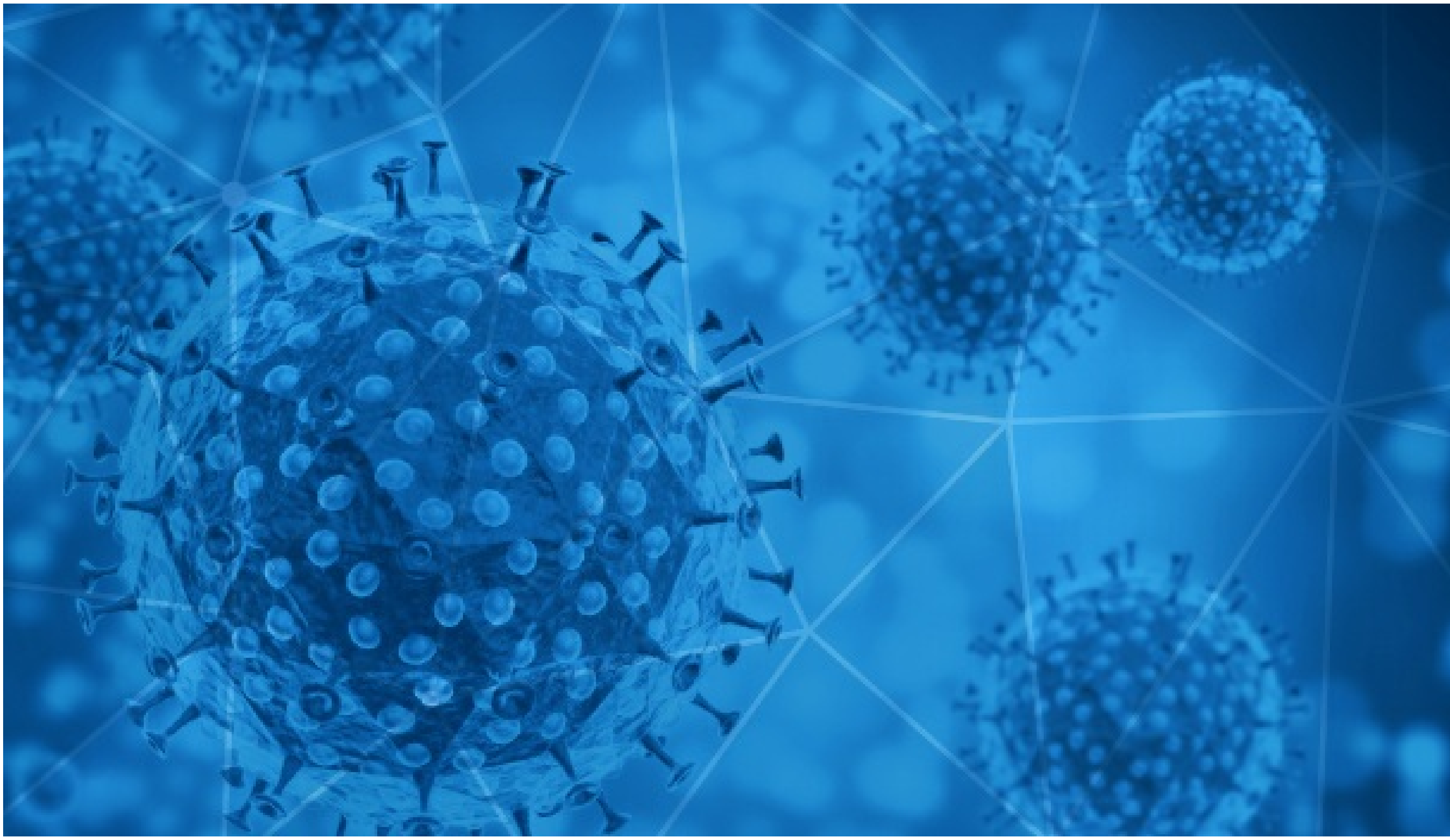
RiskIQ i3:

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

2020-09-10



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 2020-09-09 to 2020-09-10. During this period, RiskIQ analyzed 22,841 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,096 unique subject lines observed during the reporting period. The spam emails originated from 1,536 unique sending email domains and 3,320 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

#ACACaresCovid19: Building leadership, livelihoods and legacies | Clicks delists TRESemmÃ©	2235
The Corona Letter: A setback for Oxford vaccine	1893
Why a coronavirus vaccine trial was paused, police shoot a 13-year-old boy with autism, and more from Apple News	1811
Reife Frauen zu Corona-Zeiten treffen	1372
Your Relief For Coronavirus (Covid19).	962
Cuidate del COVID19 con nuestros productos	775
Frente al Coronavirus nos Cuidamos Todos…	768
MEDICAL SAFETY PPE | COVID19	722
Covid-19 Rapid Test Kits	672
COVID-19 LATEST NEWS	481
Fwd:Credito Covid-19 Aprobado.	282
Equipo portátil efectivo contra COVID-19	278
Contactless infrared body temperature thermometer defeat Coronavirus	264
Re: Defeat Coronavirus, non contact fever alarm device	255
Productos Covid-19	228
Ante el elevado riesgo de contagio por Coronavirus en Perú.	201
Precios Imbatibles / Productos COVID 19	197
W.H.O COVID-19 Response Fund	195
Frente al Coronavirus nos Cuidamos Todos !	181
Test Rápido Covid-19 Segunda Generación - 10.000 Un Entrega Inmediata	159
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	145
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	134
Let’s fight together to get through the COVID-19	133
Nuevo catálogo de productos anti-COVID 2020	129
Coach Izzo, early detection, student COVID cases and more. Read the MSUToday Weekly Update.	124

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

bizcommunity.com	2235
insideapple.apple.com	1895
timesofindia.com	1893
gmail.com	1476
data2web.de	1372
126.com	945
countermail.com	775
trendingtopic.cl	768
hbbcustomercenter.com	735
medicproduction.com	722

Top-15 IPs Sending COVID Spam

46.20.37.30	1372
177.136.47.226	968
139.99.133.125	722
51.77.33.43	573
178.79.133.59	551
109.74.200.66	503
113.116.206.195	477
109.74.200.68	471
223.38.30.100	449
190.247.240.157	412

Top-15 Countries Sending COVID Spam

US	5633
GB	2534
IN	2180
CN	1958
FR	1771
DE	1674
BR	1050
AR	967
AU	741
KR	615

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

CUMPLIMIENTO DE PROTOCOLOS DE BIOSEGURIDAD PARA MANEJO DE PANDEMIA CORONAVIRUS - COVID19	9
Covid-19 compensation fund	4
Emergenza COVID-19 WEBINAR SMART WORKING: accordi individuali, privacy, valutazione e welfare aziendale 7/10/20	4
CCS /9934 Por llegar a los 13 mil casos confirmados de COVID-19 en el estado	2
Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020	2
Interview Request - Covid Crisis Impact on Gold Prices / Stocks / Trading / Investment by Registered Financial Adviser with SEBI, Mr. Rachit Chawla	2
Child Care Initiative from Coronavirus Relief Fund to Support Working Families and September logs!	2
NP Gimnasios y centros deportivos son los nuevos aliados frente al COVID-19	1
KATALOG WRZESIEŃ!! środki ochrony COVID 19!	1
indicaciones y procedimientos covid	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: 123,573
Domains with Potential Mail Servers: 2,966
Email-Capable Domains and Hosts: 45,842
Live Hosts and Domains Not Parked: 68,667

Mobile Apps

Apps in Official Stores: 411

by Store

Apple	211
Google	185
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,301

by Store Type:

Hybrid	757
Secondary	491
Affiliate	53

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	25
Hybrid	2
Official	2