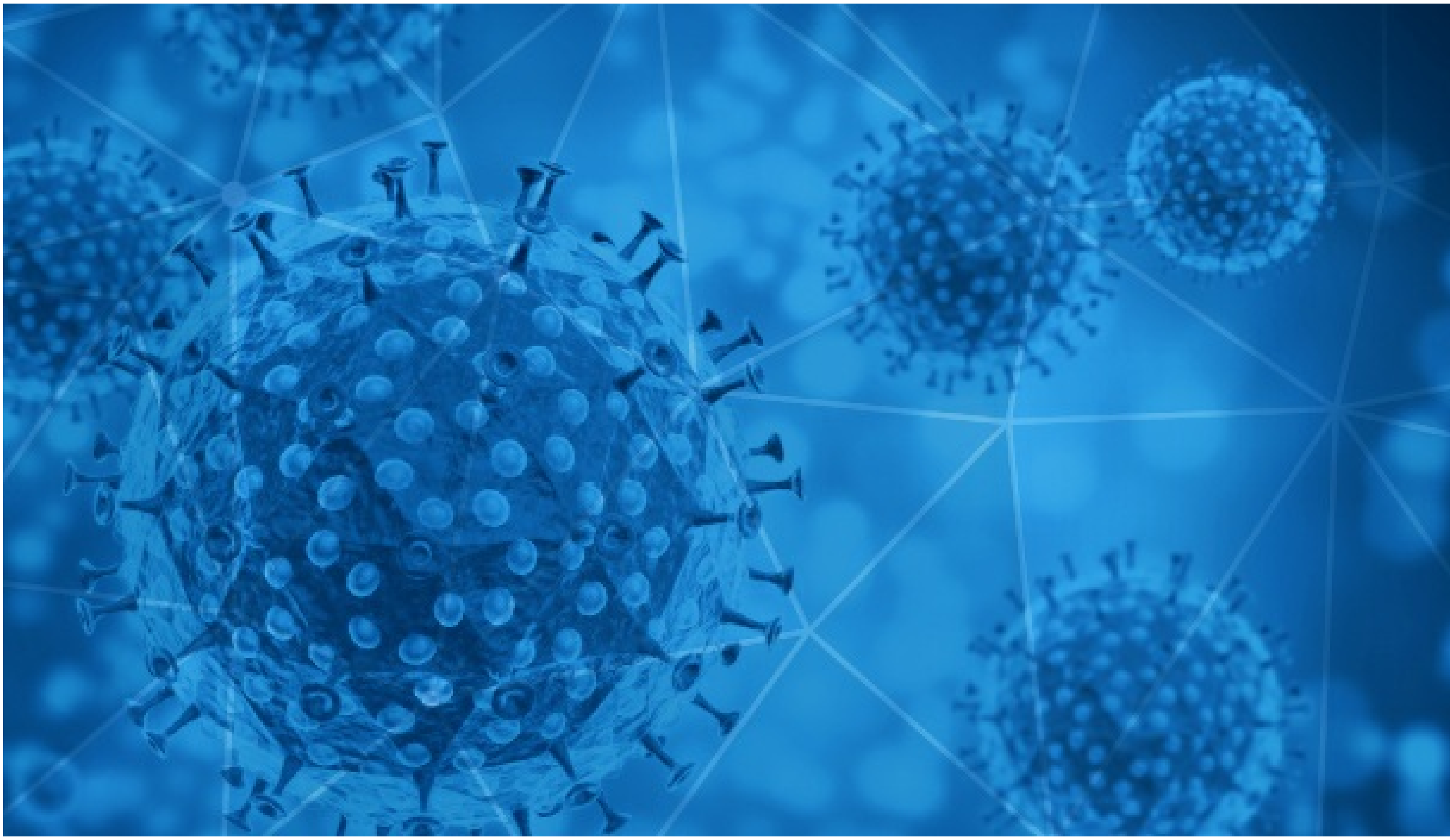
RiskIQ i3:

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

2021-02-03



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 2021-02-02 to 2021-02-03. During this period, RiskIQ analyzed 33,188 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,444 unique subject lines observed during the reporting period. The spam emails originated from 2,229 unique sending email domains and 4,085 unique SMTP IP Addresses. Analysts identified 71 emails which sent an executable file for Windows machines.

