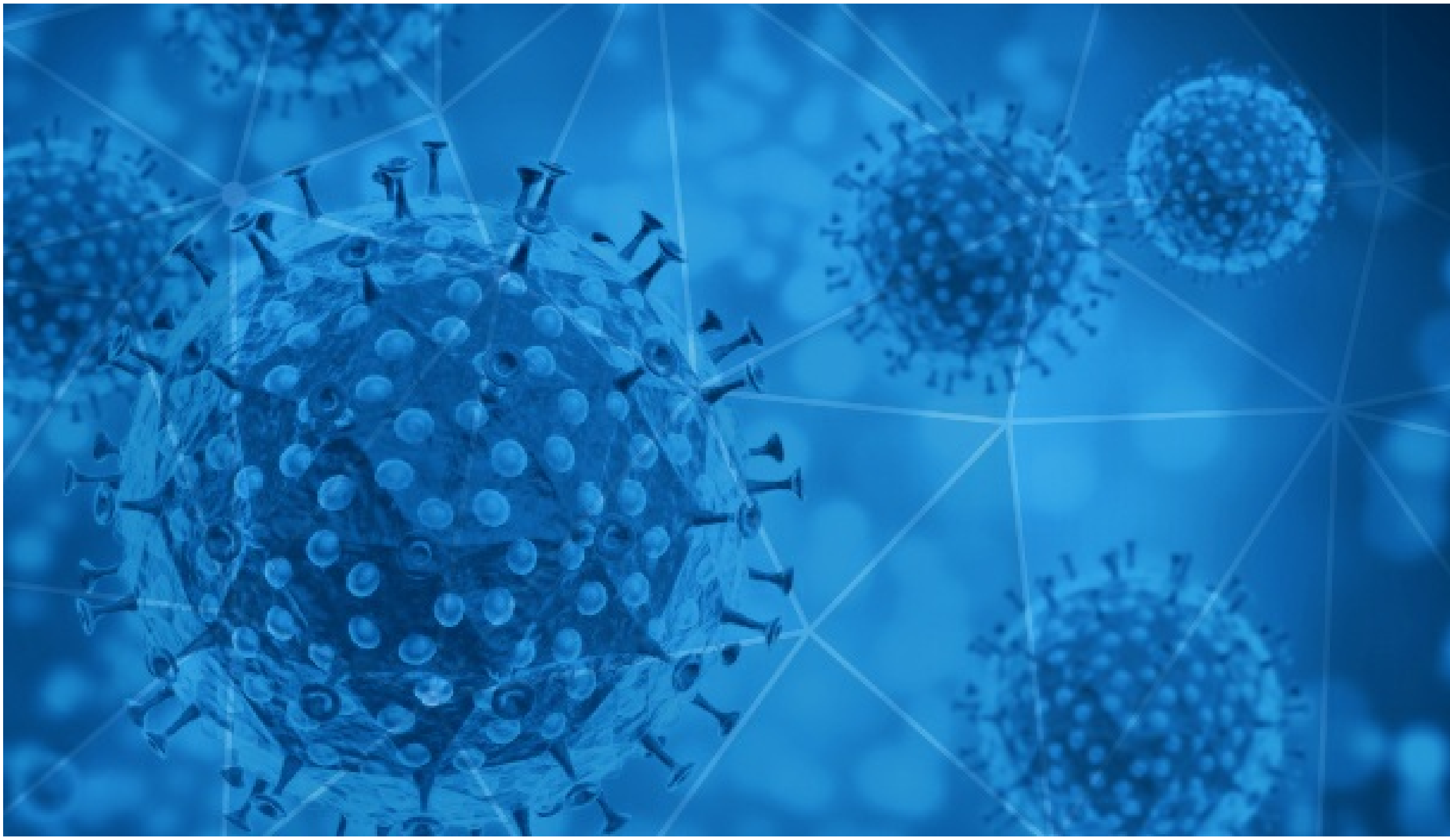
RiskIQ i3:

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

2020-06-12



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 2020-06-11 to 2020-06-12. During this period, RiskIQ analyzed 38,188 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,885 unique subject lines observed during the reporting period. The spam emails originated from 2,623 unique sending email domains and 4,967 unique SMTP IP Addresses. Analysts identified 2 emails which sent an executable file for Windows machines.

