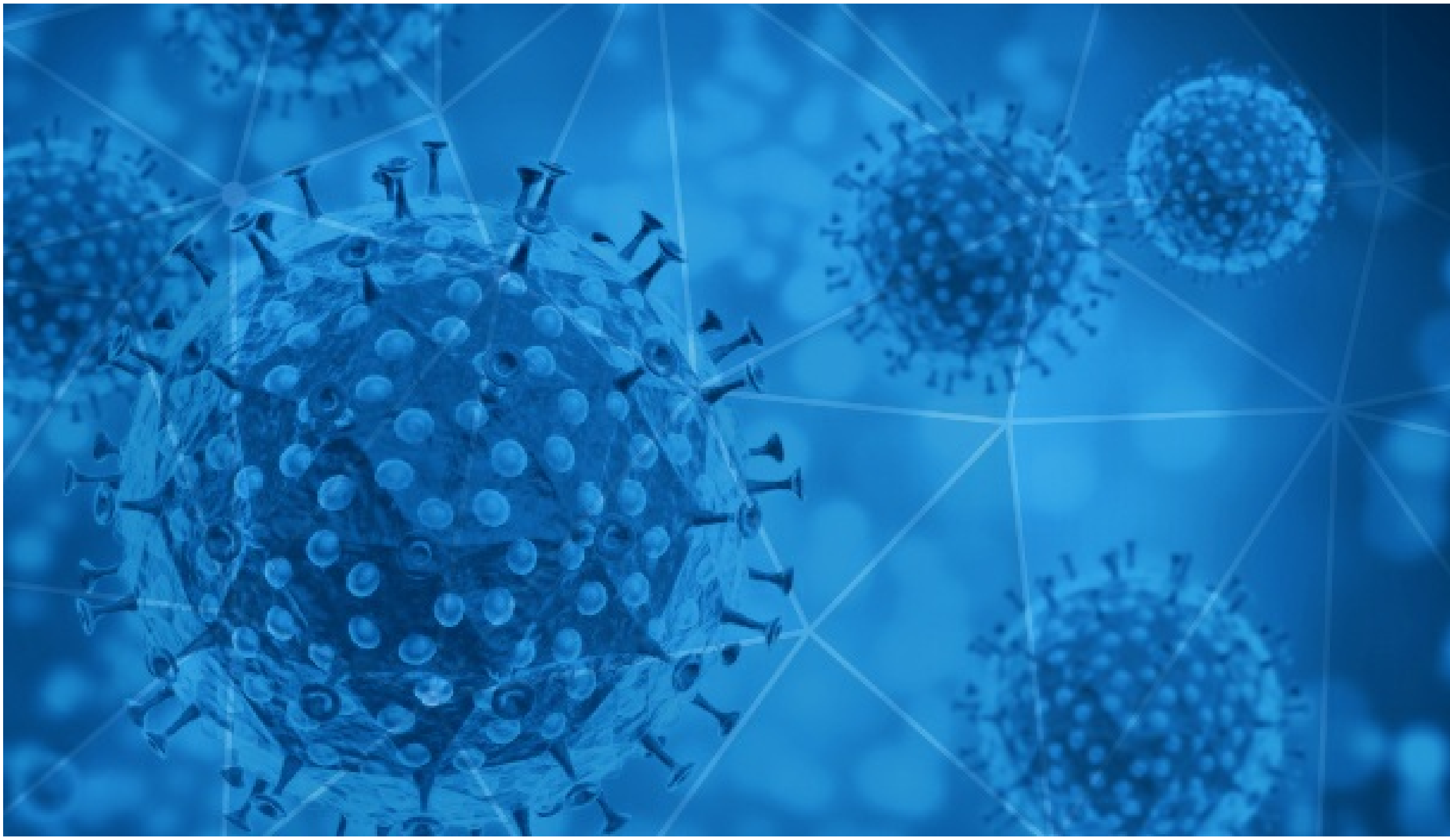
RiskIQ i3:

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

2020-08-07



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 2020-08-06 to 2020-08-07. During this period, RiskIQ analyzed 36,857 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,813 unique subject lines observed during the reporting period. The spam emails originated from 1,782 unique sending email domains and 4,315 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

TIMES TOP10: That's 20k Covid deaths in 30 days	2370
The Corona Letter: Serum Institute gets its hands on another vaccine candidate	2319
You have payment from United Nations Covid-19 Palliative/Financial Support	1849
PyMEs contra el COVID19	1578
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	1426
Nueva línea de atención exclusiva COVID19	907
{COVID-19} □□□□□□□□□□□□□□□□□□	798
I am glad you stayed safe from the Covid 19 pandemic	766
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	623
ATALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID -19	584
Covid-19 Face Mask	574
Surgical & Medical Mask for Coronaviruse / China Qualified Manufacturer	478
Especial Covid-19 - Arco Dual Detector de Temperatura y Metales	401
New Covid nightmare?!\t	386
Prevención Covid 19	374
Re: Tenemos que adaptarnos a la situacion Covid-19	357
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	342
Re: Adaptados a la nueva situacion Covid-19	340
Re: Nos tenemos que adaptar a la situacion Covid-19	339
Re: Nos adaptamos a la nueva situacion Covid-19	335
Re: Hay que adaptarnos a la situacion Covid-19	322
Re: Estamos adaptados a la nueva situacion Covid-19	314
Desinfectamos su ambiente de coronavirus	312
Totem Covid-19 Test Rápido, Mascarillas, Guantes e Insumos	310
Re: keep away from Covid-19	310

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmail.com	5368
countermail.com	2489
bounce.indiatimes.com	2370
timesofindia.com	2320
126.com	1808
163.com	1151
avaaz.org	961
saludtotal.com.co	908
hotmail.com	847
toyotacarrr.com	798

Top-15 IPs Sending COVID Spam

103.99.2.5	1865
190.247.255.33	1513
181.46.136.168	1426
200.31.17.85	908
45.143.222.149	766
190.247.226.190	664
106.75.95.195	574
181.160.221.108	438
187.72.150.252	385
119.139.136.255	313

Top-15 Countries Sending COVID Spam

US	7325
IN	5125
AR	4941
CN	4335
DE	3335
VN	2515
--	1264
FR	1115
JP	1062
CL	1020

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

PHHS 8 6 2020 End of Day COVID 19 Report	14
Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020	4
COVID-19 Focus IAS/IFRS Principi Contabili Internazionali: novità normative contabili e fiscali Milano 21/10/2020	4
Fwd: Cares Act Coronavirus Relief Fund	2
Persbericht TOM in Coronatijd	2
Press Release: Artnovion Reveals MedLine Range of Healthcare and COVID-safe Acoustic Treatment	2
Principal - #4 Letter - Covid-19 School Information - 04 Aug 2020	2
El Gobierno canario colabora con el Estado para determinar la presencia de la COVID-19 en las aguas residuales de las Islas. Saludos	2
Fwd: WEEKLY REPORT FROM 27-07-2020 TO 31-07-2020 REGARDING COVID (REVISED COLUMNS) -reg	2
Fw: Covid -19 FAQ's	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: 118,363
Domains with Potential Mail Servers: 2,875
Email-Capable Domains and Hosts: 44,269
Live Hosts and Domains Not Parked: 66,250

Mobile Apps

Apps in Official Stores: 372

by Store

Apple	195
Google	168
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 967

by Store Type:

Hybrid	620
Secondary	305
Affiliate	42

Blacklisted Mobile Apps: 23

by Store Type:

Secondary	20
Official	2
Hybrid	1