Top-25 Subjects

What's next for coronavirus relief, inside the lives of the First Dogs, and more from Apple News	5227
The Corona Letter: Pneumococcal vaccine matters	3922
COVID TASTE RESULT	2518
Public Relation Facebook Covid-19 Lottery	1973
Your Ultimate Protection against COVID-19. US FDA Registered	1716
European Union Compensation Funds for Covid19 Victims	1580
COVID-19	464
_Step_Closer_To_FDA_ Approval_ 20 People_Take COVID19_ PILL!	393
COVID-19 Pantallas Protectoras	325
TermoScanner e strumenti DPI Anti-Covid in pronta consegna con sconti oltre il 50% e prezzi a partire da Euro 49,00. Non Abbassiamo la guardia!!!	291
UN Covid-19 Winning Notificationw	285
Facebook Giveaway (Covid-19)	240
Attorney Update from Covid19	221
Coronavirus COVID-19 and the impact on car and auto auctions	215
Preenchimento do Formulário COVID no Sistema PDDE Interativo	198
Equipamentos de Proteção Individual (EPI's COVID 19)	189
CE FDA 510K GLOVES covid-19 Vaccine ,back to me	172
covid-19 lottery relief award(Congratulations)	170
Covid-19 : quels diabétiques sont les plus à risque d’une forme grave ? | Couleur, odeur, clarté : que dit l'urine sur notre santé ? | Quand faut-il laver (ou pas) les pommes de terre épluchées ? |	168
HNA Group: el gigante turístico chino va a la quiebra / ¿Qué van a querer los consumidores en la era posCovid?	159
Your new COVID19 Benefit card is on the way !	158
Good Morning, SA | New Level 3 regulations, Dlodlo summoned over SSA, SA Covid strain detected in UK in people with no travel history	154
Mi seguro insumos covid 19 protege a tu familia	151
□□□□□□□□□□□□□COVID-19□□□ <□□□□□□□□□□□□□□□□>	150
Pruebas Rápidas para Descarte COVID-19, Envíos a Todo Perú.	148

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

insideapple.apple.com	5322
timesofindia.com	3928
gmail.com	3743
vivaldi.net	1973
aol.com	1766
yandex.com	908
163.com	706
herculist.com	391
mailinator.cl	325
livejob.it	293

Top-15 IPs Sending COVID Spam

115.238.247.228	2518
87.248.52.51	1580
59.152.229.114	1112
110.186.72.61	567
216.87.190.231	392
192.81.210.244	381
111.20.159.210	307
185.221.173.42	293
219.65.85.25	284
219.65.85.34	274

Top-15 Countries Sending COVID Spam

US	12763
CN	4724
IN	4148
IT	2296
FR	1815
HK	1135
GB	807
KR	573
RU	466
DE	463

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Healthy Driven | One of the most baffling aspects of COVID-19, and more	20
02-02-21 - fiche réflexe gestion cas de Covid-19 actualisée	1

Top-15 Subjects Containing doc/xlsx Files

COVID 19 WEB ON LINE ANTICORRUZIONE E TRASPARENZA: proroga al 31/03/2021 del PTPCT – 24/02/2021	14
ECONOMIC AND SOCIAL COUNCIL (UN ECOSOC FIGHT FOR CORONA VIRUS PANDEMIC / 2020)	13
حزمة دعم الأعمال الصغيرة خلال فترة COVID-19	4
Sabato e domenica riparte lo screening anti-Covid alla stazione di Portanuova	3
Enfermería aplaude el carácter retroactivo de la norma que reconoce el COVID-19 como enfermedad profesional al incluir a las más de 80.000 enfermeras que ya se han contagiado	2
IRS Filing Season and COVID-19 Updates - February 2, 2021	2
Covid19 Test Ecourier Kit Manifest (Home) Northern Ireland Mail Centre	2
covid-19.docx	2
Tarifa Especial Productoras Test Covid-19	2
Fwd: CVASU COVID-19 TESTING LAB REPORT on 02/02/21	2

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: 141,120
Domains with Potential Mail Servers: 2,562
Email-Capable Domains and Hosts: 51,189
Live Hosts and Domains Not Parked: 43,962

Mobile Apps

Apps in Official Stores: 510

by Store

Apple	252
Google	241
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,068

by Store Type:

Hybrid	1058
Secondary	943
Affiliate	67

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1