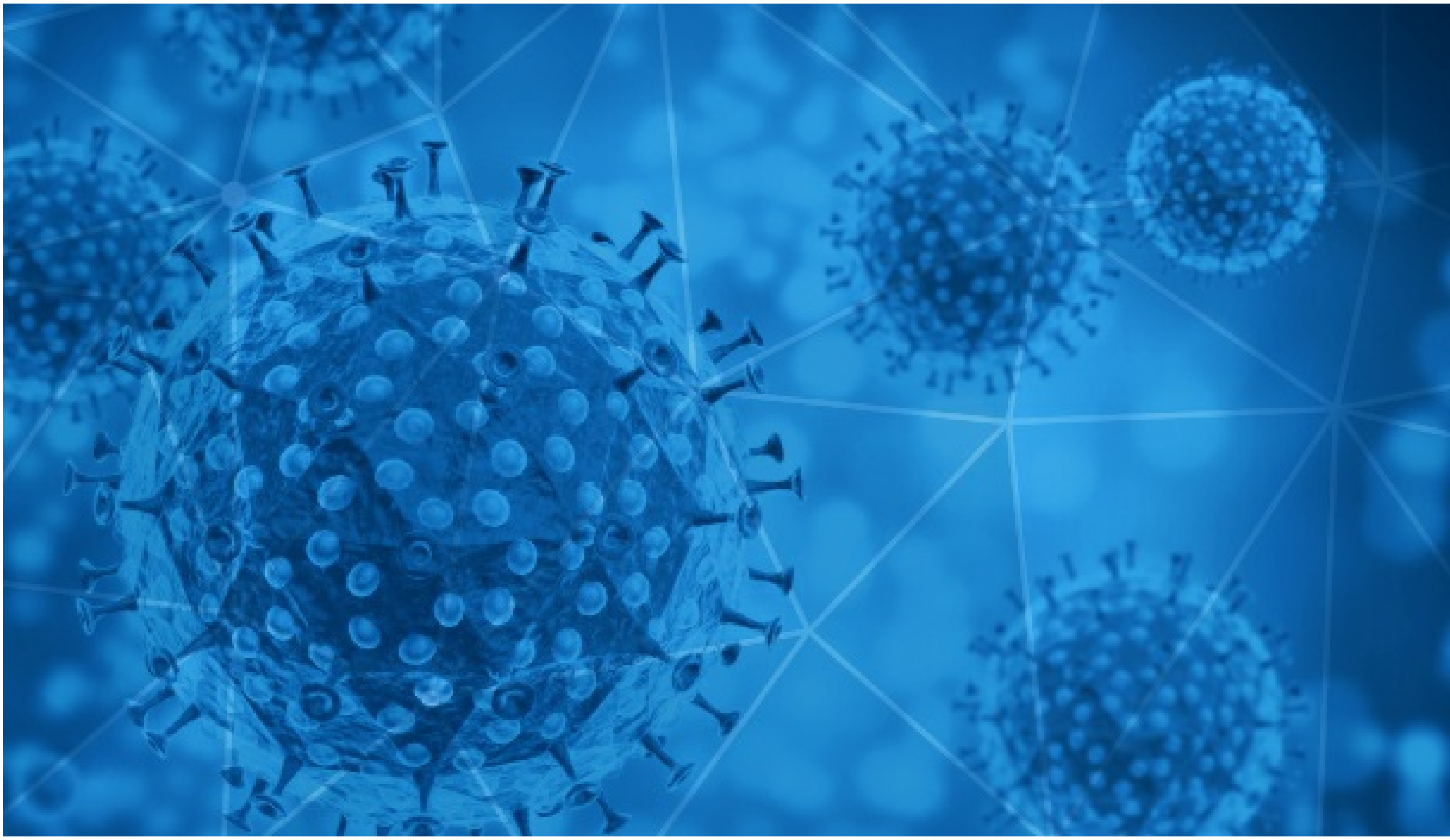
RiskIQ i3:

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

2021-03-31



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

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 2021-03-30 to 2021-03-31. During this period, RiskIQ analyzed 22,674 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,378 unique subject lines observed during the reporting period. The spam emails originated from 1,185 unique sending email domains and 2,657 unique SMTP IP Addresses. Analysts identified 14 emails which sent an executable file for Windows machines.

