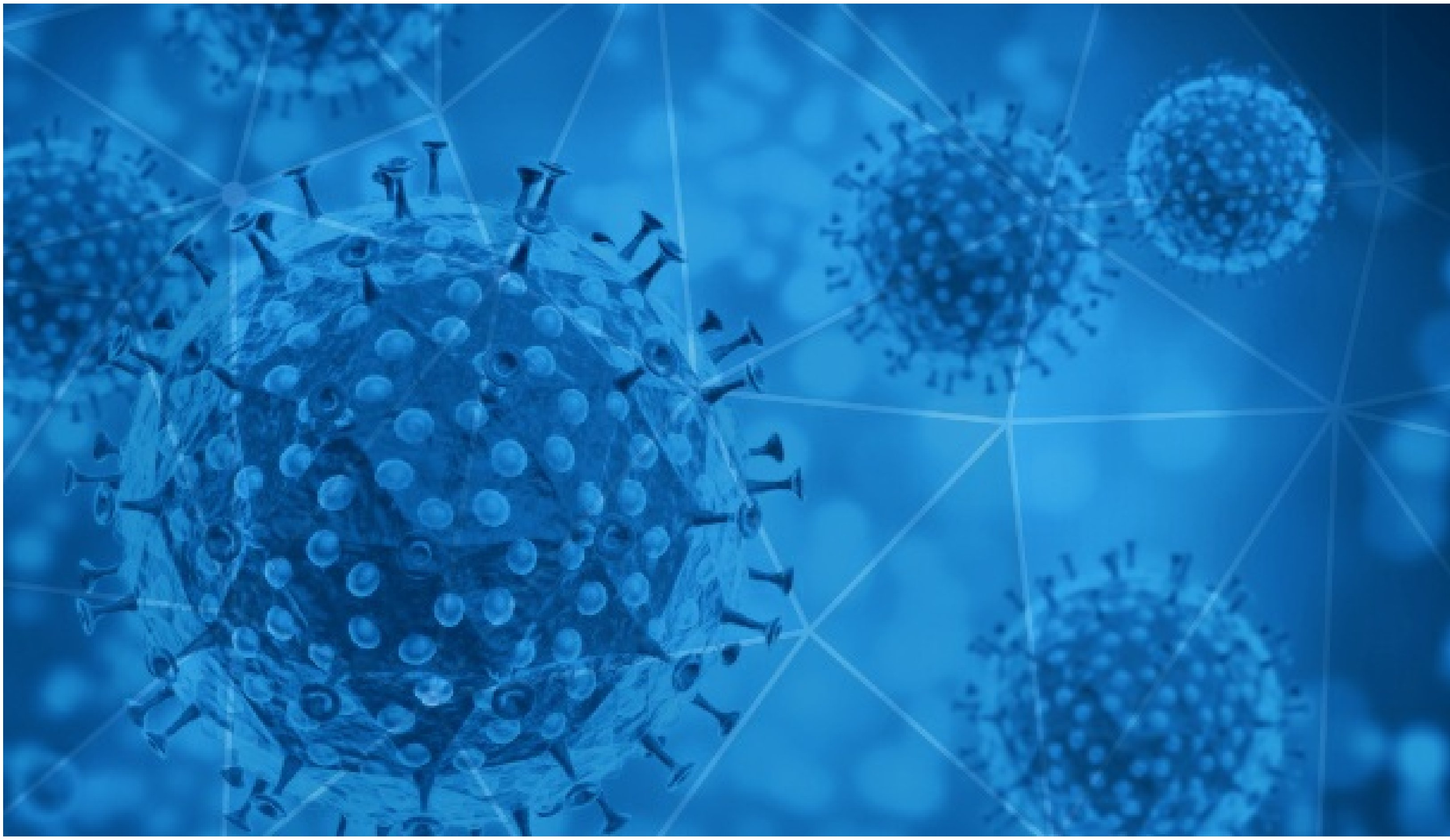
RiskIQ i3:

