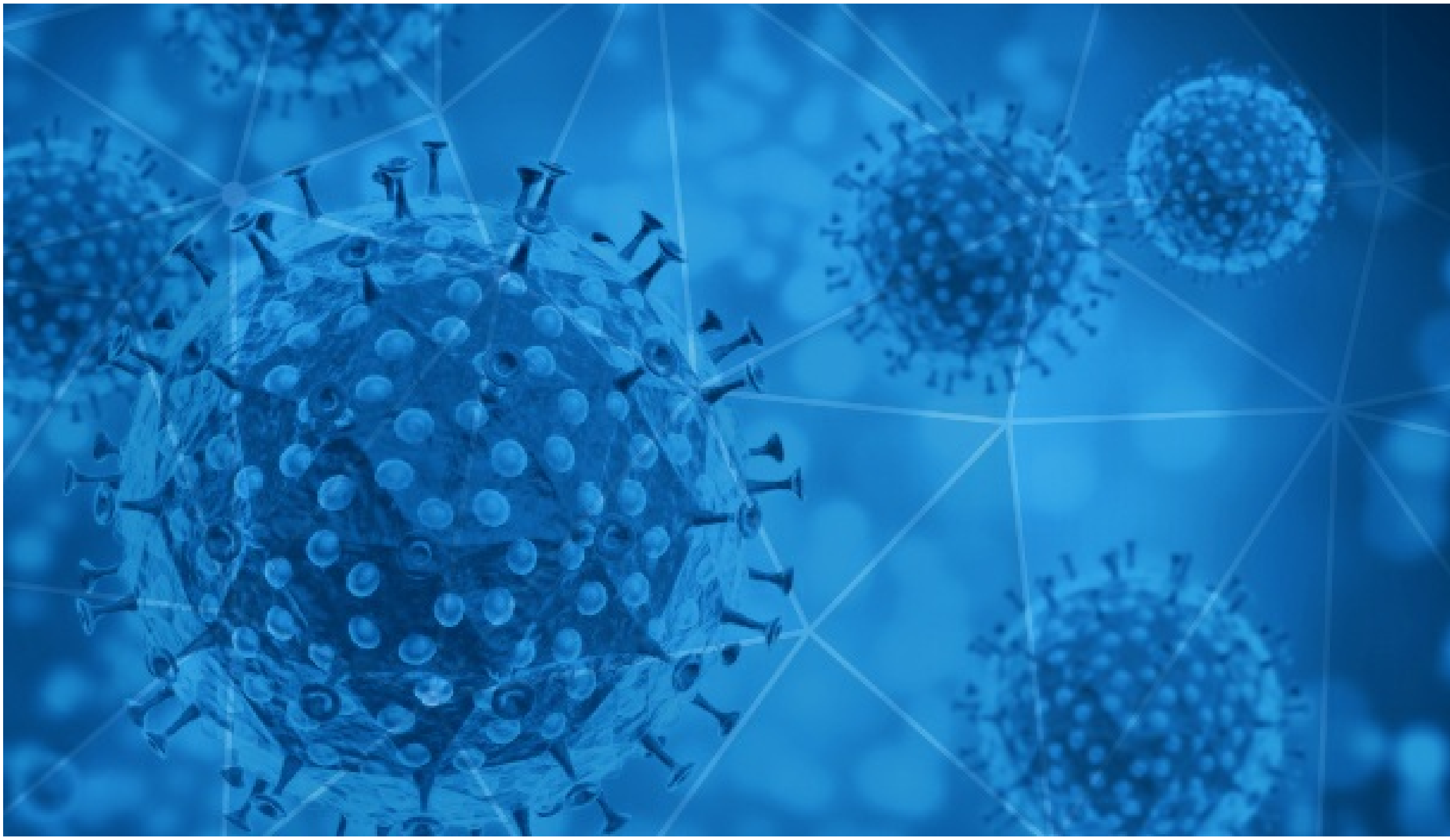
RiskIQ i3:

