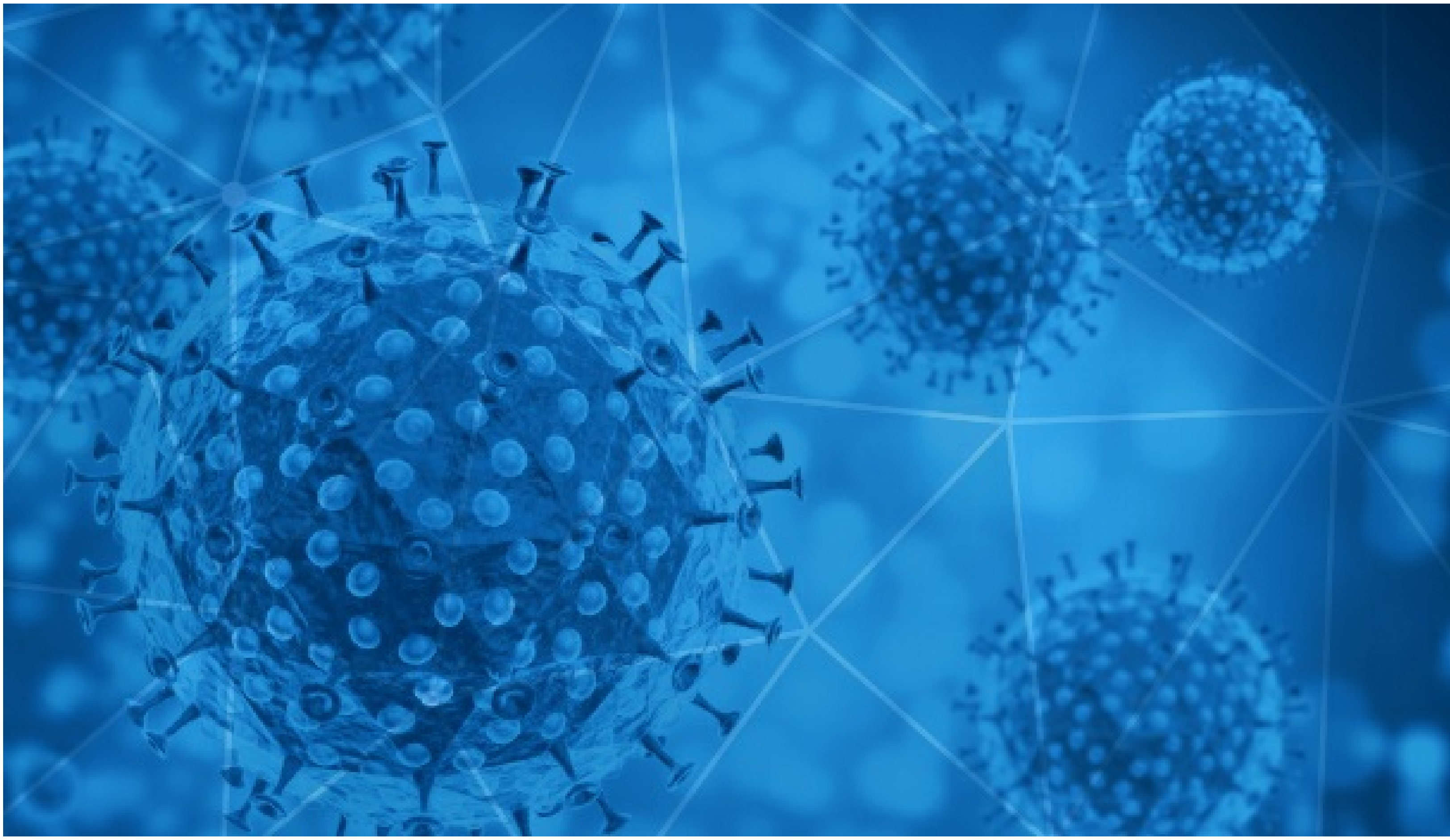
RiskIQ i3:

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

2021-04-13



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 2021-04-12 to 2021-04-13. During this period, RiskIQ analyzed 22,390 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,069 unique subject lines observed during the reporting period. The spam emails originated from 1,148 unique sending email domains and 2,360 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

