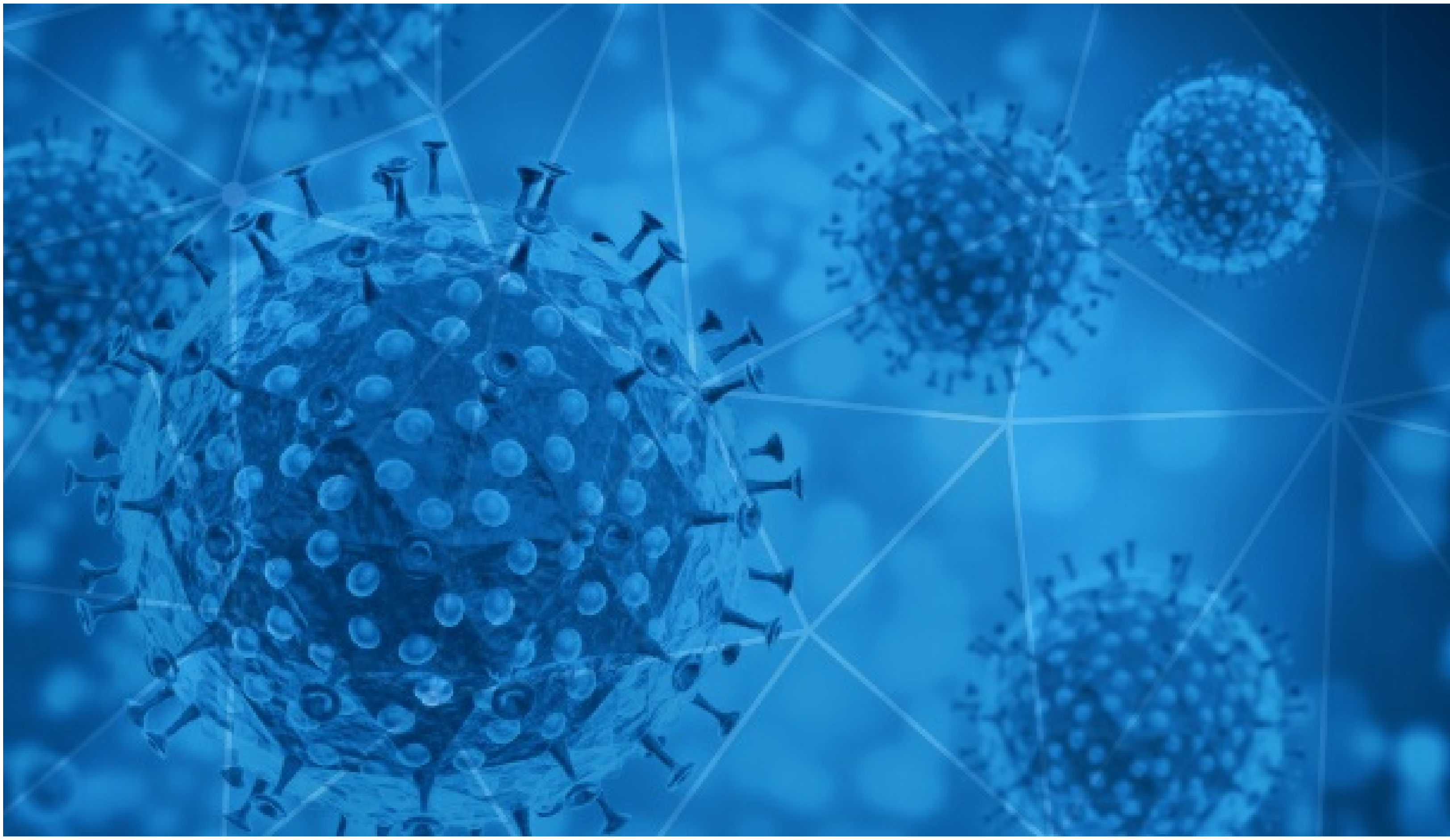
RiskIQ i3:

