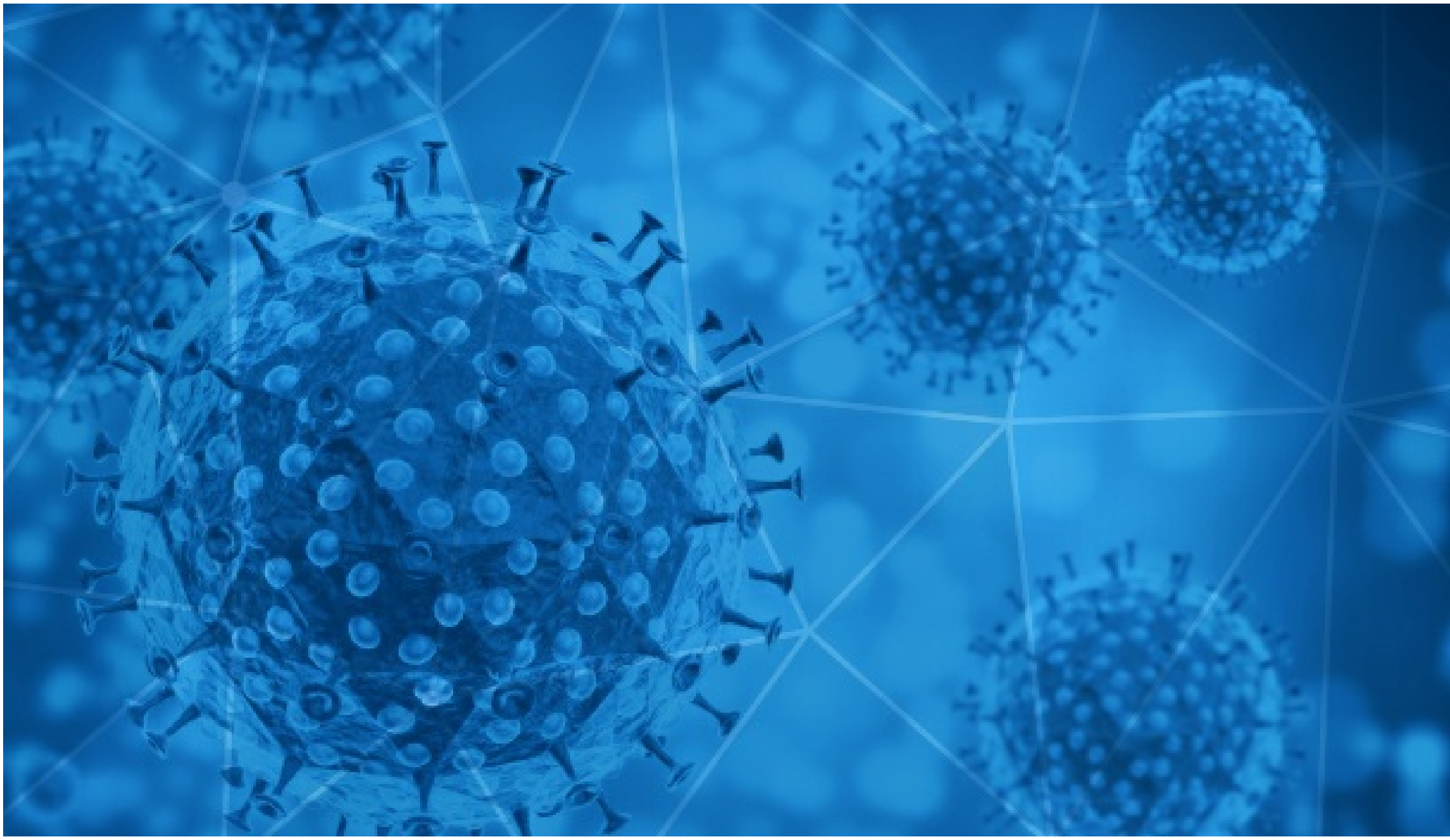
RiskIQ i3:

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

2021-04-05



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 2021-04-04 to 2021-04-05. During this period, RiskIQ analyzed 8,025 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 673 unique subject lines observed during the reporting period. The spam emails originated from 343 unique sending email domains and 617 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: What do 'adverse events' after vaccination mean?	1436
COVID-19 RELIEF FUNDS!!	1107
Recuperacion Efectiva de los Subsidios Laborales ante Essalud Post Covid19	603
UN Covid-19 Winning Notification obi	384
UN Covid-19 Winning Notification tob	381
Coronavirus passports to take 'months'	371
CONGRATS! You Can Get $50 Pfizer COVID Vaccine Survey Rewards	266
Your Fifty Dollar Pfizer COVID Vaccine Survey Offer Is Waiting	252
Congrats! You've Been Selected For $50 Pfizer COVID Vaccine Survey Reward	244
Confirmed: Your Fifty Dollar Pfizer COVID Vaccine Survey Reward	229
UN Covid-19 Winning Notification	198
COVID-19 RELIEF FUNDS!	177
UN Covid-19 Winning Notification z	121
Covid-19 Vaccination Awareness	117
Re: Mashalat Capital Funding & Relief (COVID-19).	112
(covid19) compensation	106
Engeland gaat deze maand coronapaspoort testen - Minihelikopter Ingenuity staat op Marsoppervlak - ‘Van Aert en Van der Poel zullen elkaar kunnen gebruiken’ - Jongeren bouwen feestje aan boord van trein: NMBS onderzoekt incident - Griekenland…	86
ATTN Beneficiary(COVID-19 pandemic Essential Worker Support Program (EWSP) WorldWide.	86
UN Covid-19 Winning Notification	73
Minister Says His COVID-19 Disappered in 3 Days	71
Covid19 Relief Fund	51
Re:Your Covid vaccine is approved for vacination	49
Seguro COVID19 para la construccion	40
COVID-19 Relief Fund, Please Send all Replies to benduke111@hotmail.com	37
✐ Vacunación Covid-19	34

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	1439
gmail.com	1377
netc.pl	1284
prostatee.us	991
euroavisos.com	603
email3.telegraph.co.uk	371
e2ma.net	165
cmbmutualfunds.com	151
publicbank.com.my	117
outlook.com	108

Top-15 IPs Sending COVID Spam

192.163.208.148	1320
195.62.46.153	991
221.123.163.87	905
103.18.244.112	325
120.89.46.62	112
130.248.205.95	111
195.62.15.242	106
219.65.85.17	93
130.248.205.97	93
219.65.85.20	90

Top-15 Countries Sending COVID Spam

US	2798
IN	1483
--	1172
CN	986
MY	442
PH	151
NL	123
BE	118
UA	108
CA	99

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

ANC Weekly COVID-19 Reports	7
Fwd: Covid and the economy	3
Fwd: CVASU COVID-19 Testing Lab report on 04/04/21	2
Re: Solicitud de activación ruta covid sospechosos covid rastreo	1
PEMEX INFORMA: Reporte de estado de salud de trabajadores y derechohabientes de PEMEX afectados por COVID-19	1
Covid -19 Vaccination notice	1
covid report	1
TODAY COVID 19 RTPCR REPORTS	1
Covid-19 Report Submitted For : AlHadethah Hospital	1
Coronaimpfung	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: 154,421
Domains with Potential Mail Servers: 2,545
Email-Capable Domains and Hosts: 50,395
Live Hosts and Domains Not Parked: 46,395

Mobile Apps

Apps in Official Stores: 525

by Store

Apple	262
Google	246
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,272

by Store Type:

Hybrid	1162
Secondary	1043
Affiliate	67

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1