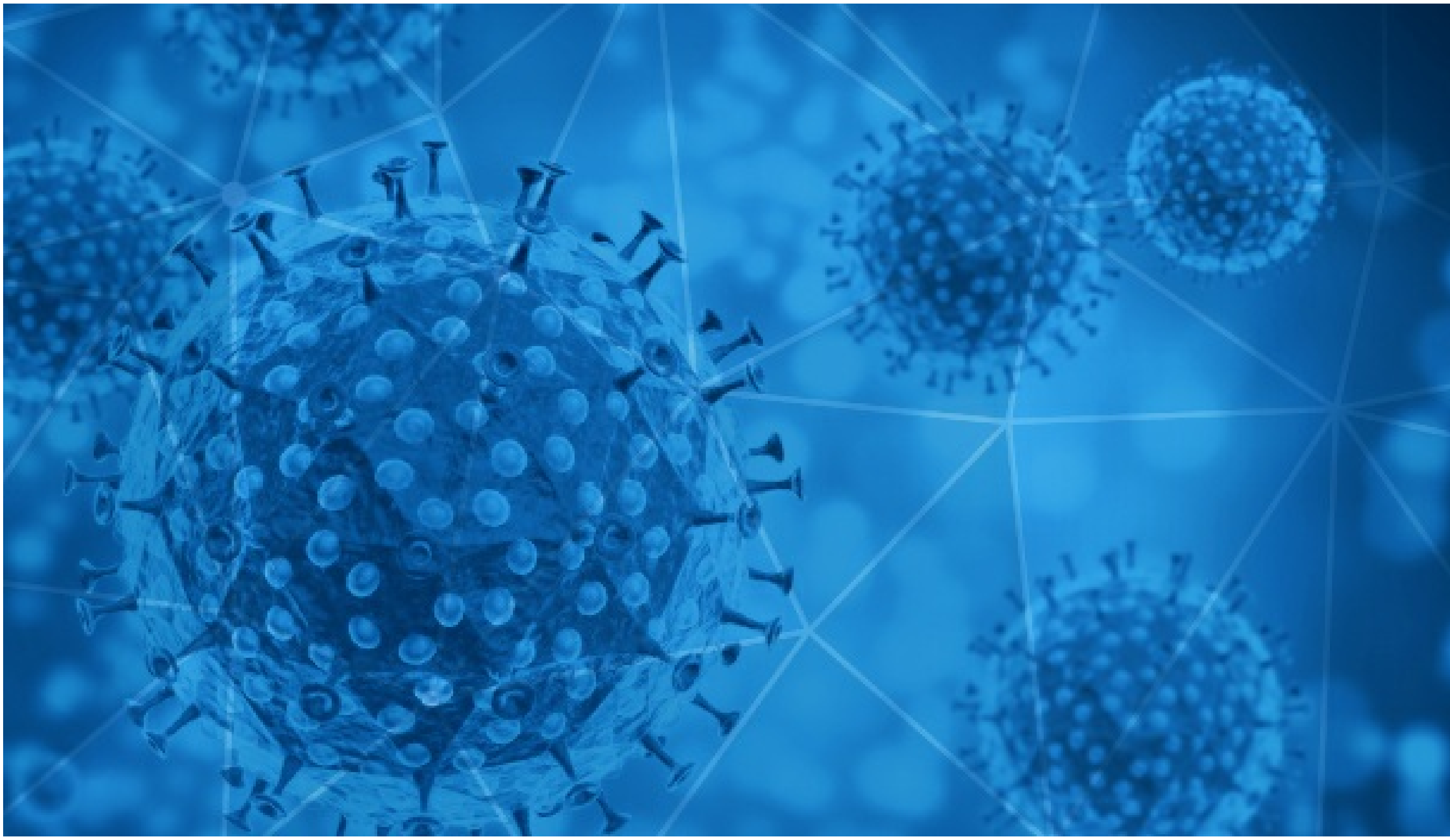
RiskIQ i3:

