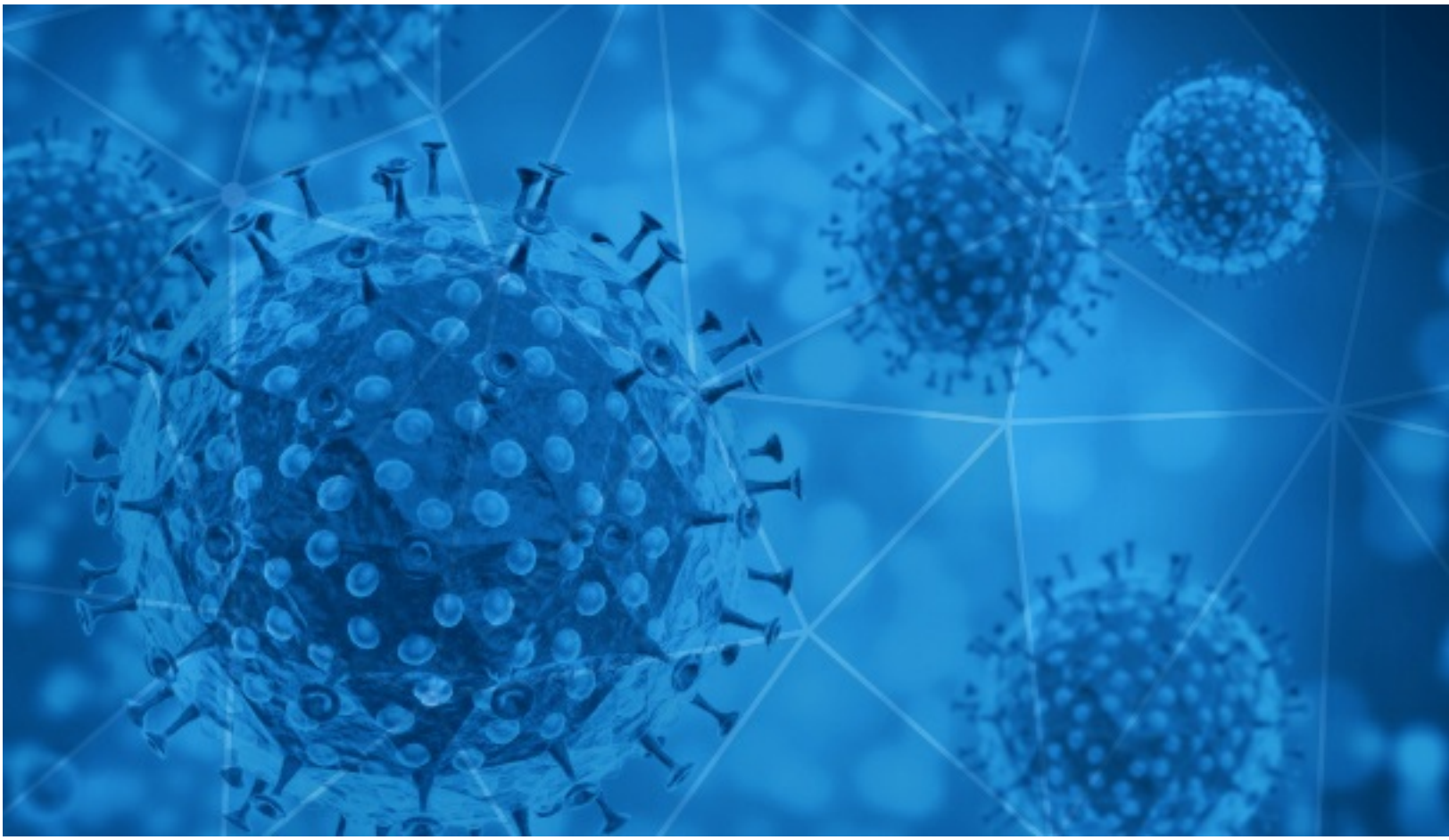
RISKIQ®

RiskIQ i3:

