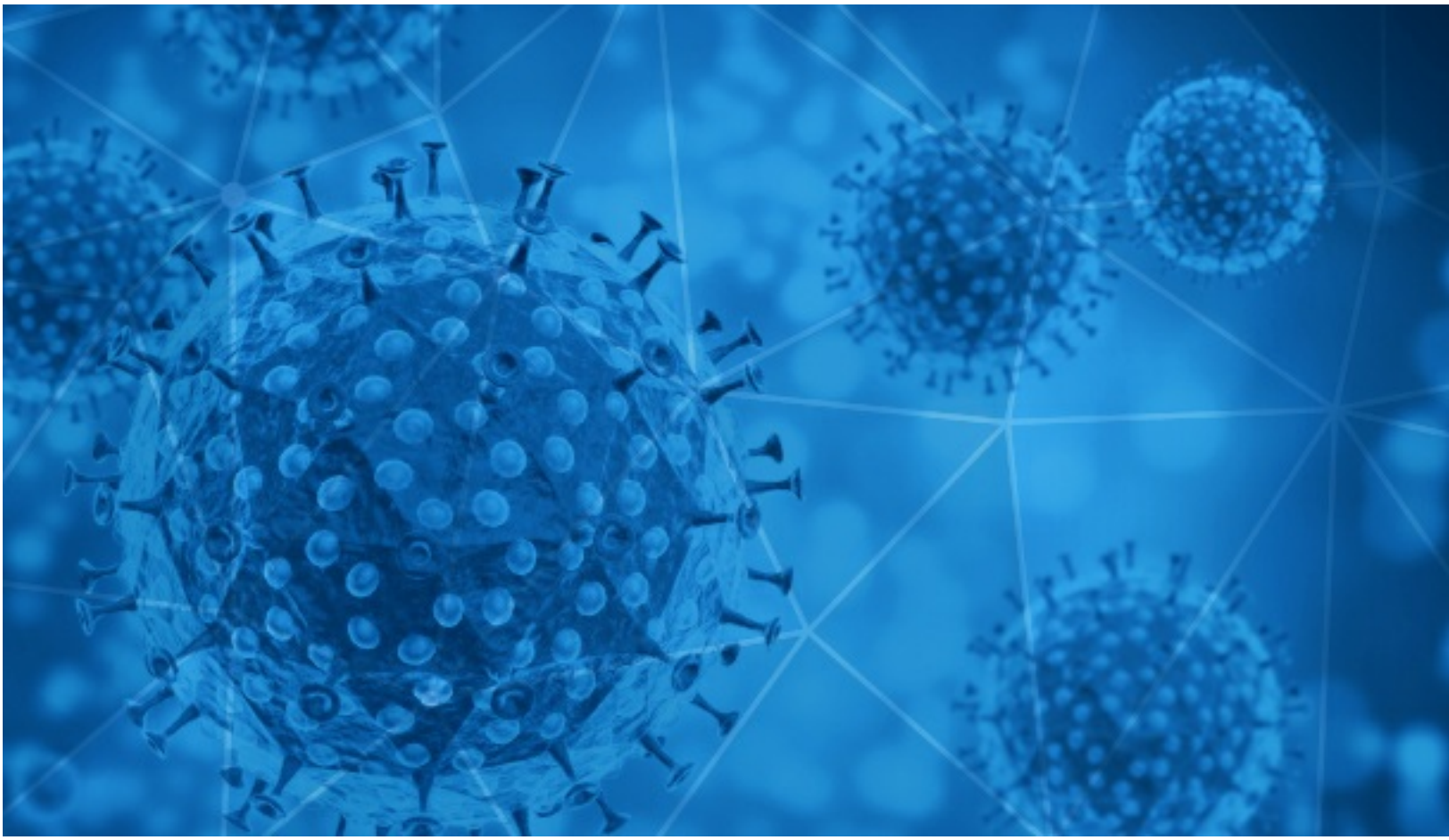
RISKIQ®

RiskIQ i3:

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

2020-10-20



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 2020-10-19 to 2020-10-20. During this period, RiskIQ analyzed 49,707 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,717 unique subject lines observed during the reporting period. The spam emails originated from 2,297 unique sending email domains and 4,748 unique SMTP IP Addresses. Analysts identified 2 emails which sent an executable file for Windows machines.

