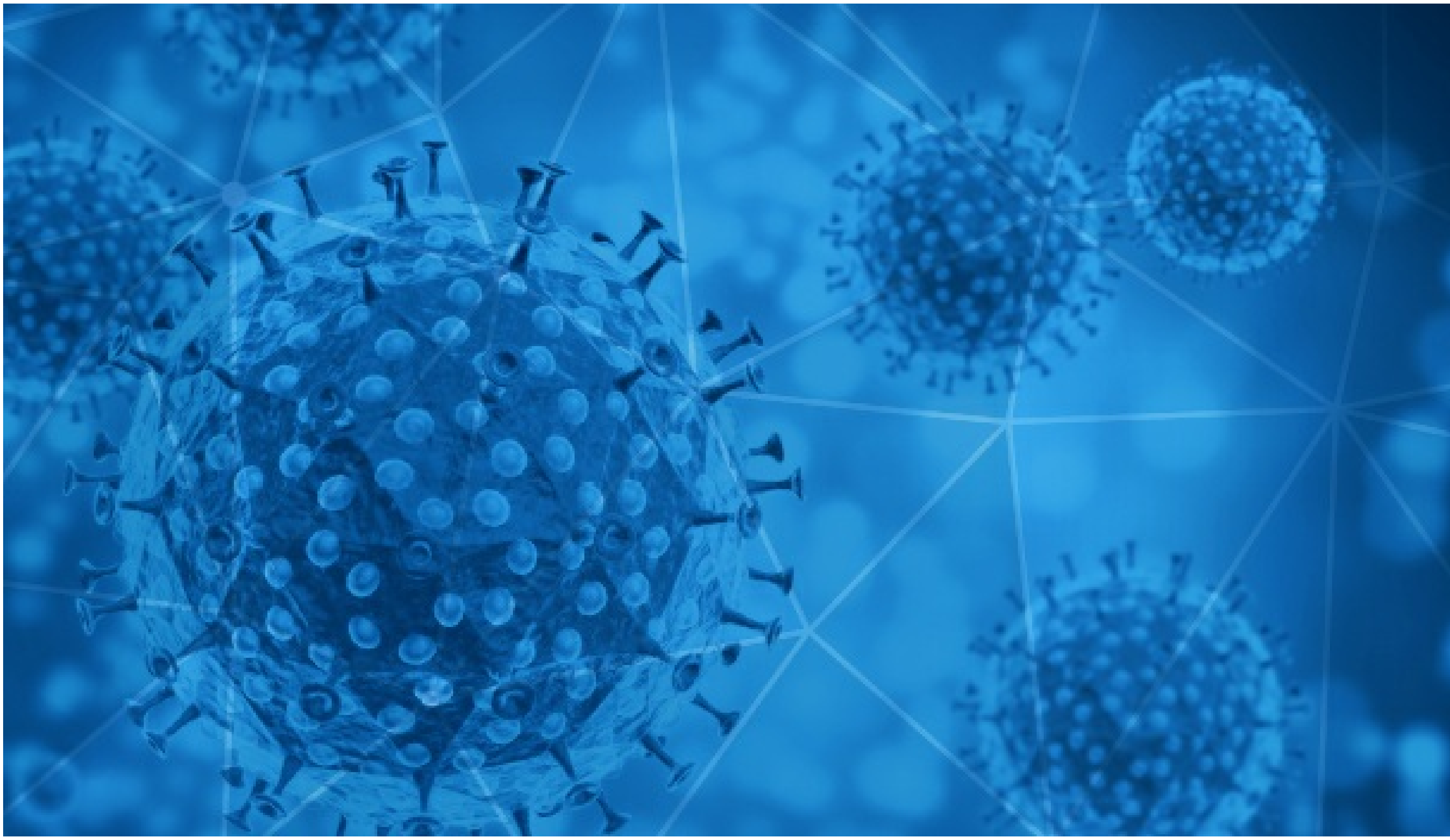
RiskIQ i3:

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

2020-08-13



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 2020-08-12 to 2020-08-13. During this period, RiskIQ analyzed 65,791 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,988 unique subject lines observed during the reporting period. The spam emails originated from 1,840 unique sending email domains and 4,635 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	19841
Will COVID-19 Impact Your Credit Scores?	2728
Protect Scores During Coronavirus	2674
COVID-19 And Your Credit Health	2627
TIMES TOP10: Russia declares Sputnik V against Covid	2004
The Corona Letter: Can a synthetic nanobody defeat the virus?	1972
Picking up prescriptions? Protect yourself from COVID-19.	1491
Re:Covid 19 Loan Relief	1023
Help the world's response to Covid-19 with the most protective mask on the market.	942
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	906
Wearing a KN95 mask is your best defense against coronavirus	868
Precios Imbatibles / Productos COVID 19	855
COVID-19 Compensation/Relief Funds.	829
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	709
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	693
COVID-19 - Send Requirements + SEO (Results Guaranteed) [REDACTED_DOMAIN]	614
Insumos para Contingencia ANTI COVID-19	588
Covid-19: Quality IT Projects | SEO (Results Guaranteed) - [REDACTED_DOMAIN]	527
face mask-Face mask- most effective for COVID-19	511
Protocolos de Salud Ocupacional en tiempos de Covid-19	442
Campaña Prevención Covid-19	433
Conditional Sales Contract Documents COVID-19 Policy Update	403
Gestion de Cobranzas y Riesgo Crediticio en Tiempos de COVID con Lineamientos Legales - PROMO 2X3.- Cupos Limitados	391
Re: Adaptados a la nueva situacion Covid-19	381
Re: Estamos adaptados a la situacion Covid-19	379

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

toyotacarrr.com	19844
gmail.com	5489
righla.cyou	3849
straline.work	2228
bounce.indiatimes.com	2004
timesofindia.com	1972
sweenseque.cyou	1952
126.com	1833
subscriptions.cms.hhs.gov	1491
countermail.com	986

Top-15 IPs Sending COVID Spam

23.231.110.145	3846
23.231.110.163	2222
23.231.110.164	1950
211.241.209.104	1023
23.231.110.151	915
23.231.110.152	892
89.175.26.197	872
216.151.221.3	830
113.89.41.103	723
181.46.136.168	693

Top-15 Countries Sending COVID Spam

JP	19943
US	19653
IN	5600
CN	4272
DE	3397
AR	2150
FR	1792
KR	1135
ES	998
RU	926

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	11
COVID-19 RELIEF FUNDING	7
NOTA DE PRENSA - LEGADO MUESTRA AVANCES EN LA CONSTRUCCIÓN DEL CENTRO DE ATENCIÓN PARA PACIENTES COVID-19 EN JULIACA - GALERÍA DE FOTOS	5
PHHS 8 12 2020 End of Day COVID 19 Response Summary	3
Covid-19, Webinars & First Aid courses 2020	2
Premier Preneed Marketing Announces $5,000 COVID-19 Grant Program for funeral homes; deadline August 20th!	2
Boletín SEP no. 217 - Realizan estudiantes y docentes del TecNM acciones para combatir los efectos del COVID-19 en las comunidades	2
FW: Leadership Communications: Covid Briefing	2
all School Manager, DrrM, Health and Guidance ConPlan for Covid19	2
PERSONAL DIRSEEST-PNP INFECTADO CON 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: 119,077
Domains with Potential Mail Servers: 2,897
Email-Capable Domains and Hosts: 44,002
Live Hosts and Domains Not Parked: 65,709

Mobile Apps

Apps in Official Stores: 383

by Store

Apple	201
Google	173
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,044

by Store Type:

Hybrid	654
Secondary	348
Affiliate	42

Blacklisted Mobile Apps: 25

by Store Type:

Secondary	22
Official	2
Hybrid	1