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

2020-10-07



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 2020-10-06 to 2020-10-07. During this period, RiskIQ analyzed 31,940 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,345 unique subject lines observed during the reporting period. The spam emails originated from 2,162 unique sending email domains and 4,770 unique SMTP IP Addresses. Analysts identified 15 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Time is still a big factor in Covid fight	4066
Test rapido para la deteccion del Coronavirus	2191
Test de deteccion rapida COVID19	2071
COVID-19 KILLED ANTHONY	950
Joe Biden: Able to stay home because Black women stocked the grocery shelves + Kanye with COVID-19	818
Limpieza y desinfeccion COVID 19	716
Protection from Coronavirus and other diseases	637
Outbound trunking enhancements, Identities & Addresses tool, and the 5G conspiracy related to Covid-19. Read the September Insider!	452
Lampy sterylizujace UV-C jako dobry sposób walki z koronawirusem (covid-19)	438
Sanitización y Limpieza contra el Covid-19	372
Fundo de socorro da OMS Covid 19	344
Coronavirus Job Retention Scheme	326
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	306
Covid-19 Cash Support für Sie	258
Protégete RESPONSABLEMENTE Contra el Covid -19 / Los Mejores Precios	253
Pruebas Rápidas COVID-19 - Marca CELLEX // EE.UU.	248
TermoScanner Anti-Covid in pronta consegna con sconti oltre il 50% e prezzi a partire da Euro 499,00. Non Abbassiamo la guardia!!!	233
Covid-19 Rapid Test Kits	232
2.000 Belgen gezocht voor fase 3 vaccin-onderzoek - Opflakkerend coronavirus fnuikt economisch herstel - Regeringsblog. Geen ministerpost voor Nathalie Muylle (CD&V): ‘Dat doet pijn’	214
AuraAir: Único Filtro que Elimina el Covid-19 llegó a Chile	204
Уникальная маска! Новая защита от Covid-19	204
Incontri online in Italia (no corona)	200
Маска ! Новая защи��а от Covid-19!	187
Mamparas de proteccion COVID19	187
Самая надежная за��ита от Covid-19	184

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

tutanota.com	5337
timesofindia.com	4067
gmail.com	1189
covid-help.pro	925
yeah.net	917
talktalk.net	835
126.com	819
caribbeanfever.com	818
didww.com	452
promieniowanieuvc.pl	438

Top-15 IPs Sending COVID Spam

181.117.26.93	3242
190.247.254.13	1088
2.94.110.112	925
49.51.186.57	726
216.87.190.232	505
46.19.209.133	452
77.55.215.149	435
194.113.89.65	341
190.247.45.104	322
201.231.27.75	316

Top-15 Countries Sending COVID Spam

US	8139
AR	5585
IN	4391
CN	3164
RU	1164
DE	1146
CA	874
BE	814
GB	664
PL	613

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

Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	15
CUMPLIMIENTO DE PROTOCOLOS DE BIOSEGURIDAD PARA MANEJO DE PANDEMIA CORONAVIRUS - COVID19	10
covid 19 Payments	6
Press Release: COVID-19 Song, Happy Magic TARAHOROVA Saves Countless life in this Pandemic	5
WEBINAR COVID-19 APPALTI e L.120/20 Semplificazioni: cosa cambia su procedure, affidamenti e aggiudicazioni 13/10/20	4
WEBINAR COVID-19 Focus OIC: deroghe contabili e fiscali, ammortamenti, riserva, rivalutazione 20/10/20	4
La segunda ola de Covid 19 y las restricciones de movilidad ponen en jaque la recuperación de zonas claves de la capital de España, tras tres meses de atonía	3
ARCOVID19 - Close Contact Packet	2
COVID 19, FALCINELLI (FILCTEM CGIL): “I LAVORATORI DEL GAS, DELL’ACQUA ED ELETTRICI HANNO IMPEDITO AL PAESE DI FERMARSI”	2
RE: Re: □□□□□□□□□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: 128,130
Domains with Potential Mail Servers: 2,819
Email-Capable Domains and Hosts: 48,511
Live Hosts and Domains Not Parked: 72,163

Mobile Apps

Apps in Official Stores: 443

by Store

Apple	225
Google	203
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,531

by Store Type:

Hybrid	840
Secondary	635
Affiliate	56

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1