Top-25 Subjects

Fino allï¿½ultimo paziente Covid-19	3758
Good news about COVID-vaccine eligibility, what America's obsession with wipes is doing to sewer systems, and more from Apple News	2939
{COVID-19} □□□□□□□□□□□□□□□□□□	2772
The Corona Letter: Children are the next vaccination frontier	1793
COVID 19 RELIEF FUND / LOAN (INVESTMENT) FOR redacted@threatwave.com	1237
- Covid Relief Donation -	731
(covid19) compensation	469
Recuperacion Efectiva de los Subsidios Laborales ante Essalud Post Covid19 -8 y 9 de Abril	360
Arma tu kit para tus colaboradores y clientes contra el Covid	278
TOSCANA, FIRENZE: sostegno della ripartenza in sicurezza delle MPMI della città metropolitana di Firenze a seguito dell'emergenza sanitaria Covid-19 - Anno 2021	232
Public Relation Facebook Covid-19 Lottery Department	232
SEMANA SANTA Y PASCUA: AplicaciÃ³n Prueba COVID-19	221
RE: COVID-19 RELIEF FUNDS	216
Minister Says His COVID-19 Disappered in 3 Days	212
Hello redacted@threatwave.com, Test Covid al mejor precio del mercado. Desde 4,95 euros. Envio inmediato.	175
Re:Your Covid vaccine is approved for vacination	165
YOUR COVID-19 STIMULUS PACKAGE WORTH..	158
Liquidación de Productos Covid -19	155
Seguro COVID19 para la construccion	126
COVID-19 Relief Fund, Please Send all Replies to benduke111@hotmail.com	115
Coronavirus Pandemic Winning Award (COVID-19).	101
COVID19 LOAN / BOND INVESTMENT OFFER	99
NCJ Daily - HumCo's 36th COVID Death. Volunteers Needed for Vax Effort. Local Response Tops $11 Million. Stand-up Via Zoom.	98
Check the availability of appointment for Covid Antibody IgG test starting at just Rs 449/-.	97
COVID-19 Grant!	89

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

ediscomspa.com	3758
insideapple.apple.com	2940
giant-pw.com	2773
gmail.com	2600
timesofindia.com	1793
aiusm.com	732
flowja.com	469
paisperu.com	360
correosmasivos.cl	278
163.com	246

Top-15 IPs Sending COVID Spam

157.245.42.150	1996
212.200.239.162	731
195.62.15.242	469
103.225.53.79	321
130.193.88.154	296
109.109.248.226	288
213.95.200.221	246
67.219.150.138	245
95.172.22.234	244
190.237.114.173	241

Top-15 Countries Sending COVID Spam

US	8258
IT	4032
JP	2794
IN	2022
RS	731
FR	566
UA	475
DE	411
CN	364
BR	310

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Subject: Mandatory Covid-19 vaccination/Form is attached	8
Mandatory Covid-19 vaccination/Form is attached.	6

Top-15 Subjects Containing doc/xlsx Files

COVID 19	3
COVID-19: +22% riscaldamento in Italia per l’home working - lo studio di tado°	2
szczepienia p/covid-19 (Pilne)	2
Correction Covid 19 #SoldTo: 11001904	2
Correction Covid 19 #SoldTo: 11001916	2
Correction Covid 19 -SoldTo: 6150333	2
RE: REPORTE COVID PEDREGAL	1
Draft--List of employees for --proposed -- Routene Covid Test - 2021 list--APRIL-2021	1
[TEP] TEP o gospodarce - Skuteczna walka z COVID wymaga zaufania a tego brakuje	1
FW: COVID Update	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: 154,131
Domains with Potential Mail Servers: 2,550
Email-Capable Domains and Hosts: 51,044
Live Hosts and Domains Not Parked: 43,357

Mobile Apps

Apps in Official Stores: 520

by Store

Apple	257
Google	246
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,263

by Store Type:

Hybrid	1158
Secondary	1038
Affiliate	67

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1