Ordern Sie Coronatests im Direktversand	3522
Fino allï¿½ultimo paziente Covid-19	3475
Bundesweite Lieferung von Covid-Tests	3418
The Corona Letter: The latest on vaccine and blood clots	1639
TIMES TOP10: More export curbs as Covid surge continues	1532
COVID-19 Update: We are open and now offering Free Virtual Consultations	482
Fighting two pandemics: Corruption and the Coronavirus	374
IMF COVID-19 FINANCIAL ASSISTANCE PROGRAM[1]	354
Infórmate sobre la población excluida del Plan Nacional de Vacunación contra COVID19	313
Mandatory Covid-19 vaccination/Link is below	257
UN Covid-19 Winning Notification toc	218
All you need to know about “Double Mutant” COVID-19	192
Re:Your Covid vaccine is approved confirm date and time	182
Curso Gestión de los Riesgos Psicolaborales + Nuevo Módulo Covid 19	164
Covid19 Relief Fund	151
COVID, Outourcing y Teletrabajo.	134
Retrogen is now performing diagnostic testing for COVID-19	118
Onderwijs weer naar toestand van voor ‘paaspauze’ - Slecht slapen vergroot kans op covid-19 - Vooruit schuift twee nieuwe namen naar voor - Gele hesjes knippen vleugels van binnenlands vliegverkeer - Ondertussen in het vaccinatie-callcenter: ‘Tweede…	104
"Eén coronacijfer verontrust mij het meest" - Krijgen we 'versoepeling van het minste kwaad'? - Wees Gilles De Coster de mol gewoonweg aan?	94
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	93
Campaña Curso Gestión de los Riesgos Psicolaborales + Nuevo Módulo Covid 19	91
COVID-19 Relief Fund, Please Send all Replies to benduke111@hotmail.com	90
De vaccinspecial van De Standaard gemist? Alles over de grote sprong voorwaarts van de covid-vaccins	84
Fwd: COVID Behaviour change campaign - regarding	81
Seguro COVID19 para la construccion	80

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmx.net	6940
ediscomspa.com	3477
timesofindia.com	1648
bounce.indiatimes.com	1532
gmail.com	548
hospiramedical.co.uk	497
da.org.za	374
yandex.com	354
saludtotal.com.co	352
aol.com	260

Top-15 IPs Sending COVID Spam

78.142.61.111	2310
185.53.169.61	1769
64.32.22.114	1634
95.154.219.194	1154
94.102.151.42	399
79.139.57.248	392
200.31.17.85	352
94.102.147.138	331
94.102.149.226	313
130.193.83.66	292

Top-15 Countries Sending COVID Spam

US	5160
IT	3540
IN	3412
BG	2311
DE	2223
GB	1345
CN	584
PL	514
AR	489
FR	356

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

COVID 19 Vaccination - Information aux médecins Libéraux du Sud Gironde	1

Top-15 Subjects Containing doc/xlsx Files

Document COVID-19 Self declaration form.docx has been completed	28
ΜΕΤΡΑ ΣΤΗΡΙΞΗΣ ΑΝΕΡΓΩΝ ΣΤΟ ΠΛΑΙΣΙΟ ΤΗΣ ΠΑΝΔΗΜΙΑΣ ΤΟΥ COVID-19	7
La Covid 19 dispara como nunca el aprendizaje del inglés e incrementa el interés por el chino	4
UN Covid 19 Relief fund.	2
Covid-19-371948508	1
Press release- Central Bank Of India launches Special Deposit Scheme for COVID 19 jab.	1
CO Introduzione treni Covid Free - AV FR 9618 e 9653	1
VACUNAS CONTRA EL COVID-19	1
COVID - UPDATES NAIROBI AND MOMBASA.xlsx	1
PERMOHONAN MAKLUMAT PUSAT JUGAAN OKU BAGI PROGRAM IMUNISASI COVID-19 KEBANGSAAN	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: 155,649
Domains with Potential Mail Servers: 2,545
Email-Capable Domains and Hosts: 49,742
Live Hosts and Domains Not Parked: 43,039

Mobile Apps

Apps in Official Stores: 525

by Store

Apple	262
Google	246
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,293

by Store Type:

Hybrid	1176
Secondary	1049
Affiliate	68

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1