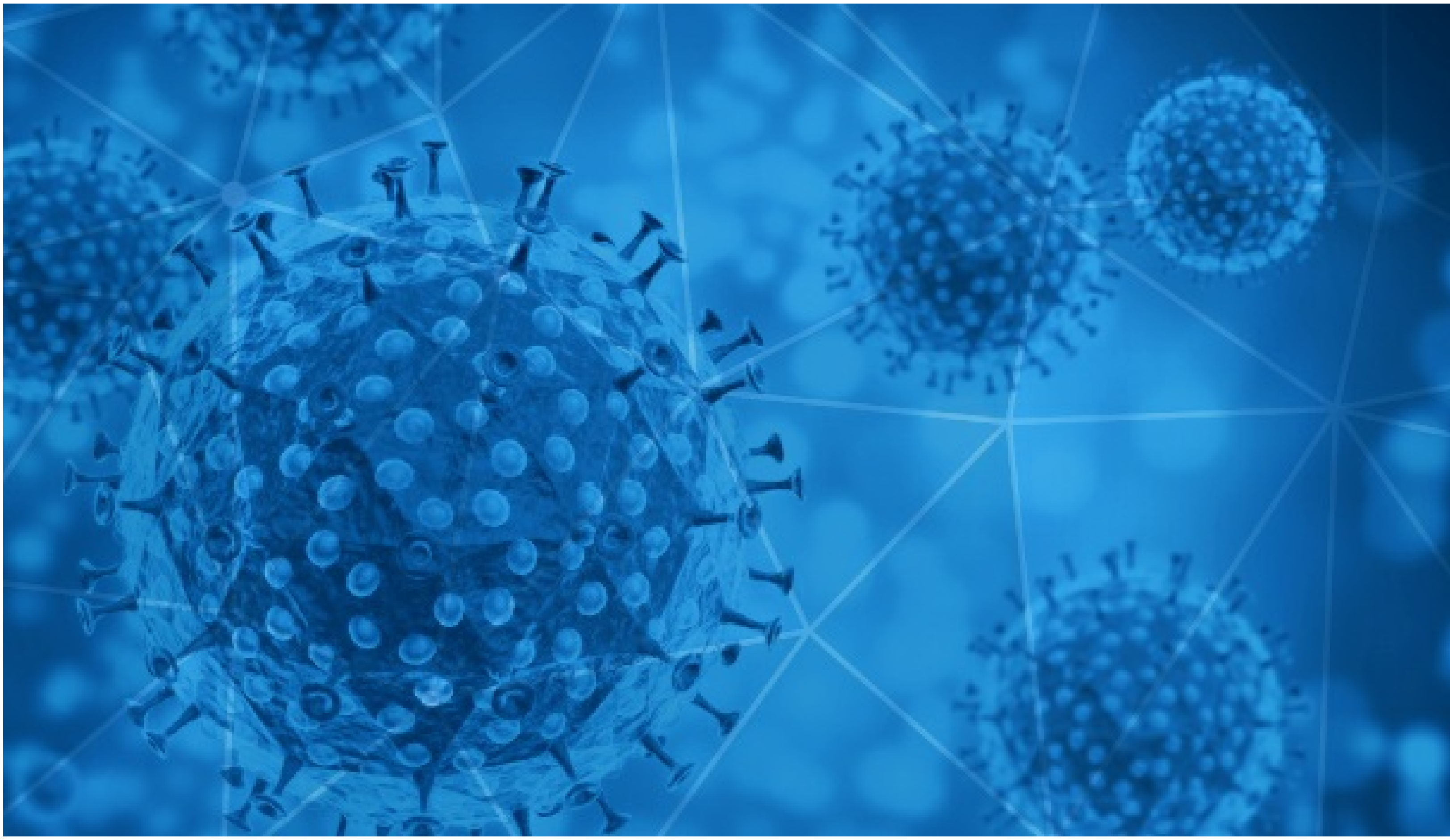
RiskIQ i3:

