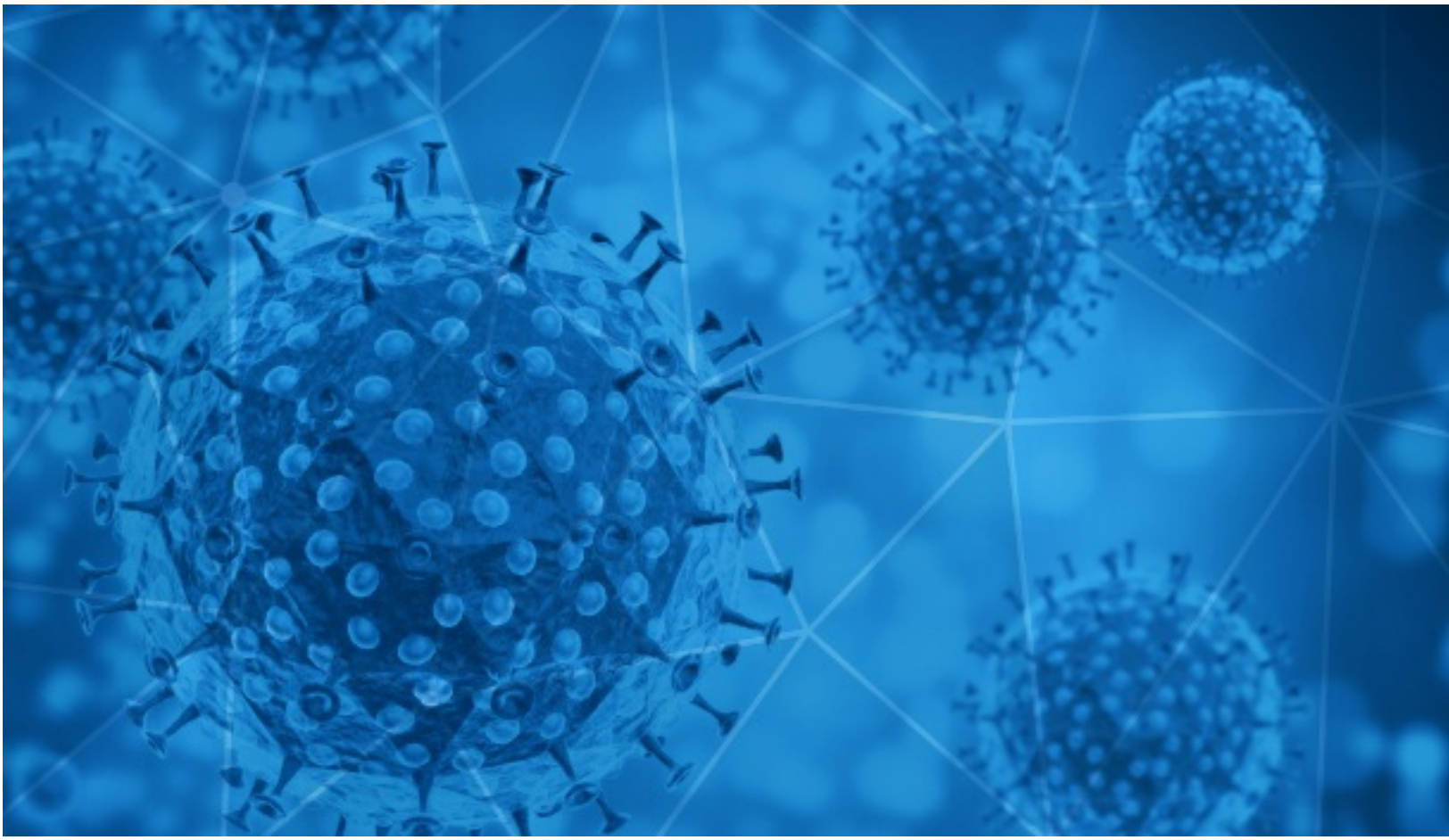
RiskIQ i3:

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

2020-10-16



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 2020-10-15 to 2020-10-16. During this period, RiskIQ analyzed 43,114 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,539 unique subject lines observed during the reporting period. The spam emails originated from 2,267 unique sending email domains and 4,759 unique SMTP IP Addresses. Analysts identified 7 emails which sent an executable file for Windows machines.

