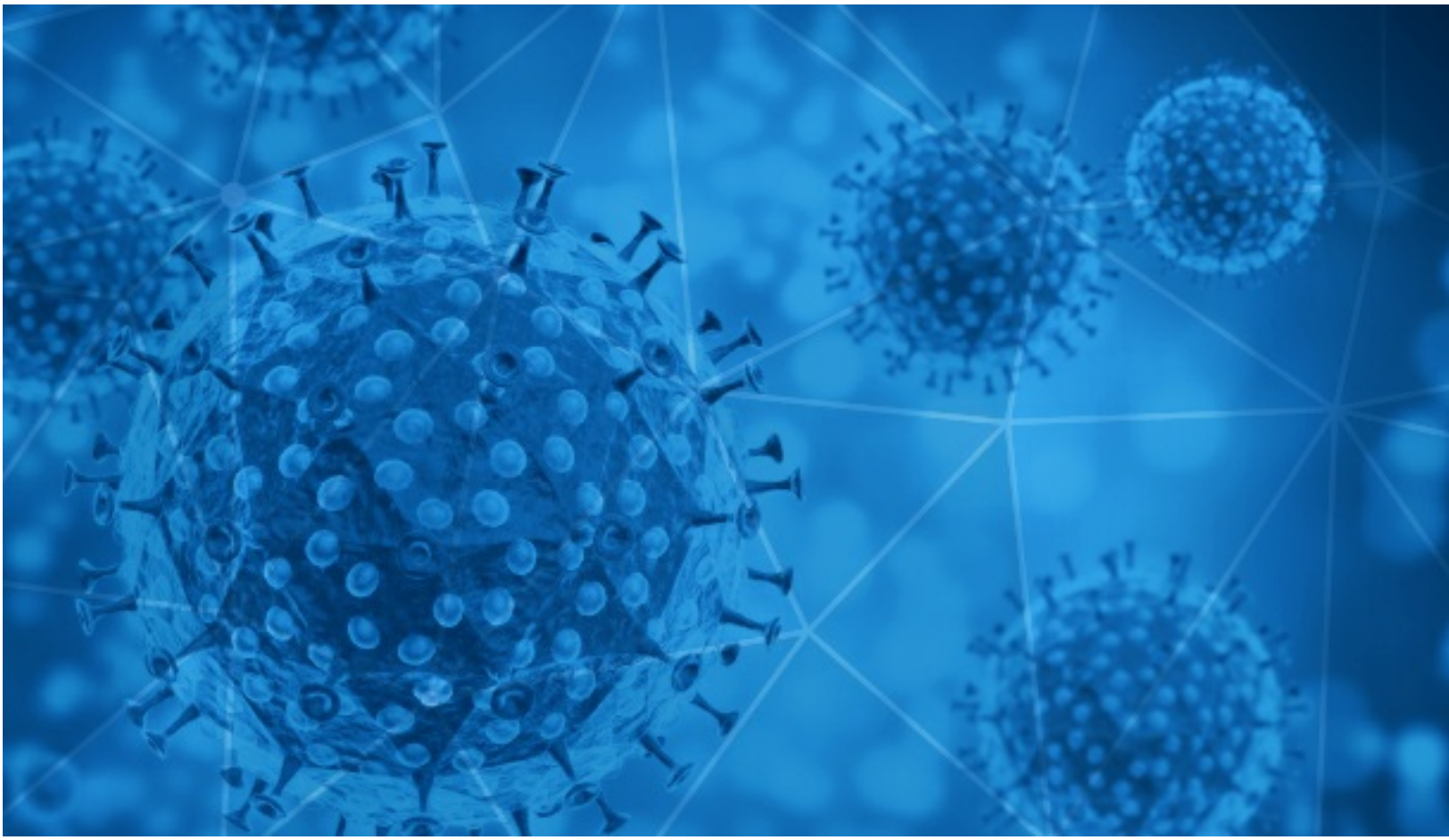
RISKIQ®

RiskIQ i3:

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

2020-10-28



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 2020-10-27 to 2020-10-28. During this period, RiskIQ analyzed 35,947 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,986 unique subject lines observed during the reporting period. The spam emails originated from 2,333 unique sending email domains and 4,724 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