Top-25 Subjects

PM calls for ensuring election-like arrangement for Covid-19 vaccine delivery; Highlights India’s commitment to Global Food Security…More in the newsletter!	7600
Pelosi sets deadline for stimulus talks, the states with the best COVID-19 responses, and more from Apple News	5440
TIMES TOP10: There's community transmission of Covid-19 but…	5135
The Corona Letter: What's behind the fall in Covid numbers?	3973
Don't want COVID? Don't worry, CVS Pharmacy Got you!	2266
Test de deteccion rapida COVID19	1265
Test rapido para la deteccion del Coronavirus	1240
Limpieza y desinfeccion COVID 19	1212
UN. CORONA-VIRUS RELIEF FUND	712
Proteccion Covid Totem de Control	697
PE in the age of COVID-19	648
Your COVID-19 Registration	603
COVID 19 community Dialogue Initiative 2020	539
LOMBARDIA: prorogata al 13 novembre la scadenza del bando "Reattivi contro il Covid". Riconversione e Ampliamento attività produttive per produzione dispositivi di protezione individuale (DPI) e dispositivi medici (DM) per gestire l'emergenza Covid19	529
Prepare your Workforce for Post-Covid - HR.com General eBulletin for the Week of October 19, 2020	465
Evite el coronavirus en su negocio	438
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	424
Test Rápido Covid-19 Segunda Generación - 10.000 Un Entrega Inmediata	342
[CND Español - 4252]. 8 pasajeros contrajeron la Covid 19 a bordo del Costa Diadema	254
mi seguro insumos covid 19 protege a tu familia	254
Contactless infrared body temperature thermometer defeat Coronavirus	230
Covid-19 Marketing that won't break the bank	219
Re: Defeat Coronavirus, non contact fever alarm device	216
Help to fight COVID-19 fever alarm security door	210
Let’s fight together to get through the COVID-19	188

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

sampark.gov.in	7600
insideapple.apple.com	5546
bounce.indiatimes.com	5135
tutanota.com	4286
timesofindia.com	3974
deltawin.club	2123
gmail.com	1844
yeah.net	1063
outlook.com	708
trendingtopic.cl	697

Top-15 IPs Sending COVID Spam

139.99.193.208	2135
190.247.240.8	839
201.231.115.82	774
201.231.6.207	768
201.231.6.78	766
66.43.119.17	711
113.89.40.176	656
67.192.51.27	647
190.247.227.64	616
45.143.223.147	539

Top-15 Countries Sending COVID Spam

IN	16730
US	14616
AR	4440
CN	3361
AU	2435
FR	1499
DE	1204
IT	1110
--	685
BE	367

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

WHO EBOOK ON CORONA VIRUS	2

Top-15 Subjects Containing doc/xlsx Files

BHP – obowiązki pracodawcy i pracownika w dobie Covid 19	15
Online Workshop on "Kaizen Response to COVID Challenge – Improve Productivity Rapidly!" - 28 – 29 October 2020: 3.00 – 6.00 p.m.	11
NP - Celestyal Cruises incluye un seguro de viaje gratuito con cobertura para COVID-19 incluida	5
Ndp_ENLIGHTED ABRE SU EDICIÓN 2020 CON LA EDUCACIÓN COMO PALANCA CLAVE PARA LIDERAR EL NUEVO MUNDO DIGITAL post-COVID	5
ULTIMO SOLLECITO COVID-19 WEBINAR DIRETTA STREAMING Green Economy, Fonti Rinnovabili, Sviluppo Sostenibile 22/10/20	4
Fwd: Due to covid Admission Date extended till 30 th 0ct 2020 at IMED INSTITUTE BELAPUR,NAVI MUMBAI	3
MANIFIESTO de la Profesión Enfermera sobre la vacunación y realización de pruebas diagnósticas de COVID-19, en las oficinas privadas de farmacia.	3
Upcoming Compliance Activities for Covid Centre Pvt Ltd	3
ULTIMO SOLLECITO COVID-19 WEBINAR DIRETTA STREAMING Focus IAS/IFRS 21/10/20 (intera giornata)	3
RVHS: Positive COVID-19 Classmate	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: 129,855
Domains with Potential Mail Servers: 2,741
Email-Capable Domains and Hosts: 49,034
Live Hosts and Domains Not Parked: 46,582

Mobile Apps

Apps in Official Stores: 464

by Store

Apple	237
Google	212
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,609

by Store Type:

Hybrid	860
Secondary	692
Affiliate	57

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1