Top-25 Subjects

Test de deteccion rapida COVID19	5564
Test rapido para la deteccion del Coronavirus	5508
New coronavirus lockdowns in Europe, Americans break early-voting records, and more from Apple News	4281
The Corona Letter: The pandemic's digital shadow	3328
Proteccion Covid Totem de Control	1346
Equipos de Protección y Prevención del COVID-19	1269
Limpieza y desinfeccion COVID 19	989
Evite el coronavirus en su negocio	796
Mascarillas y Otros Covid	757
Mamparas de proteccion contra el coronavirus	488
Mamparas de proteccion COVID19	483
[UK 1] When the dust [covid-19] settles you will need this to train your NEW leaders	393
Save your family! Covid19 initiative	378
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	370
[UK 2] When the dust [covid-19] settles you will need this to train your NEW leaders	368
TermoScanner Anti-Covid in pronta consegna. Prezzi dimezzati e modelli a partire da soli Euro 499,00. Non Abbassiamo la guardia!!!	279
Protégete RESPONSABLEMENTE Contra el Covid -19 / Los Mejores Precios	262
Para Desinfectar y Matar el CoronaVirus con UVC	258
Líneas ICO Covid para inversión	254
Corona Virus pandemic (Covid-19) Update	234
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ COVID-19□□□□□□□□□□□□□□	228
Help to fight COVID-19 fever alarm security door	213
Re: Defeat Coronavirus, non contact fever alarm device	212
Contactless infrared body temperature thermometer defeat Coronavirus	201
[How-To Guide] Display COVID-19 policies on a TV	193

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	13828
insideapple.apple.com	4295
timesofindia.com	3328
trendingtopic.cl	1346
focazen.com	1269
yeah.net	969
gmail.com	852
bizuk01.com	761
isap.enviador.cl	757
126.com	716

Top-15 IPs Sending COVID Spam

201.231.10.120	9271
190.247.254.85	1596
190.247.226.162	1403
190.247.223.41	893
216.15.151.42	760
165.22.32.231	757
113.89.42.42	626
51.77.33.39	592
190.247.242.253	544
185.221.173.42	279

Top-15 Countries Sending COVID Spam

AR	14107
US	12282
IN	3704
CN	3268
FR	2281
GB	974
DE	694
ES	623
IT	590
--	578

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

***IMPORTANT* Bulk Quote Request-Covid19**	7

Top-15 Subjects Containing doc/xlsx Files

WEBINAR COVID 19 Licenziamento del dirigente: specialità, giustificatezza, ricambio, soluzioni alternative, contenzioso 18/11/20	6
COVID 19 i škole - Zajednički i neprestani rad umanjuje posljedice pandemije	4
WEBINAR COVID 19 Processi di digitalizzazione: documento informatico- presidi normativi e industria 4.0-dal CAD al GDPR 1/12/20	4
Socializo Resultados PCR covid19, Negativos y positivos del 01 al 15 octubre, fuente NetLab2	4
Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	4
Ocena ryzyka zawodowego (aktualizacja pod względem COVID -19)	4
BHP – obowiązki pracodawcy i pracownika w dobie Covid 19	3
El Consejo General de Enfermería pide a Sanidad que incorpore a las enfermeras en la toma de decisiones contra el COVID-19 y desarrolle una planificación de recursos humanos que dé respuesta a las necesidades de los pacientes	3
PHHS 10 15 2020 End of Day COVID 19 Response Summary	3
15 Public Health Organizations Condemn Herd Immunity Scheme for Controlling Spread of SARS CoVID-2	3

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: 129,489
Domains with Potential Mail Servers: 2,765
Email-Capable Domains and Hosts: 48,866
Live Hosts and Domains Not Parked: 46,624

Mobile Apps

Apps in Official Stores: 462

by Store

Apple	235
Google	212
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,580

by Store Type:

Hybrid	854
Secondary	669
Affiliate	57

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1