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

2020-09-21



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 2020-09-20 to 2020-09-21. During this period, RiskIQ analyzed 24,168 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,760 unique subject lines observed during the reporting period. The spam emails originated from 732 unique sending email domains and 2,334 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: The law needs a shot in the arm	5021
Mamparas de proteccion COVID19	1804
Mamparas de proteccion contra el coronavirus	1792
Test de deteccion rapida COVID19	1470
Help to fight COVID-19 fever alarm security door	1218
Videos para la prevencion de Covid	1148
Prevencion de covid19	1124
Your appointment for Covid Antibody IgG + IgM test is fixed at Rs 750 only.	559
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	487
Re: COVID-19 : Project Discussion | Website | Mobile Application | SEO (Results Guaranteed)!	332
Elimina el COVID-19 100% COMPROBADO Y CERTIFICADO	317
Vermiste Ilias is terecht - Generatie Corona begint aan het nieuwe academiejaar - De Roover en Dewael nog altijd op ramkoers - Iedere twee uur één ongeval met vluchtmisdrijf - Onderhandelaars werken in alle discretie naarstig verder	257
Let’s fight together to get through the COVID-19	231
Benefício Liberado - COVID 19	225
Re: Covid-19 acrylic protect shield	216
Re: Personal & Business Relief (COVID-19).	214
Unhealthy posture can Affect the Coronal and Lumber section of your Body	198
RE: COVID 19 RELIEF FUND FOR redacted@threatwave.com	186
Limited period offer for Covid Antibody IgG test starting at Rs 750 | Confirm soon.	183
Re: Personal & Business Relief (COVID-19).*	182
Elimina el COVID-19 100%!C(MISSING)OMPROBADO Y CERTIFICADO	179
(MUST READ) Google COVID-19 Relief Fund	159
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products).	159
Re:▯coronavirus civil mask / Chinese qualified manufacturer	150
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products).	148

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

countermail.com	7338
timesofindia.com	5021
keyable.net	1218
gmail.com	1214
yeah.net	1212
seajin.chtah.com	742
126.com	682
serviciosrentables.cl	496
cmbmutualfunds.com	433
163.com	381

Top-15 IPs Sending COVID Spam

190.247.254.65	6842
113.116.205.234	1129
190.247.226.201	496
164.90.181.158	495
157.119.122.97	330
219.65.85.27	279
219.65.85.35	276
219.65.85.26	274
219.65.85.33	263
219.65.85.34	263

Top-15 Countries Sending COVID Spam

AR	7376
IN	5743
CN	3819
US	3393
DE	475
PH	433
BE	323
BR	307
GB	288
MX	270

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

ANC Weekly COVID-19 Reports	37
COVID-19 RELIEF FUNDING	7
Concursos Especial Coronavirus	3
CCS / 10039: Rebasan la barrera de 14 mil los casos confirmados de COVID-19	2
IMSS VERSIÓN ESTENOGRÁFICA Y AUDIO. Sesión de preguntas y respuestas del director general del IMSS, Zoé Robledo, en la conferencia de prensa sobre el informe diario de la situación del Coronavirus en México, Palacio Nacional(AUDIOS)	2
IMSS VERSIÓN ESTENOGRÁFICA Y AUDIO. Palabras del director general del IMSS, Zoé Robledo, durante su participación en la conferencia de prensa sobre el informe diario de la situación del Coronavirus en México, Palacio Nacional (AUDIO)	2
la Covid à la Saint-Camille	2
IMSS Boletín 647.- Rodrigo, primer trasplante de hígado de donante vivo durante la emergencia sanitaria por COVID-19 en Jalisco (FOTOS)	2
Fwd: PANGENOMICS_COVID 19_MEHSANA_20-9-2020	1
Re: Report on SMAP Project's contribution to farmers affected by COVID-19 pandemic.	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: 126,105
Domains with Potential Mail Servers: 2,956
Email-Capable Domains and Hosts: 47,697
Live Hosts and Domains Not Parked: 71,620

Mobile Apps

Apps in Official Stores: 420

by Store

Apple	211
Google	194
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,402

by Store Type:

Hybrid	794
Secondary	553
Affiliate	55

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	25
Hybrid	2
Official	2