Proteja su negocio de COVID19 y ofrezca seguridad a sus clientes	4733
The Corona Letter: More doubts over herd immunity	3299
Test rapidos de covid19 aprobados por ANMAT	1451
Precio test covid19	1416
"Die Corona-Krise…", Stellenangebote, Newsletter-…, Betriebsnachfolge, Tipps und Story	715
Evite el coronavirus en su negocio	698
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	675
COVID-19 Asesoramiento contable para tu empresa	630
ATENCION COVID-19 Estudio Contable, Legal e Impositivo para tu negocio	620
Re: Notification your test results COVID-19 [note-7893]	483
Aprovecha productos COVID en oferta!!!	472
Fwd:Aviso Su Credito COVID-FOGAPE fue Aprobado.	449
WORLD HEALTH ORGANIZATION $500,000 GRANT CONFIRMATION FOR CORONA VIRUS	438
CORONA-VIRUS RELIEF FUND {UNITED NATION OFFICE,GEVEVA}	347
Re:Corona virus Protection Pills and sex pills.	342
TermoScanner Anti-Covid in pronta consegna. Prezzi dimezzati e modelli a partire da soli Euro 499,00. Non Abbassiamo la guardia!!!	316
Payment Slip_Re□Shipment_Re□Order NA4497T COVID	305
Re: Defeat Coronavirus, non contact fever alarm device	293
Rýchly test Nadal® Covid-19 Ag - Len pre medicínske účely	292
NCJ Daily - Humboldt Marks 10th COVID Death. EPD ID's Killed Cyclist. Major Injury Accident in Eureka Under Investigation. Find Your Ballot. Witches on the Water.	286
Contactless infrared body temperature thermometer defeat Coronavirus	272
Help to fight COVID-19 fever alarm security door	272
[How-To Guide] Display COVID-19 policies on a TV	270
Servicio de Pruebas Rápidas, Moleculares para COVID19 a Empresas y Domicilio.	270
Your appointment for Covid Antibody test is fixed at Rs 750 only.	248

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

walla.co.il	9548
timesofindia.com	3303
gmail.com	2119
keyable.net	837
126.com	836
yeah.net	794
bancoestado.cl	765
handels-vertretungen.net	715
serviceprovidedbythem.com	570
163.com	370

Top-15 IPs Sending COVID Spam

190.247.255.240	6364
201.231.8.20	1163
113.116.207.168	837
95.217.4.0	714
190.247.255.163	704
201.231.83.187	696
181.46.136.168	675
138.201.29.247	447
118.24.114.228	434
66.43.119.17	412

Top-15 Countries Sending COVID Spam

AR	10560
US	8096
CN	4030
IN	3752
DE	1480
FR	1277
FI	749
IT	693
BE	548
CL	539

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Fwd: Covid 19 - Nouveau protocole	1

Top-15 Subjects Containing doc/xlsx Files

CUMPLIMIENTO DE PROTOCOLOS DE BIOSEGURIDAD PARA MANEJO DE PANDEMIA CORONAVIRUS - COVID19	8
Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020	6
COVID19 WEBINAR DIRETTA STREAMING Licenziamento DIRIGENTE: liceità, specialità, giustificatezza, soluzioni, contenzioso 18/11/20	6
COVID-19 VENDITA REGISTRAZIONE + ATTI Partecipate Pubbliche, P.A. e PPP nella L. 120/20 Semplificazioni: opportunità 14/10/20	3
CHANGE TO WEBINAR LINK: COVID-19 Vaccine Webinar on Thursday, October 29th at noon	2
Hope you and your family are staying safe from corona virus_Office Address Change Notice_Fee Schedule 0f 2020	2
Религиозные лидеры 19 стран объединились в молитве, чтобы победить COVID-19. 600 человек, 5 континентов, 7 основных религий. Пресс-релиз, фото, видео.	2
[KYNURSE:] KDPH COVID-19 Exposure and Quarantine Process	2
Coronavirus, consegnate 5 barelle di contenimento biologico all'ASP di Catanzaro	2
IMPORTANTE: Gestión administrativa del Departamento de Salud Ocupacional y Protocolos Covid-19 en las Empresas.	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: 130,653
Domains with Potential Mail Servers: 2,637
Email-Capable Domains and Hosts: 49,441
Live Hosts and Domains Not Parked: 46,560

Mobile Apps

Apps in Official Stores: 466

by Store

Apple	235
Google	216
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,652

by Store Type:

Hybrid	870
Secondary	724
Affiliate	58

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1