mediante termoniebla</b>	631
<b>covid-19 and children - how does it affect them?</b>	599
<b>Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)</b>	587
<b>COVID-19 COMPENSATION UNIT.</b>	498
<b>Equipos de protección COVID 19</b>	490
<b>Bryo Contra Covid19</b>	470
<b>Re: Defeat Coronavirus, non contact fever alarm device</b>	363
<b>Contactless infrared body temperature thermometer defeat Coronavirus</b>	329
<b>Covid-19: Quality IT Projects   SEO (Results Guaranteed) - [REDACTED_DOMAIN]</b>	318
<b>Aprovecha productos de protección Covid en Oferta!!!</b>	286
<b>Insumos COVID-19-Los mejores precios</b>	285
<b>Re: keep away from Covid-19</b>	283
<b>Keep your elevator controlled &amp; COVID-19 contamination free</b>	266
<b>Covid-19: Quality IT Projects   SEO (Results Guaranteed) [REDACTED_DOMAIN]</b>	260
<b>Let's fight together to get through the COVID-19</b>	236
<b>COVID-19 Pandemic - Most valuable financial lessons learnt</b>	212

- CONFIDENTIAL -

## COVID-19 Email Spam Statistics (Continued)

### Top-15 Domains Sending COVID Spam

<b>countermail.com</b>	4789
<b>gmail.com</b>	2999
<b>medicproduction.com</b>	2579
<b>toyotacarr.com</b>	2244
<b>timesofindia.com</b>	1996
<b>data2web.de</b>	1861
<b>126.com</b>	1670
<b>hotmail.com</b>	951
<b>keyable.net</b>	692
<b>sopytecchile.com</b>	662

### Top-15 IPs Sending COVID Spam

<b>86.104.194.169</b>	2579
<b>46.20.37.30</b>	1860
<b>201.231.8.80</b>	1438
<b>201.231.83.58</b>	1298
<b>181.46.136.168</b>	1276
<b>201.231.6.22</b>	1257
<b>113.116.206.81</b>	675
<b>46.101.218.158</b>	662
<b>113.30.139.37</b>	608
<b>201.231.6.254</b>	492

### Top-15 Countries Sending COVID Spam

<b>AR</b>	6337
<b>US</b>	5084
<b>IN</b>	3744
<b>DE</b>	3456
<b>CN</b>	3025
<b>RO</b>	2589
<b>JP</b>	2411
<b>--</b>	757
<b>FR</b>	636
<b>IT</b>	399

- CONFIDENTIAL -

## COVID-19 Email Spam Statistics (Continued)

### Top Subjects Containing exe Files

### Top-15 Subjects Containing doc/xlsx Files

<b>Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020</b>	21
<b>Covid Testing opportunity:</b>	15
<b>NUEVA FORMACION COVID PARA EMPRESAS</b>	6
<b>COVID-19 RELIEF FUNDING</b>	6
<b>FE DE ERRATAS - El Ojo 2020 reconocerá a las Mejores Ideas relacionados al Covid-19</b>	2
<b>RE: Lab stakeholders - COVID-19 issues</b>	2
<b>Ενημέρωση για COVID-19 από το Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών (31/8/2020)</b>	2
<b>OIL SPILLAGE DISASTER IN MAURITIUS &amp; COVID 19 - SEGA TOURS UPDATE 28.08.20</b>	2
<b>reitero solicitud a efectos se expida resultado de prueba covid 19 y otros</b>	1
<b>COVID 19 Line List</b>	1

- CONFIDENTIAL -

## 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: 121,576  
Domains with Potential Mail Servers: 2,960  
Email-Capable Domains and Hosts: 45,297  
Live Hosts and Domains Not Parked: 66,829

### Mobile Apps

#### Apps in Official Stores: 409

by Store

Apple	211
Google	183
WindowsPhone	14
Amazon	1

#### Apps in Secondary/Hybrid/Affiliate Stores: 1,260

by Store Type:

Hybrid	730
Secondary	478
Affiliate	52

#### Blacklisted Mobile Apps: 27

by Store Type:

Secondary	24
Official	2
Hybrid	1