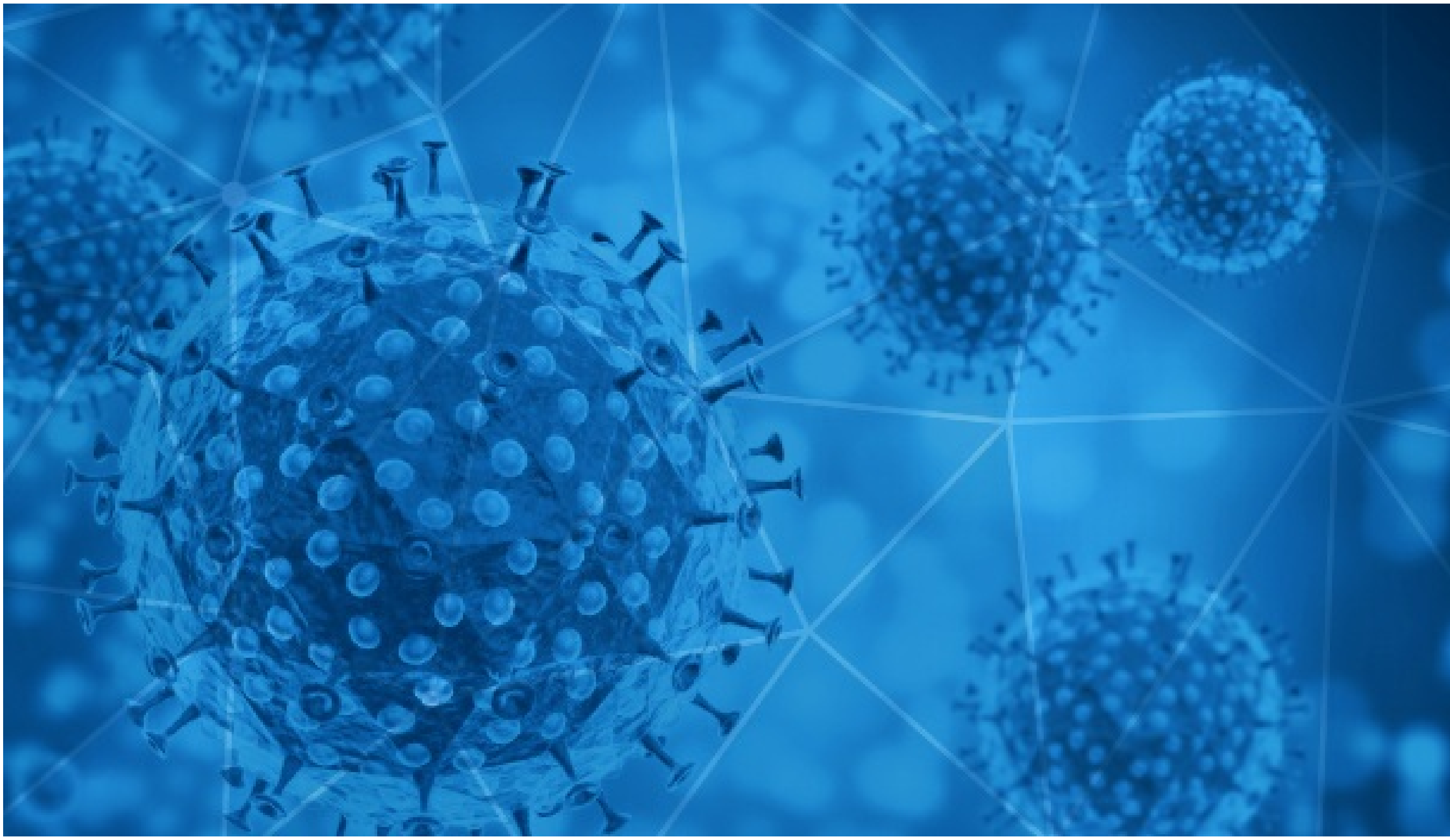
RiskIQ i3:

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

2020-07-09



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 2020-07-08 to 2020-07-09. During this period, RiskIQ analyzed 26,435 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,568 unique subject lines observed during the reporting period. The spam emails originated from 2,072 unique sending email domains and 3,853 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Why do case counts fall every Monday?	2648
COVID-19 - Mobile App Development/ PHP, Magento, Drupal, E-Commerce -etc [REDACTED_DOMAIN]	1727
Covid 19 Wohltätigkeitsfonds	1299
{COVID-19} □□□□□□□□□□□□□□□□□	1142
PyMEs contra el COVID19	678
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	656
Activos Fijos - Tratamiento Contable y Tributario en Tiempos de COVID-19	590
Sistema de detección Térmico Contra Covid-19	547
IMF COVID-19 DSP	545
UIF Support During Coronavirus Pandemic Approved	456
Implacable contra el COVID-19 AMONIOX	402
Oferta Test Rápidos COVID-19, Mascarillas, Alcohol Gel y Amonio Cuaternario.	401
Mantene tu lugar de trabajo libre de covid19	265
Evita el Covid19 en tu lugar de trabajo	243
Productos Covid 19 - Entrega Gratis RM	227
Tienes Disponible unÂ Credito FOGAPE - COVID-19	219
Venta de Pruebas Rapidas COVID-19	206
Fonds de soutien (COVID-19)	205
Re: keep away from Covid-19	196
Air cargo Import for Anti-COVID	194
COVID protective gear in stock!	178
Covid-19 relief payments	177
Korea Trend News-COVID19(4)	163
Get Tested TODAY for COVID -19- Day of Action!	159
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO ANTE EL COVID19	158

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmail.com	4602
timesofindia.com	2649
countermail.com	1188
toyotacarrr.com	1142
126.com	1118
163.com	752
focazen.com	591
seekscanenchile.com	547
absa.co.za	456
serviciosrentables.cl	402

Top-15 IPs Sending COVID Spam

170.231.82.35	1299
157.119.122.139	678
119.122.91.133	656
159.65.80.166	547
122.34.222.210	545
157.119.122.138	494
46.4.12.75	437
157.119.122.135	417
164.90.181.158	402
190.247.242.146	324

Top-15 Countries Sending COVID Spam

US	6591
IN	4658
CN	2158
JP	1597
AR	1563
FR	1347
PE	1311
DE	1270
GB	1053
KR	744

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

Excel training & Coping with COVID19 today & tomorrow webinar	8
PHHS 7 7 2020 End of Day COVID Report	7
PPE items against Covid-19	7
RV: CUMPLIMIENTO DE PROTOCOLOS DE BIOSEGURIDAD PARA MANEJO DE PANDEMIA CORONAVIRUS - COVID19	6
COVID-19 RELIEF FUNDING	6
Re: [MCOH-EH] COVID-19 employee contact tracing in healthcare facilities	4
ÚLTIMAS PLAZAS Cena-encuentro: 'OSAKIDETZA ante el Covid-19', con Juan Luis Diego Casals, director general de OSAKIDETZA / AZKEN TOKIAK Afari-tertulia: 'OSAKIDETZA Covid-19aren aurrean', Juan Luis Diego Casalsekin, OSAKIDETZAko zuzendari nagusia	3
Instrucción Interna: Pautas preventivas frente a la COVID-19 y autoevaluación del Teletrabajo	3
NP SEMI · 65 investigaciones en marcha sobre SARS-CoV-2 con datos del Registro SEMI-COVID-19 (08.07.20).	3
Barometru de opinie Frames & Hygienium. Ce cred românii despre pandemia de coronavirus	3

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: 112,663
Domains with Potential Mail Servers: 2,765
Email-Capable Domains and Hosts: 42,680
Live Hosts and Domains Not Parked: 54,833

Mobile Apps

Apps in Official Stores: 324

by Store

Apple	178
Google	137
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 862

by Store Type:

Hybrid	540
Secondary	285
Affiliate	37

Blacklisted Mobile Apps: 21

by Store Type:

Secondary	19
Hybrid	1
Official	1