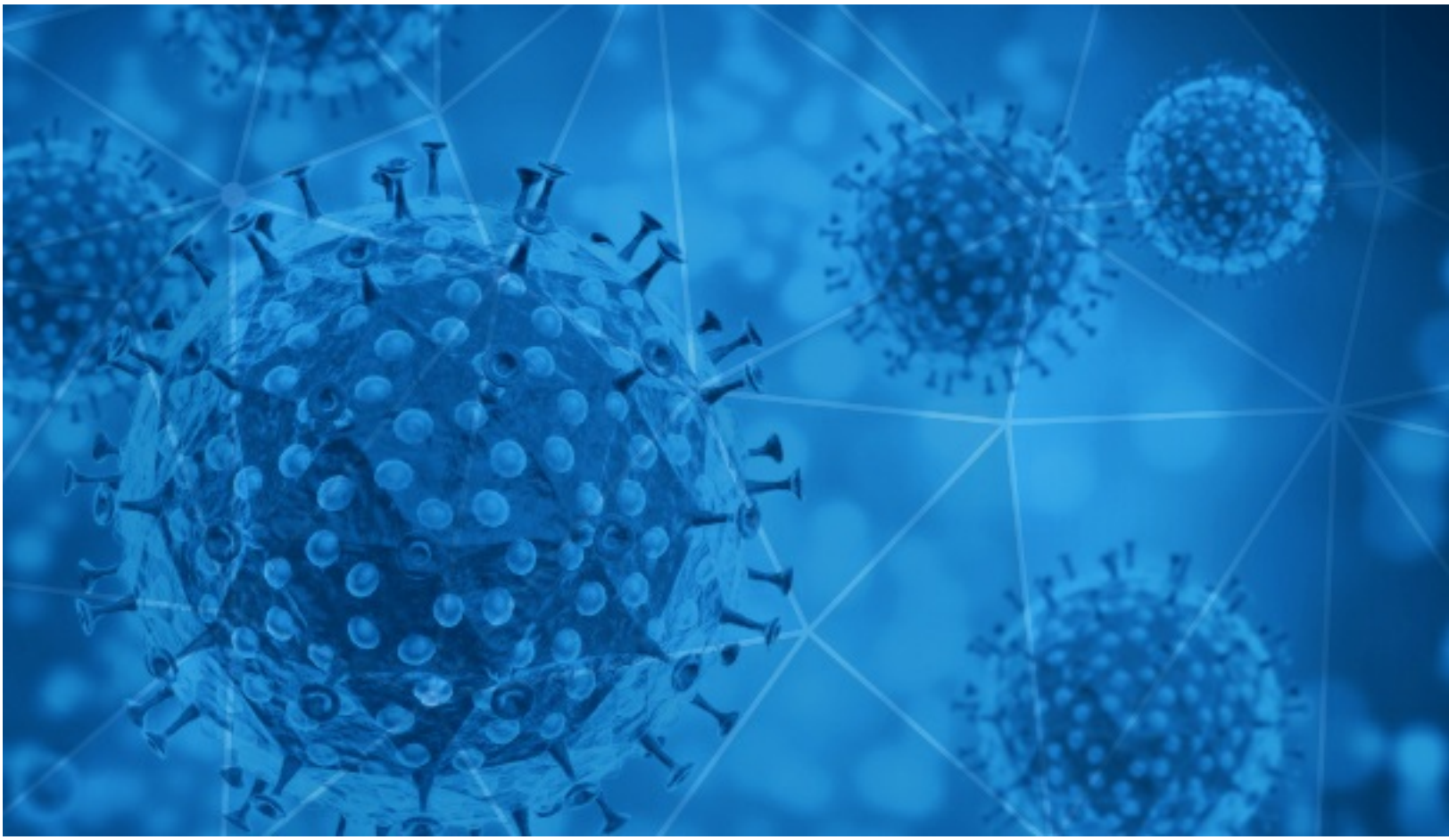
RiskIQ i3:

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

2020-09-25



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 2020-09-24 to 2020-09-25. During this period, RiskIQ analyzed 22,533 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,738 unique subject lines observed during the reporting period. The spam emails originated from 1,663 unique sending email domains and 3,879 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

Reife Frauen zu Corona-Zeiten treffen	1716
Test de deteccion rapida COVID19	1155
The Corona Letter: For vaccines, one target, different methods	832
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	793
Help to fight COVID-19 fever alarm security door	735
My COVID-19 Donation	675
Re:$500,000.00 Covid-19 Pandemic Relief	646
Covid-19 Zuschuss	609
Insumos protección covid	369
Re: COVID-19 - E-Commerce Website | SEO (Results Guaranteed) - [REDACTED_DOMAIN]	348
Resuming after Covid-19 Important Information	347
RE: WB/UNITED NATIONS SCAM VICTIMS COMPENSATIONS PAYMENTS (COVID-19 2020)	338
Trucking Number : DE9712458389 : COVID-19	330
In caso di sintomi influenzali in AZIENDA, come SI FA a distinguere un normale raffreddore dal coronavirus?	299
Prevencion de covid19	299
Videos para la prevencion de Covid	287
Protege a Quienes más Quieres del COVID-19 Manteniendo el Aire Limpio y Libre de Gérmenes	284
- Compensation / Grant For Everyone Affected By (COVID-19) Pandemic -	246
ANTI-COVID-19 Materials	223
Protégete RESPONSABLEMENTE Contra el Covid -19 / Los Mejores Precios	222
Elimina el COVID-19 100% COMPROBADO Y CERTIFICADO	221
Provision of COVID-19 Materials	198
[NOT IN EAP] COVID-19Numbers [Daily-Pub]	196
Protégete del Covid solo con productos Certificados	178
Prueba Rápida Covid-19 para Empresas y Domicilio	177

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmail.com	3276
countermail.com	1911
data2web.de	1716
126.com	1227
timesofindia.com	834
keyable.net	735
protonmail.com	665
yeah.net	544
vip.163.com	421
tie.cl	369

Top-15 IPs Sending COVID Spam

46.20.37.30	1716
190.247.223.204	1101
113.116.204.66	731
43.239.110.184	675
200.68.61.134	646
181.112.154.212	608
119.122.89.6	528
190.247.243.103	457
201.189.169.230	369
178.62.40.158	347

Top-15 Countries Sending COVID Spam

US	5443
CN	3039
IN	2357
DE	2287
AR	2002
CL	1387
GB	907
RU	871
EC	616
FR	531

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

URGENT INFORMATION LETTER: COVID-19 CASE REPORT UPDATES AND NEW APPROVED VACCINES	1

Top-15 Subjects Containing doc/xlsx Files

Online upskilling Program on covid19 management for Nurses and Nursing students	3
PHHS 9 24 2020 End of Day COVID 19 Report	3
Update on COVID-19 Practices	2
REPORTE COVID 19 DEL PERSONAL CAS DE LA EESTP-PNP-TRUJILLO DEL DIA JUEVES 24SET2020.	1
Contatti di caso sospetto COVID19 frequentante i servizi educativi per l'infanzia: aggiornamenti in merito alla gestione	1
Información cadáveres COVID-19	1
NANO DEZENFEKTAN ve COVİD 19 ANTİKOR KİT TESTİ HK.	1
DEFUNCION CASO CONFIRMADO COVID19_GEMD	1
CCCU-COVID-Risk-Assessment-Form-for-students-on-placement.docx	1
Pensión 65 lanza concurso escolar digital "Los Abuelos Ahora" para concientizar la prevención del COVID-19 en adultos mayores	1

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: 126,585
Domains with Potential Mail Servers: 2,924
Email-Capable Domains and Hosts: 47,880
Live Hosts and Domains Not Parked: 69,355

Mobile Apps

Apps in Official Stores: 429

by Store

Apple	220
Google	194
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,452

by Store Type:

Hybrid	802
Secondary	595
Affiliate	55

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	25
Hybrid	2
Official	2