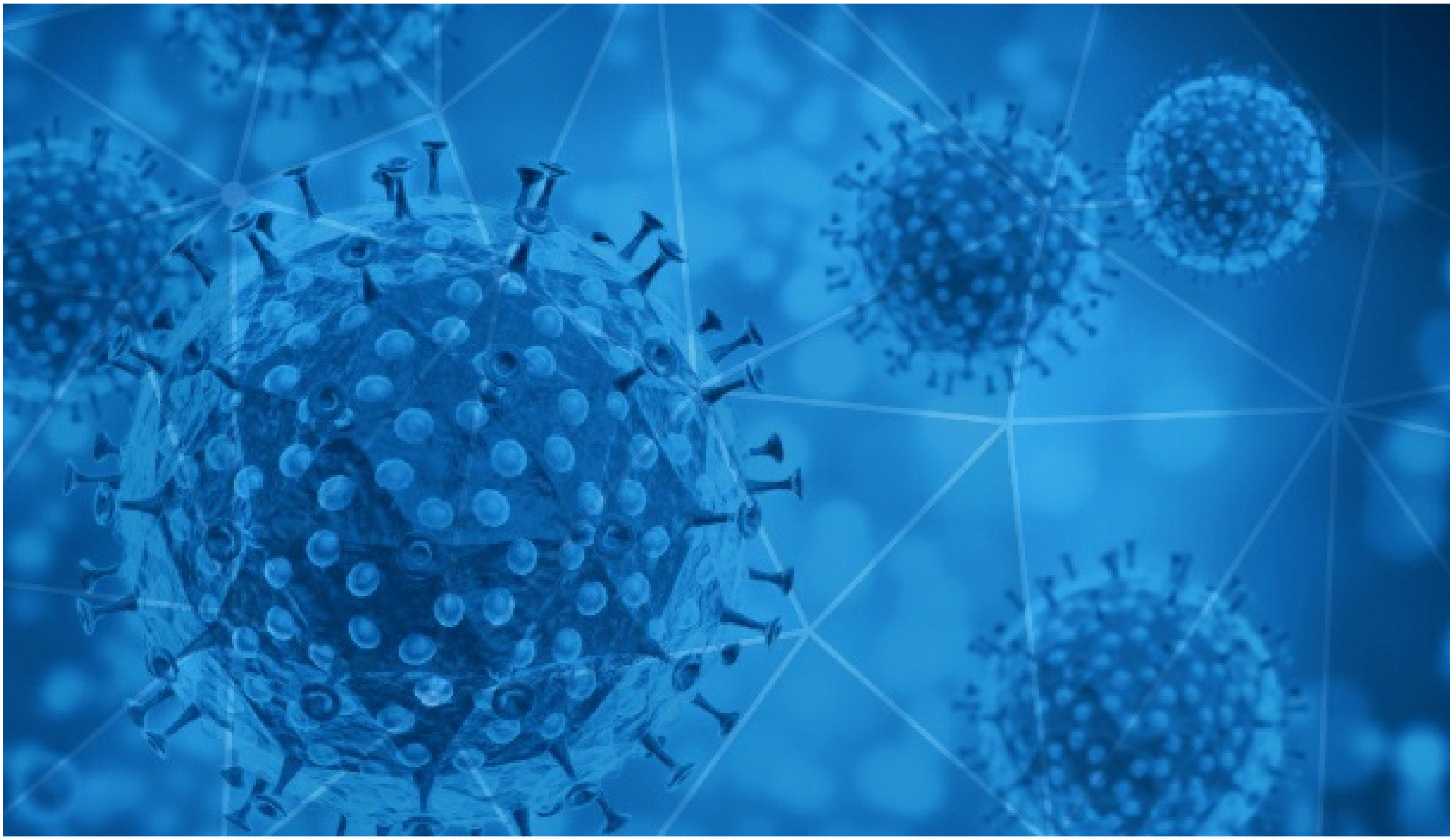
RiskIQ i3:

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

2020-12-14



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 2020-12-13 to 2020-12-14. During this period, RiskIQ analyzed 44,837 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,679 unique subject lines observed during the reporting period. The spam emails originated from 967 unique sending email domains and 2,410 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□□	19298
Covid19- Fund Compensation Notice	5615
The Corona Letter: Should pregnant women get the vaccine shot?	4633
Your Email Has Been Awarded 1 Million Pounds In 2020 Coca Cola Covid-19 Pandemic Award	1247
Prevenir el Coronavirus	1125
(□□) 5□□□ □□□ □□! Qoo10 Day #> □□□□ □□□ □□[CORONA □□□ □□ □□ □□□] / □□□ □□□ □□□[1+1 □□ □ □□□ □□□] / □□ □□□ □! [Xiaomi□□□ □□□□] > 11□□ □□□□ □□□□ □□□□ □□□ □□□!	983
Help the world's response to Covid-19 with the most protective mask on the market.	799
Ingresaron TEST COVID19 de deteccion rapida	781
Wearing a KN95 mask is your best defense against coronavirus	756
Re: Covid-19 Donations..	620
Covid-19 Relief Funds Award	516
Governor Tests Positive For COVID19, Officials Urge The Use Of KN95 Masks	433
Covid-19 expenses on your mind?	417
Covid-19 Pandemic	382
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	363
Covid-19 Pandemic Victim	358
Opnieuw geen akkoord over Brexit, onderhandelingen gaan door - Duitsland weer in harde lockdown: scholen en winkels dicht - Hoe Europa de scepsis tegen coronavaccins wegneemt	254
Let’s fight together to get through the COVID-19	232
Reserve Your Seat. Building a career in IT in the post-Covid world	165
Puricador y Sanitizador de Aire, Estirilización contra Coronavirus	161
HHS Waiver and Non-Enforcement Rules for the COVID-19	135
Know about Emerging trends in AI and ML post COVID scenario	134
protective supplies for corona	132
A COVID Christmas tale …	127
Should Democrat Governor Andrew Cuomo Face Charges over his Mishandling of Coronavirus Nursing Home Deaths?	124

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

epc-store.com	19300
yahoo.com	5640
timesofindia.com	4634
lifesense.guru	1555
gmail.com	1437
hotmail.com	1380
cimahso.com.ar	1125
qoo10.com	983
grupolylsalud.com	781
zohomail.eu	654

Top-15 IPs Sending COVID Spam

5.9.229.139	5614
107.158.49.28	1554
192.3.136.7	1247
181.239.232.96	781
153.126.159.103	740
103.225.53.125	695
103.225.53.103	643
203.201.164.82	620
103.225.54.103	570
103.225.53.194	569

Top-15 Countries Sending COVID Spam

JP	20056
DE	5998
US	5850
IN	5119
AR	1920
KR	1006
--	692
ID	675
CN	616
BR	582

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

ANC Weekly COVID-19 Reports	27
Actualidad | Caos vehicular; cómo evitar contagios de Covid-19	3
Masques tour de cou COVID et tour de cou standard	2
[editors--peacevoice] submission: op-ed: mental health, Portland, covid-19, violence, trauma, protest, police, Victor Frankl	2
Completed: Please DocuSign: COVID Testing Letter 12.12.2020.docx, Coronavirus Resident Testing Consent.pdf	2
Comparto 'Edvin Vásquez (Covid-19 en Paraguay)' con usted	2
Buletin de presa 13.12.2020 + comunicat actiuni COVID19	2
IMSS Boletín 831.- Instrumenta IMSS medidas para asegurar continuidad de servicios médicos ante incremento de contagios por COVID-19 (LINK VIDEO Y FOTOS)	2
Agendamento COVID	1
Comparto 'URUGUAY COVID-2' con usted	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: 136,151
Domains with Potential Mail Servers: 2,618
Email-Capable Domains and Hosts: 51,841
Live Hosts and Domains Not Parked: 45,961

Mobile Apps

Apps in Official Stores: 484

by Store

Apple	243
Google	226
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,884

by Store Type:

Hybrid	973
Secondary	852
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1