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

2021-03-17



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 2021-03-16 to 2021-03-17. During this period, RiskIQ analyzed 43,918 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,933 unique subject lines observed during the reporting period. The spam emails originated from 2,022 unique sending email domains and 3,793 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	13207
Corona Schnelltest	7064
Covid Schnelltest	3911
The Corona Letter: Understanding blood clots and correlation	3059
COVID-19 Financial Relief to receive your R35,400 government issued financial relief	1777
Box de dépistage Covid-19 disponibles sur les parvis de gares	436
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	379
BEST PRICE IN EUROPE - Nitrile Gloves | KN95 Face Mask | COVID-19 Products | DISCOUNT CODE#:684419775	304
Re: Digital signage solution for Covid-19	276
covid 19 financial support.	274
Covid19 Relief Fund	247
Equipos de limpieza, esterilización y desinfección de ambientes, elimina Covid, Bacterias, Moho, mal olor etc.	243
Live Webinar - EEOC & CDC Guidance for Employers Mandating COVID Vaccines at Work	232
Paneles de protección anti COVID-19	208
Gran Venta Outlet - Productos Covid 19	206
COVID-19 Update: We are open and now offering Free Virtual Consultations	203
ATTN Beneficiary(COVID-19 pandemic Essential Worker Support Program (EWSP) WorldWide.	177
Dealing with a Covid-19 related loss.	173
Coronavirus briefing: Camilla backs AstraZeneca	171
Re: covid-19 touch monitor	170
Covid19 Relief Payments	162
Re: Mashalat Capital Relief (COVID-19).	162
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove...etc.	160
Try our popular COVID-19 online learning course	156
Retrogen is now performing diagnostic testing for COVID-19	155

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

giant-pw.com	13209
gmx.net	10975
timesofindia.com	3074
standardbank.co.za	1777
126.com	446
newsletter.oui.sncf	436
pro-ahr1.com	404
163.com	404
medecongreateco.com	377
aol.com	373

Top-15 IPs Sending COVID Spam

78.47.93.254	6618
185.173.235.78	2996
85.144.35.137	1777
107.167.2.207	1061
103.225.54.102	737
103.225.55.205	531
103.225.54.80	525
103.225.54.186	478
103.225.55.188	421
103.225.53.165	405

Top-15 Countries Sending COVID Spam

JP	13301
DE	7618
US	7017
NL	5033
IN	3194
CN	1405
FR	1000
GB	847
CA	364
PE	327

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

El colegio Santurtzi Calasanz de Bizkaia implanta un sofisticado método de control del aire contra los contagios de Covid	5
BHP – obowiązki pracodawcy i pracownika w dobie covid-19	4
Liga Portuguesa Contra o Cancro divulga estudo sobre o impacto da covid-19 nos doentes oncológicos	2
Promocion Guatemala 2 x 1 promocion Post Covid.	2
Buletin de presa 16.03.2021 + comunicat actiuni COVID	2
Press Release: Takeda and IDT Support Manufacturing of Johnson & Johnsonâs COVID-19 Vaccine - Order# 52395652	2
COVID: NONOSTANTE CASO ASTRAZENECA, NON ARRETRA FIDUCIA SU VACCINI	1
Re: [MPALISTSERV] In office guidelines for COVID	1
positiver Corona Fall	1
REPORTE DE PERSONAL CON SISTOMAS O SOSPECHAS DE COVID-19 16 DE MARZO DEL 2021 EN CERVECERIA.	1

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: 149,995
Domains with Potential Mail Servers: 2,565
Email-Capable Domains and Hosts: 51,992
Live Hosts and Domains Not Parked: 46,082

Mobile Apps

Apps in Official Stores: 515

by Store

Apple	253
Google	245
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,201

by Store Type:

Hybrid	1123
Secondary	1010
Affiliate	68

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1