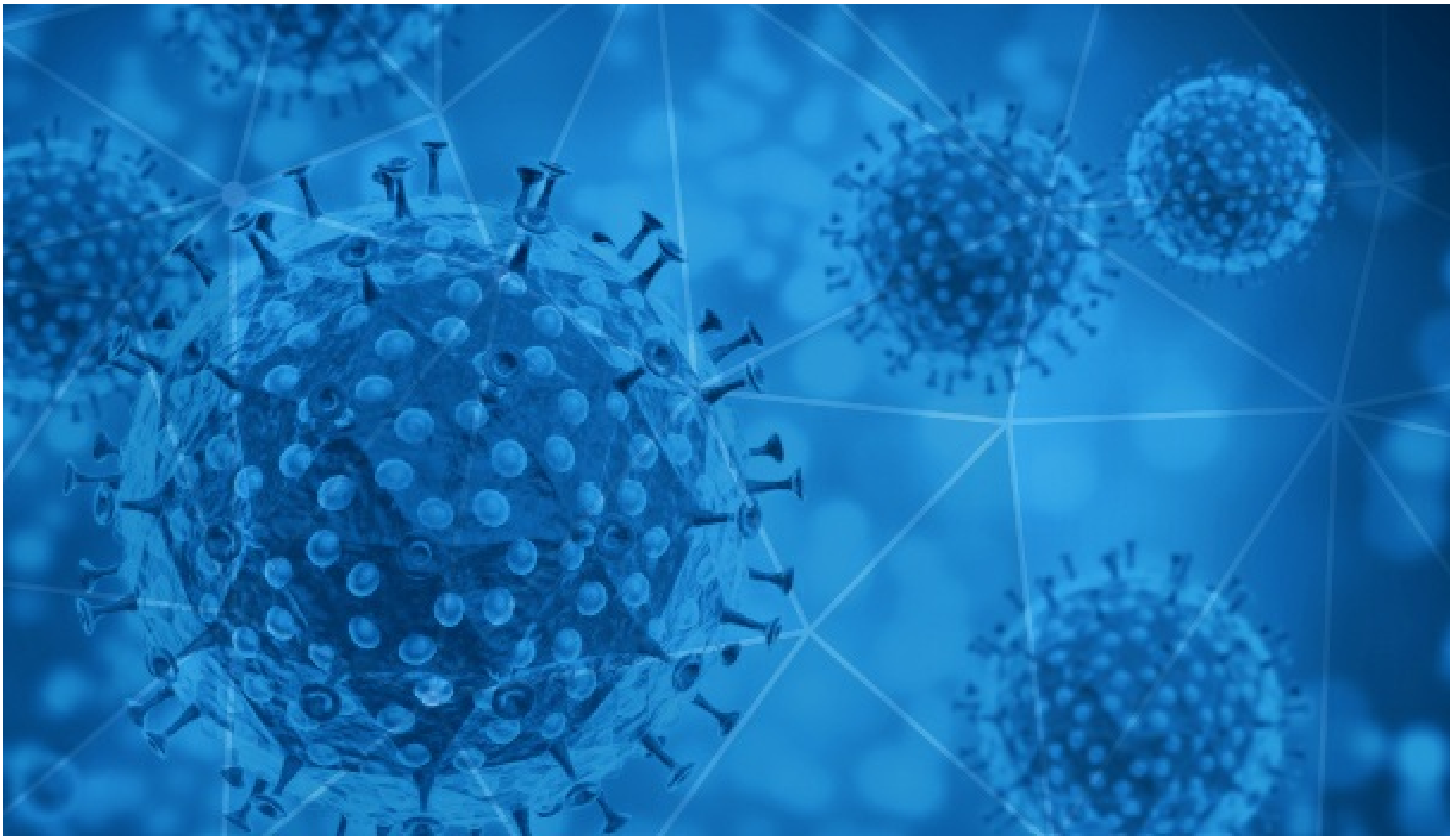
RiskIQ i3:

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

2021-02-16



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 2021-02-15 to 2021-02-16. During this period, RiskIQ analyzed 41,957 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,860 unique subject lines observed during the reporting period. The spam emails originated from 1,657 unique sending email domains and 3,313 unique SMTP IP Addresses. Analysts identified 10 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□□□	19026
Covid19 Relief Fund	4928
The Corona Letter: Was the Covid outbreak in Wuhan worse than expected?	3876
[USA L00] Covid-19 means Supervision is more in demand than ever.	2076
Re: Corona virus Protection Pills.Order confirmation	335
Test zur Erkennung von COVID-19 Antigen und Antikörper zum besten Preis an	309
(□□)□□□□19(COVID-19)□ □□ □□□□□□□□□□□□□ □□□□□□	309
UN Covid-19 Winning Notificationw	301
A Covid update for our stores across the country	297
Re: These new sterilizers with combination of strong UVC radiation and photocatalysis can really kill Covid	231
TermoScanner e strumenti DPI Anti-Covid in pronta consegna con sconti oltre il 70% e prezzi a partire da Euro 39,00 + spedizione gratuita. Non Abbassiamo la guardia!!!	226
KN95 Masks Are The Reason COVID19 Virus Is Being Curved, Stock Up Today While Supplies Last	188
Lo que necesitas saber sobre las vacunas contra la COVID-19.	157
Waarom doemberichten over corona u doen afhaken - Hoe we van vrieskou naar 16 graden gaan in één week - ‘Vijftien jaar na onze scheiding trouwden we opnieuw’ - Voorzichtig met droogblazers en haardrogers: nieuwe adviezen voor kappers, scholen en…	149
COVID-19 RELIFE FUND NOTIFICATION.REF/MX 303583	146
ProbarÃin en Harvard estrategia de mexicanos para tratar pacientes con COVID-19	141
Re: Mashalat Capital Relief (COVID-19).	136
Re: covid-19 touch monitor	115
Re: Personal, SME & Business Relief [COVID-19].	108
Job : for EDI Developer with Seeburger experience in Jackson, MI (Remote till Covid or post that also depending upon the situation) |	108
Your Ultimate Protection against COVID-19. US FDA Registered	102
□Tapabocas Corporativos desde $1.900 la unidad 😂 Ganemos la Batalla contra el COVID 19□	100
You're invited! News24 Frontline | Covid-19 vaccines	97
Covid19-Darlehensprogramm	93
COVID-19 Update: We are open and now offering Free Virtual Consultations	90

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

giant-pw.com	19029
gmail.com	6335
timesofindia.com	3876
usab2bmail.com	2207
moststablecoin.com	335
compratest.es	309
onecard.eid.co.nz	297
vui-inc.us	262
cmbmutualfunds.com	244
livejob.it	243

Top-15 IPs Sending COVID Spam

59.12.54.10	4926
184.175.86.164	2207
103.225.54.240	567
103.225.53.93	565
103.225.54.26	476
103.225.54.230	458
157.245.42.150	449
103.225.52.158	405
103.225.52.223	399
103.225.52.4	396

Top-15 Countries Sending COVID Spam

JP	19110
US	6957
KR	5270
IN	4043
FR	665
CN	581
IT	534
GB	504
DE	475
NZ	428

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Pfizer-BioNTech COVID-19 VACCINES UPDATE	3
COVID-19 Update	2
Pfizer-BioNTech Covid-19 Vaccines First Interim	1

Top-15 Subjects Containing doc/xlsx Files

Correction Covid 19	11
Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	3
IMSS FOTO NOTA.- Personal de enfermería del IMSS participa en vacunación contra COVID-19 para adultos mayores en Ciudad de México	3
Changes to pool and fitness room covid rules	3
UN Covid 19 Relief fund.	2
NP cribados covid 6 municipios esta semana	2
PR - A CLEANING TECHNOLOGY BREAKTHROUGH IN THE FIGHT AGAINST COVID PANDEMIC	2
RV: Encuesta Covid-2019 Vacuna	2
NP-Un nuevo equipo de profesionales en salud viaja a la región Áncash para reforzar respuesta en salud ante la COVID-19	1
Welcome to Southeast Point of Distribution (POD) for COVID-19 Vaccines	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: 143,902
Domains with Potential Mail Servers: 2,578
Email-Capable Domains and Hosts: 52,295
Live Hosts and Domains Not Parked: 44,713

Mobile Apps

Apps in Official Stores: 514

by Store

Apple	255
Google	242
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,095

by Store Type:

Hybrid	1069
Secondary	959
Affiliate	67

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1