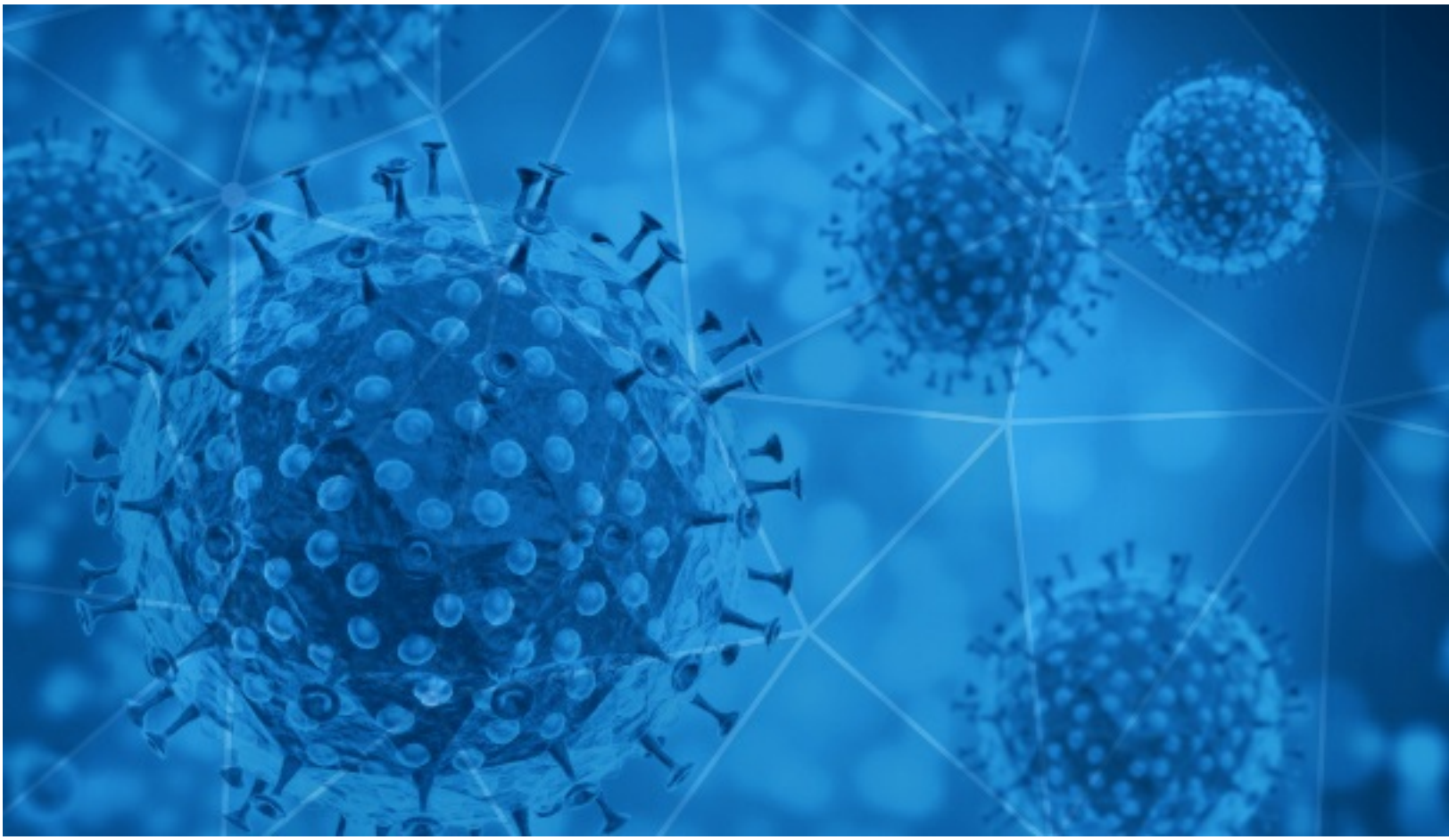
RISKIQ®

RiskIQ i3:

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

2020-10-30



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 2020-10-29 to 2020-10-30. During this period, RiskIQ analyzed 63,081 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,631 unique subject lines observed during the reporting period. The spam emails originated from 2,500 unique sending email domains and 5,410 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	16871
States impose new COVID-19 restrictions, the race to prevent a space war, and more from Apple News	7715
The Corona Letter: Aerosol study provides a breather	3566
5 tys. zł za zachorowanie dziecka na COVID-19. Sprawdź>>	1813
Proteja su negocio de COVID19 y ofrezca seguridad a sus clientes	1174
Test rapido para la deteccion del Coronavirus	1044
Coronavirus cases hit record high +Woman's Butt FELL OFF After Surgery +Y Sisters Stab man 27 times?	1004
Gestión de riesgos y auditoría en tiempos de covid19	919
Boost your internet speeds while you're quarantined from the CoronaVirus	791
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	743
ATENCION COVID-19 Estudio Contable, Legal e Impositivo para tu negocio	689
COVID-19 Asesoramiento contable para tu empresa	661
[Your Guide] Need to display COVID-19 mask policies on a TV?	643
Ingresaron TEST COVID19 de deteccion rapida	621
Test rapidos de covid19 aprobados por ANMAT	567
Evite el coronavirus en su negocio	565
Precio test covid19	515
Triple test para COVID19 de deteccion rapida	486
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	389
October Covid-19 palliative Award USD$3,500,000.00	380
Re: Your Order Corona virus pills and Sex pills	364
Productos Covid-19	355
Protégete RESPONSABLEMENTE Contra el Covid -19 / Los Mejores Precios	316
<□□> States impose new COVID-19 restrictions, the race to prevent a space war, and more from Apple News	308
How to make $3780.23/mth during the 'corona recession'	300

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

epc-store.com	16875
insideapple.apple.com	8024
walla.co.il	6322
timesofindia.com	3569
promotions.overstock.com	2902
mailman.com.pl	1813
gmail.com	1591
caribbeanfever.com	1004
focazen.com	922
yeah.net	778

Top-15 IPs Sending COVID Spam

190.247.240.83	2112
190.247.255.7	1702
201.231.5.120	852
103.225.55.31	802
190.247.241.93	779
181.46.136.168	743
94.152.193.151	704
103.225.55.29	649
185.19.30.32	642
103.225.52.133	562

Top-15 Countries Sending COVID Spam

US	20389
JP	17133
AR	7294
IN	4177
CN	2977
PL	1930
FR	1716
CL	929
DE	837
IT	804

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

COVID-19 WEBINAR DIRETTA STREAMING Gestione impresa tra adeguati assetti e MOG 231/01: obbligatorietà e responsabilità 2/12/20	4
Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020	4
Normas Covid E.F	3
Skierowanie do pracy przy zwalczaniu Covid-19	3
CCS /10466 Llega el estado de Chihuahua a 24 mil 626 casos acumulados de COVID-19	2
Saruna par COVID-19 vakcīnu podkāstā "Sargiet galvas!"	2
Covid	2
CCS10470 SS NO ES OBLIGATORIA LA CREMACIÓN DE PERSONAS FALLECIDAS POR COVID19 ACLARA SECRETARÍA DE SALUD 29OCT (fe de erratas en el cargo de la funcionaria que ya es directora)	2
Hume COVID-19 RCoT/REMT - Out of Sessions update	2
Covid-19	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: 130,896
Domains with Potential Mail Servers: 2,643
Email-Capable Domains and Hosts: 49,587
Live Hosts and Domains Not Parked: 46,505

Mobile Apps

Apps in Official Stores: 466

by Store

Apple	235
Google	216
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,660

by Store Type:

Hybrid	872
Secondary	729
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1