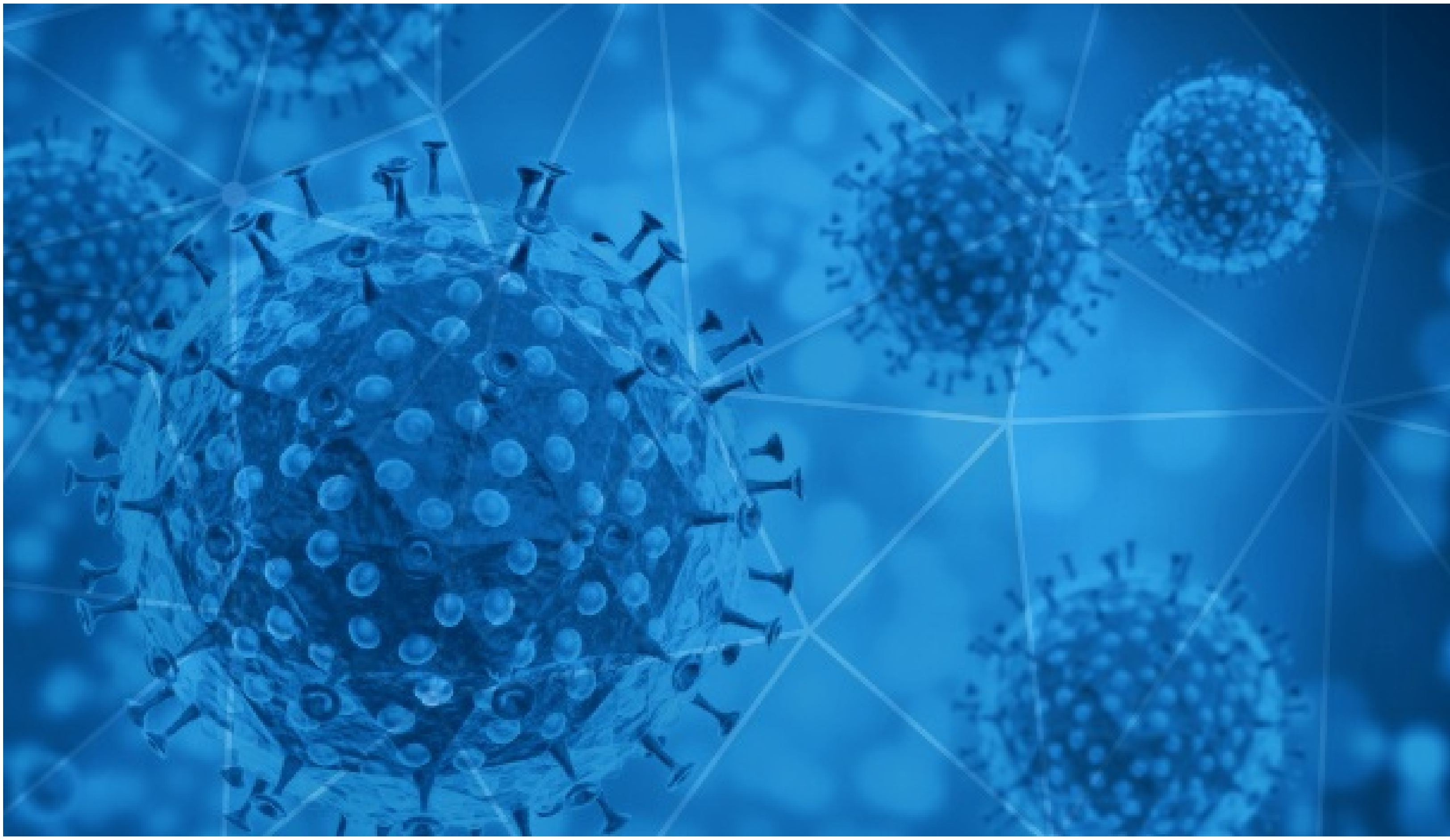
RiskIQ i3:

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

2020-08-31



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 2020-08-30 to 2020-08-31. During this period, RiskIQ analyzed 24,544 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,015 unique subject lines observed during the reporting period. The spam emails originated from 1,610 unique sending email domains and 2,385 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: How robust would our immunity be?	2565
Soluciones para la prevencion del covid19	1920
Como volver a la actividad post coronavirus?	1902
Cabinas para la prevencion del coronavirus	1872
Coronavirus: 'Stay home - earning big money at home'	1385
Evite contagios, no al Covid19, Accese, Asistencia biométricos	960
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	945
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	740
Reife Frauen zu Corona-Zeiten treffen	553
Re: Defeat Coronavirus, non contact fever alarm device	367
Oops: It Looks Like the Vast Majority of Positive COVID Results Should Have Been Negative	353
Contactless infrared body temperature thermometer defeat Coronavirus	320
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	287
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	287
COVID-19 PPE TENDER FUND PROPOSAL	275
Re: keep away from Covid-19	260
Covid-19: Quality IT Projects | SEO (Results Guaranteed) - [REDACTED_DOMAIN]	258
covid-19 and children - how does it affect them?	237
Equipos de protección COVID 19	223
Covid-19	221
Cuidate del COVID19 con nuestros productos	217
International Conference on the Global Impact of the Coronavirus COVID-19, November 24- 29, 2020	216
COVID-19 LATEST NEWS	197
** Sven Elverfeld im Podcast, Gratis-Coronatests für die Gastro und vieles mehr**	190
AUGUST COVID-19 RELIEF FUND	177

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

countermail.com	6306
timesofindia.com	2565
gmail.com	2231
126.com	2009
sopytecchile.com	960
hotmail.com	703
keyable.net	687
data2web.de	553
townhallmail.com	353
emailmarketingservices.us	237

Top-15 IPs Sending COVID Spam

190.247.243.236	4733
46.101.218.158	960
181.46.136.168	945
113.116.207.198	624
119.122.90.172	592
46.20.37.30	552
190.247.241.134	545
177.11.103.6	429
190.247.241.67	426
190.247.227.6	315

Top-15 Countries Sending COVID Spam

AR	7285
CN	3419
US	3379
IN	3056
DE	1855
BR	548
FR	496
NL	399
RU	390
--	362

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

COVID19 en MRS - Préventions 2ème vague: Directives IrisCare	1

Top-15 Subjects Containing doc/xlsx Files

Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020	35
ANC Weekly COVID-19 Reports	23
Covid-19 compensation fund	3
COVID -19 DUTY SCHEDULE OF DNB/CPS RESIDENTS	2
FW: shock-report-week-cdc-quietly-updated-covid-19-numbers	2
Re: MACAW // Updated Humanity Crew COVID Protocols // Shoot Dates: Sept 5-7 // HIGH PRIORITY	2
Covid-19 compensation fund	2
AISLAMIENTO DE PERSONAL POLICIAL POR COVID-19	1
covid self declaration form	1
Fwd: Concurso : ¿Qué hemos aprendido de la Covid-19?	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: 121,460
Domains with Potential Mail Servers: 2,957
Email-Capable Domains and Hosts: 45,266
Live Hosts and Domains Not Parked: 66,576

Mobile Apps

Apps in Official Stores: 409

by Store

Apple	211
Google	183
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,255

by Store Type:

Hybrid	727
Secondary	476
Affiliate	52

Blacklisted Mobile Apps: 26

by Store Type:

Secondary	23
Official	2
Hybrid	1