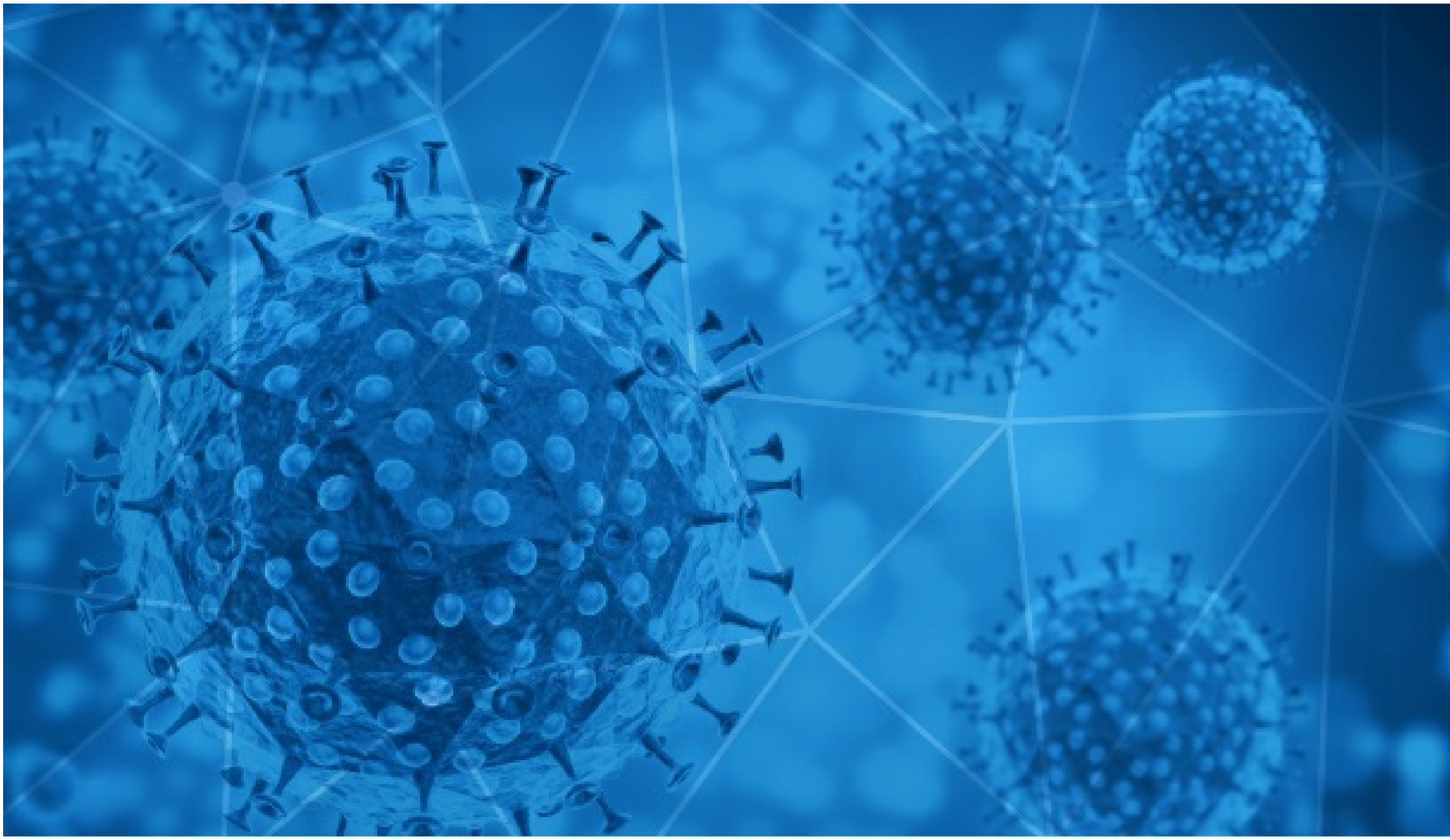
RiskIQ i3:

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

2020-06-26



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 2020-06-25 to 2020-06-26. During this period, RiskIQ analyzed 55,821 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,569 unique subject lines observed during the reporting period. The spam emails originated from 2,931 unique sending email domains and 5,767 unique SMTP IP Addresses. Analysts identified 9 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Herd immunity threshold could be lower	3902
New U.S. coronavirus cases hit record high, why Americans are drinking less, and more from Apple News	2231
BANNED GOODS DUE TO COVID 19 PANDEMIC	1891
Minimice el Riesgo de contagio del Coronavirus - Validacion Biometrica	1549
COVID-19 EMERGENCY DELIVERY OF YOUR CONSIGNMENT BOX TODAY.	1058
Empresas responden, empiezan a hacer pruebas de COVID-19 a empleados	1047
Sistema de detección Térmico Contra Covid-19	851
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	685
Beneficios y Alternativas Legales para Empresas en tiempos de Covid-19	671
Tratamiento de Aire contra Covid 19	567
COVID-19 - Mobile App Development/ PHP, Magento, Drupal, E-Commerce -etc [REDACTED_DOMAIN]	540
COVID-19 / DONATION FOR YOU	537
Implacable contra el COVID-19 AMONIOX	520
Cabinas para la prevencion del coronavirus?	498
Protección y Testeo Covid19	476
Evita el Covid19 en tu lugar de trabajo	476
Como volver a la actividad post coronavirus?	464
Soluciones para la prevencion del covid19	459
COVID-19 - Custom Projects | Mobile Application | SEO !! -etc [REDACTED_DOMAIN]	446
Mantene tu lugar de trabajo libre de covid19	436
COVID-19 Unterstützungsfonds	392
FW:Bono Covid 827257905	384
MICROSOFT CORONAVIRUS RELIEF FUND	376
Mamparas de proteccion COVID19	374
PEC e Covid-19: 6 servizi accessibili in modalità semplificata	374

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

notticiassemfoco.com.cl	11196
timesofindia.com	3902
countermail.com	3328
gmail.com	3176
insideapple.apple.com	2311
gov.org	1891
sopytecchile.com	1549
163.com	1410
126.com	1197
hotmail.com	1185

Top-15 IPs Sending COVID Spam

207.199.252.3	1857
167.99.191.76	1549
159.65.80.166	851
201.231.58.126	742
201.231.6.163	741
190.247.242.106	741
201.231.5.39	728
119.122.89.249	685
81.95.112.26	597
113.88.157.150	595

Top-15 Countries Sending COVID Spam

US	20191
IN	5415
AR	3725
GB	3596
CN	3360
DE	2256
CA	2118
BR	1790
AU	1596
JP	1527

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

COVID 19 SUPPORT ITEMS	9

Top-15 Subjects Containing doc/xlsx Files

BHP – obowiązki pracodawcy i pracownika w dobie Covid 19	10
La crisis del coronavirus refuerza el liderazgo complementario	10
Covid-19 Related Products Price List	8
PROTEGE A TU EMPRESA FRENTE AL COVID	7
Όμιλος ΟΤΕ: Υλοποίηση του Εθνικού Μητρώου Ασθενών με COVID-19	3
Medidas Estratégicas Para Facilitar La Recuperación del Negocio Hotelero En Escenario Post-Covid.	3
Labor Arbeitsauftrag 26.06.-02.07.2020 (Covid-19)	2
NP_Digitalización y protocolos ‘hands free’, esenciales para proteger la oficina contra el Covid-19	2
Corona Virus update from Churches Together in Cumbria	2
Covid policies	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: 108,951
Domains with Potential Mail Servers: 2,747
Email-Capable Domains and Hosts: 41,711
Live Hosts and Domains Not Parked: 46,913

Mobile Apps

Apps in Official Stores: 301

by Store

Apple	170
Google	123
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 751

by Store Type:

Hybrid	460
Secondary	257
Affiliate	34

Blacklisted Mobile Apps: 20

by Store Type:

Secondary	19
Official	1