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

2020-11-13



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

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 2020-11-12 to 2020-11-13. During this period, RiskIQ analyzed 27,987 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,282 unique subject lines observed during the reporting period. The spam emails originated from 2,261 unique sending email domains and 4,541 unique SMTP IP Addresses. Analysts identified 2 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: How can common household drugs help?	3483
Atencion covid Estudio Contable Legal e Impositivo para tu negocio	1122
Coronavirus 'Stay home - earning big money home'	754
Aprovecha Productos COVID en Oferta!	514
Your exclusive health plan covers Covid-19 + other health expenses at Rs 8/day* | Know more.	479
Beantragen Sie Ihr Coronavirus Bounce Back Loan für 2% Jahreszins	443
Taller , Jornadas de trabajo y su Implementación Práctica y normas especiales covid 19	401
Bonus Covid: Polizza auto da 189€	364
Re: Corona virus Protection Pills.Order confirmation	336
Alle Belgen wekelijks testen op corona? Nog niet zo’n gek idee - Bouchez: ‘We vieren Kerstmis niet via Skype’ - Eerste groen voorstel zorgt al voor opstootje in meerderheid - Trump verschijnt voor het eerst sinds verkiezingsuitslag	317
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	317
Taller: Jornadas de Trabajo, su Implementación Práctica y Normas Especiales Covid 19	287
Re: Digital signage solution for Covid-19	284
Help to fight COVID-19 fever alarm security door	267
Contactless infrared body temperature thermometer defeat Coronavirus	255
Re: Defeat Coronavirus, non contact fever alarm device	253
Precios IMPACTO / Productos COVID 19	247
Let’s fight together to get through the COVID-19	246
Congratulation!!! You have been awarded United Nations Covid-19 funds	224
COVID-19 Support Donation	215
COVID-19 test before flight!	206
Donate to support. Fight Covid-19 together	192
Re: COVID-19 PAYMENT.	185
Covid -19 spende	176
Marketing during Covid19 - If You're Not Marketing, What's the Sense?	175

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	3487
stargoldmedics.com	1125
walla.co.il	1122
gmail.com	1110
126.com	1005
yeah.net	857
keyable.net	775
sihovision.com	713
seajin.chtah.com	527
quinnlncompanyltd.com	443

Top-15 IPs Sending COVID Spam

192.3.3.143	787
113.116.206.123	733
113.116.194.155	713
45.127.62.106	443
201.231.6.38	423
86.104.194.84	337
67.219.150.138	336
201.231.115.154	327
190.247.255.124	294
89.248.97.65	224

Top-15 Countries Sending COVID Spam

US	9256
IN	4513
CN	4056
FR	1551
AR	1181
DE	1032
IT	594
BE	590
ES	574
CL	524

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Tr : Coronavirus - Point de situation dans le Nord - 10 novembre 2020	2

Top-15 Subjects Containing doc/xlsx Files

COVID 19 WEB DIRETTA STREAMING CYBERSECURITY, COMPLIANCE e GDPR: perimetro nazionale sicurezza (in vigore dal 5/11/20) 15/12/20	23
Fw: CMCC-1281-2020 Shifting of Demand of instalments/ EMI in respect of elligible Term Loan Accounts marked for COVID-19 relief	7
El Colegio Mayor Universitario Marqués de la Ensenada instala una cámara termográfica para detectar alteraciones de temperatura de sus residentes frente al COVID- 19	4
Viguatur Portafolio de Servicios 2021 y Protocolo de Salud y Seguridad ante el Covid 19 2do Envio	4
MEDIA RELEASE [Ade Bajomo becomes President of FinTechNGR, says technology and innovation will drive Nigeria's baking sector post-COVID]	3
NV COVID Update 11/12	2
COVID-19 ■■■■▯ ■■■▯■■▯■■▯■ ■■■■■■■■■▯■■▯■■▯■▯ ■■■■■▯■■■ ■■ ■▯■▯■■■■■■■■■■■■▯■■▯■■ ■■■■■■▯▯■■▯■■■■■■▯■■▯■■▯Quotation ■■■■■▯■▯■▯■■▯ Specification ■■■■■■■■■■■▯■▯■■▯ ■■■■■■ G3	2
DifusiÃ³n Reglamento Interno y Anexo Covid-19	2
WIJ GRONINGEN CORONA NIEUWSBRIEF NR. 66	2
Déclaration des cas positifs COVID 19	2

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: 132,419
Domains with Potential Mail Servers: 2,654
Email-Capable Domains and Hosts: 50,390
Live Hosts and Domains Not Parked: 45,697

Mobile Apps

Apps in Official Stores: 475

by Store

Apple	241
Google	219
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,734

by Store Type:

Hybrid	910
Secondary	765
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1