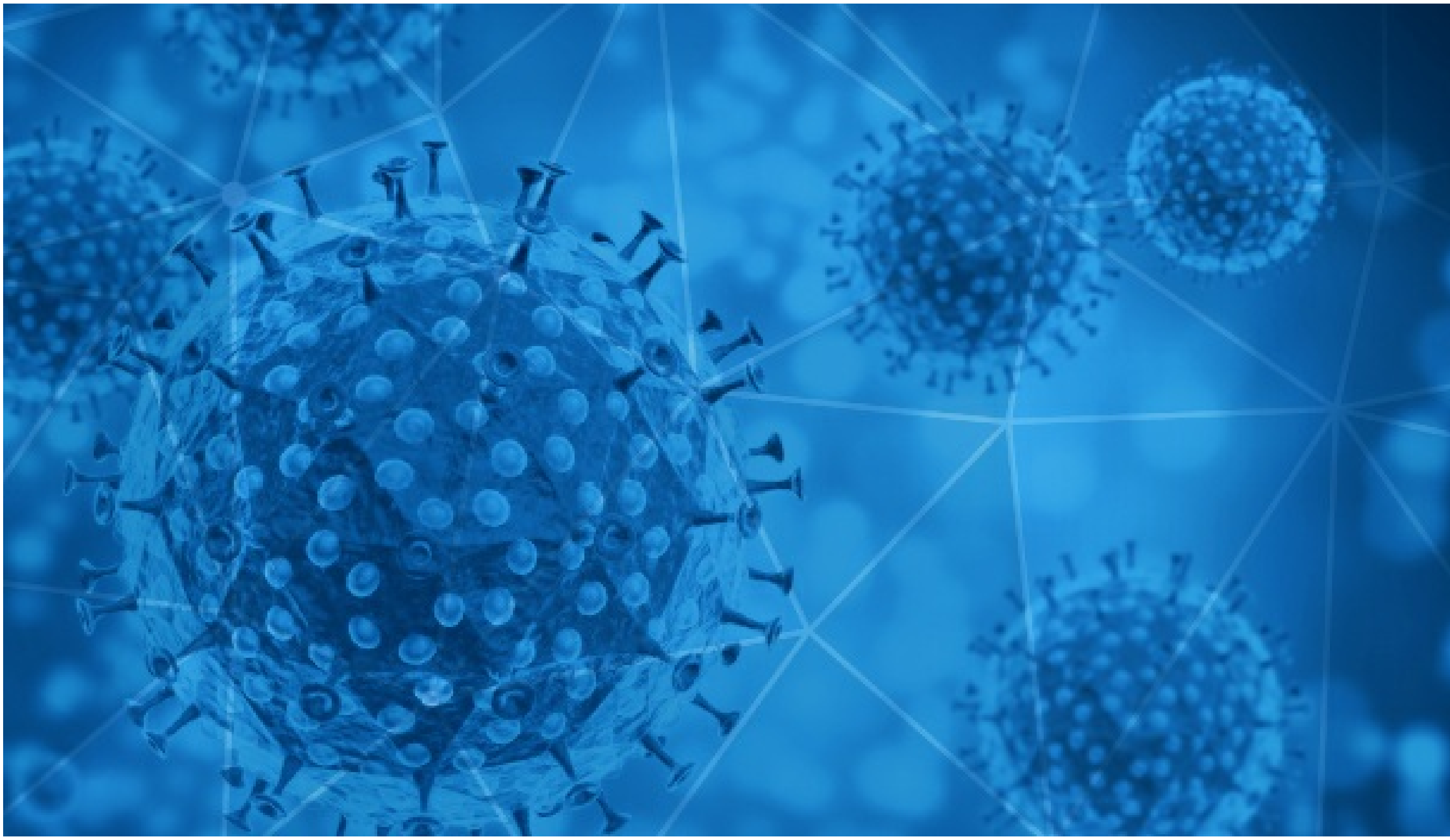
RiskIQ i3:

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

2021-04-19



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 2021-04-18 to 2021-04-19. During this period, RiskIQ analyzed 19,542 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 829 unique subject lines observed during the reporting period. The spam emails originated from 416 unique sending email domains and 1,215 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□	5986
Claim Your Fifty Dollar Pfizer COVID Vaccine Survey Reward	2824
Claim Your Fifty Dollar Pfizer COVID Vaccine Survey Offer	2716
Your Fifty Dollar Pfizer COVID Vaccine Survey Offer Is Waiting	2670
The Corona Letter: Why scientists say Covid is airborne	1706
COVID-19 Update: We are open and now offering Free Virtual Consultations	323
Plane makes emergency landing just feet from swimmers on busy beach+Feds suspend J & J COVID vaccine	253
Covid 19 Payment to you	172
COVID-19 PANDEMIC COMPENSATION FUND	138
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO ANTE EL COVID19	136
IMF COVID-19 FINANCIAL ASSISTANCE[3]	110
Corona zelftest: veilig snel en discreet!	92
Limpieza Preventiva COVID19	89
Re: Personal, SME & Business Capital Relief (COVID-19)	84
Hi, Your test for Covid IgG Antibody is fixed at Rs.449/- | Select your schedule.	73
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	72
Book your pre-flight COVID-19 test before you Go!	70
Aktuelle Corona-News für Unternehmer	63
"Werken met schrik voor je leven, is traumatiserend" - Meghan liet tóch van zich horen op begrafenis - K3 hekelt coronamaatregelen - 'Morning after pil' tegen corona in de maak	61
COVID-19 weekend lockdown: These states, cities to have restrictions from today, check complete list	51
Do you have Covid Antibodies ?	50
Re: Maslahat Mutual Relief (COVID-19).	44
Covid-19 Face mask (Stock)	44
RELIEF FUND - COVID 19 INVESTMENT LOAN!	36
✔ Testiranje na COVID-19 | Split, testiranje na COVID-19 | Antistres masaža -51% Centar | Ultrazvuk abdomena -50% Maksimir | Prvi ORL pregled s endoskopijom -30% | Depilacija -29% Trešnjevka | Oftalmološki pregled -43% Gajnice	35

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

antisoap.guru	8210
giant-pw.com	5987
timesofindia.com	1711
caribbeanfever.com	253
gmail.com	251
sampark.gov.in	229
protonmail.com	172
megalotintl.com	138
cmbmutualfunds.com	128
yandex.com	112

Top-15 IPs Sending COVID Spam

195.62.32.74	8210
103.225.55.235	417
103.225.53.30	287
103.225.52.109	271
103.225.52.197	239
103.225.55.234	195
103.225.52.37	185
103.225.52.169	183
103.225.53.127	174
103.225.53.245	163

Top-15 Countries Sending COVID Spam

RU	8253
JP	6132
IN	2001
US	1402
NL	273
AR	258
CN	158
GB	150
DE	150
PH	128

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

ANC Weekly COVID-19 Reports	6
covid report	2
CCS/11950 Suman más de 62 mil contagios de COVID-19 en el estado de Chihuahua	2
B JEFFERSON MANOR EMPLOYEE Covids	1
RE: Buenas noches Dra. Gloria Esperanza Enviamos consolidado deplanilla covid 21 de enero 2021	1
Fw: Ónodiné Csatos Erika covid pozitív kontakt gyermekek szüleinek küldendő dokumentum	1
CM Press Note Corona Guideline 18-04-2021	1
REPORTE DE COVID	1
Anexo II e III - Declaração de Veracidade (Covid- 19)	1
CV- na stanowisko konsultant Infolinii Narodowego Programu Szczepień przeciw COVID-19	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: 156,850
Domains with Potential Mail Servers: 2,525
Email-Capable Domains and Hosts: 48,935
Live Hosts and Domains Not Parked: 42,401

Mobile Apps

Apps in Official Stores: 525

by Store

Apple	262
Google	246
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,314

by Store Type:

Hybrid	1188
Secondary	1058
Affiliate	68

Blacklisted Mobile Apps: 31

by Store Type:

Secondary	28
Official	2
Hybrid	1