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

2021-02-26



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 2021-02-25 to 2021-02-26. During this period, RiskIQ analyzed 36,378 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,125 unique subject lines observed during the reporting period. The spam emails originated from 1,977 unique sending email domains and 3,928 unique SMTP IP Addresses. Analysts identified 2 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	11223
The Corona Letter: A single dose, half the task	3484
Retrogen is now performing diagnostic testing for COVID-19	2456
COVID-19 Financial Relief to receive your R30,400 government issued financial relief	1233
Coronavirus COVID-19 and the impact on car and auto auctions	1030
Equipos de limpieza, esterilización y desinfección de ambientes, elimina Covid, Bacterias, Moho, mal olor etc.	834
Línea de prendas médicas anti covid, especialmente fabricadas para sentirse cómodo todo el día.	752
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	686
COVID19 LOAN RELIEF OFFER / INVESTMENT	534
COVID -19 BENEFIT FUNDS	466
¡No dejemos de cuidarnos, Pruebas de detección Covid-19! | CLÍNICA SANENS	397
Re: Personal, SME & Business Relief [COVID-19]	396
[Free Recorded Webinar] Covid-19 is Turning Digitalization A Permanent Trend For All Global Sellers!	321
[GobizKOREA] Covid-19 K-Quarantine Mask Special pavilion	317
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	307
How COVID-19 has accelerated the need from an annual planning to an ongoing process	303
Gemeinsam gegen Corona	272
Pruebas Antígenas para COVID-19, Resultado en 15 Minutos, Envíos todo Perú.	264
[Spam]Your compensation $2,500,000.00, dou coronavirus(Covid-19).	220
Good Morning, SA | People are pretending to be health workers to get the Covid-19 jab, warns Western Cape health dept	200
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	197
Communications Hardware Global Market Report 2021: COVID-19 Impact and Recovery to 2030	160
Review of Coronavirus Food Assistance Program Continues	153
COVID -19 VÝHODNÉ FONDY	153
Ofertas Test Rapido Covid 19	145

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

giant-pw.com	11223
timesofindia.com	3484
retrogenmail.com	2456
standardbank.co.za	1233
govauctionn.cyou	1030
gmail.com	1012
mail2royal.com	686
yandex.com	656
tamsa.net.pe	435
public.govdelivery.com	433

Top-15 IPs Sending COVID Spam

207.38.83.47	2456
195.62.46.157	1030
103.212.120.21	671
72.15.201.15	626
198.38.84.190	532
79.189.61.109	518
103.225.52.190	483
78.88.190.206	463
190.187.107.74	435
190.187.111.88	399

Top-15 Countries Sending COVID Spam

JP	11323
US	9368
IN	4337
--	1615
PE	1592
PL	1039
CN	796
FR	599
DE	588
GB	569

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Communiqué de presse - COVID 19 - Arrivée du Vendée Globe à huis clos dans le cadre de l'urgence sanitaire le vendredi 26 février 2021	1
Latest Covid Safety related Products and Promotional Items.	1

Top-15 Subjects Containing doc/xlsx Files

UN Covid 19 Relief fund	6
WEB OnLine COVID 19 Appalti e subappalti: direzione e controllo, gestione cantieri e tutela dei lavoratori 25/3/21	5
UN Covid 19 Relief fund.	4
WEB COVID 19 Superbonus 110%: Legge Bilancio 2021, Circolare 30/E AdE, procedure per cessione bonus fiscale 11/3/21 4 CFP Odcec	3
Press release EY Forensics | COVID-19 headwinds heighten integrity challenges for emerging markets: EY'	3
DIPUTACION DE ALICANTE- Nota Incremento ayudas gasto social Covid	2
CORONA LANZA PLATAFORMA DE CATAS SENSORIALES INVITANDO A LOS MEXICANOS A DESCUBRIR Y DISFRUTAR DEL BRILLO DE LA MÁS FINA DESDE CASA	2
Україна взяла участь в Міжнародному форумі «Тренди медіа та тенденції реалізації Цілей сталого розвитку ООН в епоху пост COVID-19». Прес-реліз, фото, відео	2
02.03 DPS - KIEROWANIE, DOKUMENTACJA ELEKTRONICZNA,COVID, DOCHÓD, ODPŁATNOŚĆ, ZWOLNIENIA	2
Buletin de presa 25.02.2021 + comunicat actiuni COVID	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: 147,442
Domains with Potential Mail Servers: 2,557
Email-Capable Domains and Hosts: 53,721
Live Hosts and Domains Not Parked: 45,201

Mobile Apps

Apps in Official Stores: 515

by Store

Apple	255
Google	243
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,131

by Store Type:

Hybrid	1080
Secondary	983
Affiliate	68

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	26
Official	2
Hybrid	1