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

2020-12-31



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

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 2020-12-30 to 2020-12-31. During this period, RiskIQ analyzed 50,593 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,871 unique subject lines observed during the reporting period. The spam emails originated from 1,702 unique sending email domains and 3,594 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□	21863
New coronavirus variant detected in U.S., McConnell blocks vote on stimulus checks, and more from Apple News	4421
The Corona Letter: A year of living with Covid-19	4211
Puricador y Sanitizador de Aire, Estirilización contra Coronavirus	1829
Help the world's response to Covid-19 with the most protective mask on the market.	1354
Wearing a KN95 mask is your best defense against coronavirus	1344
Surviving COVID-19	657
Todo En Insumos Covid 19	561
Let’s fight together to get through the COVID-19	520
Flu/Covid-19 Weekly questionnaire - Reminder 1	295
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	292
Oferta de préstamo Covid-19	289
Offering N95 FACE MASK (3M 1860,1860S, Makrite 9500 N95,N95S,HARLEY, SAMPLING SWAB AND TUBE KITS,Novel Coronavirus (COVID-19) Test ,quick delivery in a couple days	289
Pruebas rápidas de COVID-19	268
Fake news about COVID-19 is spreading faster than virus	231
Covid-19 Relief Grant	221
Bemoedigend coronanieuws: 14,4 procent Belgen heeft antistoffen én we verplaatsten ons weinig in kerstperiode - Wat met dubbele dosis coronavaccin, wanneer bent u aan de beurt en wat als u twijfelt?	210
Formati per la trasformazione digitale post Covid	204
Re: Personal, SME & Business Relief [COVID-19]	199
Promoción Insumos Covid-19 Especial Para Empresas	183
How You Can Stop COVID Lies From Spreading	167
Good Morning, SA | Lockdown support from business groups, Covid strikes Zuma's lawyer	166
SBA Extends COVID-19 Economic Injury Disaster Loan Application Deadline through Dec. 31, 2021	157
Re:□coronavirus civil mask / Chinese qualified manufacturer	150
NJ COVID-19 Updates	144

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

epc-store.com	21867
insideapple.apple.com	4422
timesofindia.com	4211
perpetualincome.buzz	2698
grupocorreomasivo.com	1813
gmail.com	902
163.com	725
rhbgroup.com	657
mailinator.cl	577
public.govdelivery.com	379

Top-15 IPs Sending COVID Spam

195.62.32.18	2698
103.225.55.188	726
103.225.52.109	716
103.225.52.173	679
103.225.55.84	601
103.225.55.242	551
51.83.246.189	547
103.225.54.213	540
51.83.246.190	527
51.83.246.191	525

Top-15 Countries Sending COVID Spam

JP	22118
US	11006
IN	4388
RU	3095
FR	2728
CN	1635
GB	1071
SG	809
IT	461
BE	409

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

FW: Updates to COVID-19 related-matters	1

Top-15 Subjects Containing doc/xlsx Files

COVID-19 - Testes rápidos de saliva da Biojam disponiveis a partir de hoje	9
Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	8
IMSS Boletín 869.- IMSS prevé concluir en enero vacunación contra COVID-19 a trabajadores de la salud que atienden pandemia (FOTOS)	4
Positive Case of COVID-19: Summitview Elementary	3
COVID-19 Vaccine	3
Spending Bill’s Bankruptcy Provisions Target Some Covid-19 Woes	3
Правителството отпусна още 125 милиона лева за ваксини срещу COVID–19	3
CCS/10983 Suma Chihuahua 45 mil 900 casos confirmados y 4 mil 225 defunciones por COVID-19	2
Η Περιφέρεια Κρήτης στήριξε τους ελέγχους ταχείας ανίχνευσης αντιγόνου Covid-19 (rapid test) μέσα από αυτοκίνητο (drive through), που έγιναν σήμερα στο Ηράκλειο (βίντεο και φωτο)	2
ÖNEMLİ!!!!! Diş Hekimi Muayenehanelerinde Çalışan Sağlık Personeli ve Diğer Personel Listesi (Covid-19 Aşı Planlaması Hk.)	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: 137,955
Domains with Potential Mail Servers: 2,579
Email-Capable Domains and Hosts: 52,542
Live Hosts and Domains Not Parked: 49,519

Mobile Apps

Apps in Official Stores: 499

by Store

Apple	244
Google	239
WindowsPhone	15
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,968

by Store Type:

Hybrid	1010
Secondary	898
Affiliate	60

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1