Top-25 Subjects

TIMES TOP10: Covid hits Gaganyaan	3457
The Corona Letter: A belated response	3176
COVID-19 / DONATION FOR YOU	3065
Paneles anti Covid-19 para atención de Público.	1562
Coronavirus cases rise in 20 states, Louisville police release Breonna Taylor report, and more from Apple News	1455
3 minutes to fight COVID	1010
Calificacion De Origen Laboral Enfermedad Covid-19	997
COVID-19 - Custom Projects | Mobile Application | SEO !! -etc [REDACTED_DOMAIN]	739
STAY SAFE CORONA-VIRUS (COVID 19) IS REAL!!!	607
BANNED GOODS DUE TO COVID 19 PANDEMIC	604
Planes Mensuales Especial Coronavirus	567
COVID-19 Tax Law Benefits: What you need to know to benefit financially & Eliminate Future Taxes!	535
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	431
Test COVID-19 Aprobados por el ISP	416
How to find a job during COVID-19 lockdown?	340
¿Estás buscando VINIL DE ALTO TRÁNSITO para el distanciamiento social? - Productos ANTICOVID	312
Mamparas de proteccion contra el coronavirus	291
Korea Trend News-COVID19-2	280
Sanitizador de calzado anticovid	276
Elija su Kit de PROTECCION Covid19	275
Credito fiscal COVID para innovacion	267
Mamparas de proteccion COVID19	260
Plan de Vigilancia, Prevención y Control del Covid-19 para el reinicio de actividades	244
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	200
Re: COVID-19 Financial Relief Funds for you	199

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmail.com	5743
bounce.indiatimes.com	3457
timesofindia.com	3176
publica20.club	1562
insideapple.apple.com	1519
naukri.com	1025
ccapacitaonline.com	997
163.com	939
126.com	837
countermail.com	818

Top-15 IPs Sending COVID Spam

212.227.254.175	3065
160.20.147.106	1562
207.154.221.139	997
133.167.123.176	742
210.112.10.145	607
181.46.136.165	431
157.119.122.135	386
157.119.122.138	353
103.214.115.215	339
103.214.115.213	322

Top-15 Countries Sending COVID Spam

US	9994
IN	8912
DE	5010
CN	2371
--	1732
FR	1557
AR	1329
JP	1162
KR	973
GB	944

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Fw: APPOINTMENT FOR COVID-19 SWAB TESTS IN PREPARATION FOR SAFE AND CONTROLLED RESTART OF CONSTRUCTION SECTOR	1

Top-15 Subjects Containing doc/xlsx Files

Important : Post-Coronavirus	52
COVID-19	5
NdP_ COVID-19, un virus también digital	4
NP- ASCAME impulsará un plan para reactivar y repensar la economía mediterránea post COVID19	3
NOTA La rehabilitación de los pacientes COVID-19 mejora gracias a las técnicas de movilización precoz	2
Unterlagen zur Corona Pandemie	2
Press Release: Hytera Keeps Abu Dhabi Police Connected During the Coronavirus Pandemic - Order #52230831	2
CCS9019 GOB 5ZM RECONVIERTE EDENA UNIDADES MÉDICAS PARA ATENDER COVID19 EN CHIHUAHUA 11JUN	2
March of Dimes Facebook Live - Systemic Racism affects on Moms & Babies; AB 3216 Paid Leave Advocacy Day, BWW Bring and Brother to Breakfast, SPA 6 Health Neighborhood Mtg, Fatherhood Event, and No. Cal Black Physicians Forum and COVID19 Resources	2
acta “PASO A PASO CON RESPECTO AL REPORTE DE ACCIDENTE DE TRABAJO POR EXPOSICIÓN A COVID-19"	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: 106,407
Domains with Potential Mail Servers: 2,698
Email-Capable Domains and Hosts: 40,997
Live Hosts and Domains Not Parked: 42,362

Mobile Apps

Apps in Official Stores: 297

by Store

Apple	169
Google	120
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 673

by Store Type:

Hybrid	409
Secondary	231
Affiliate	33

Blacklisted Mobile Apps: 20

by Store Type:

Secondary	19
Official	1