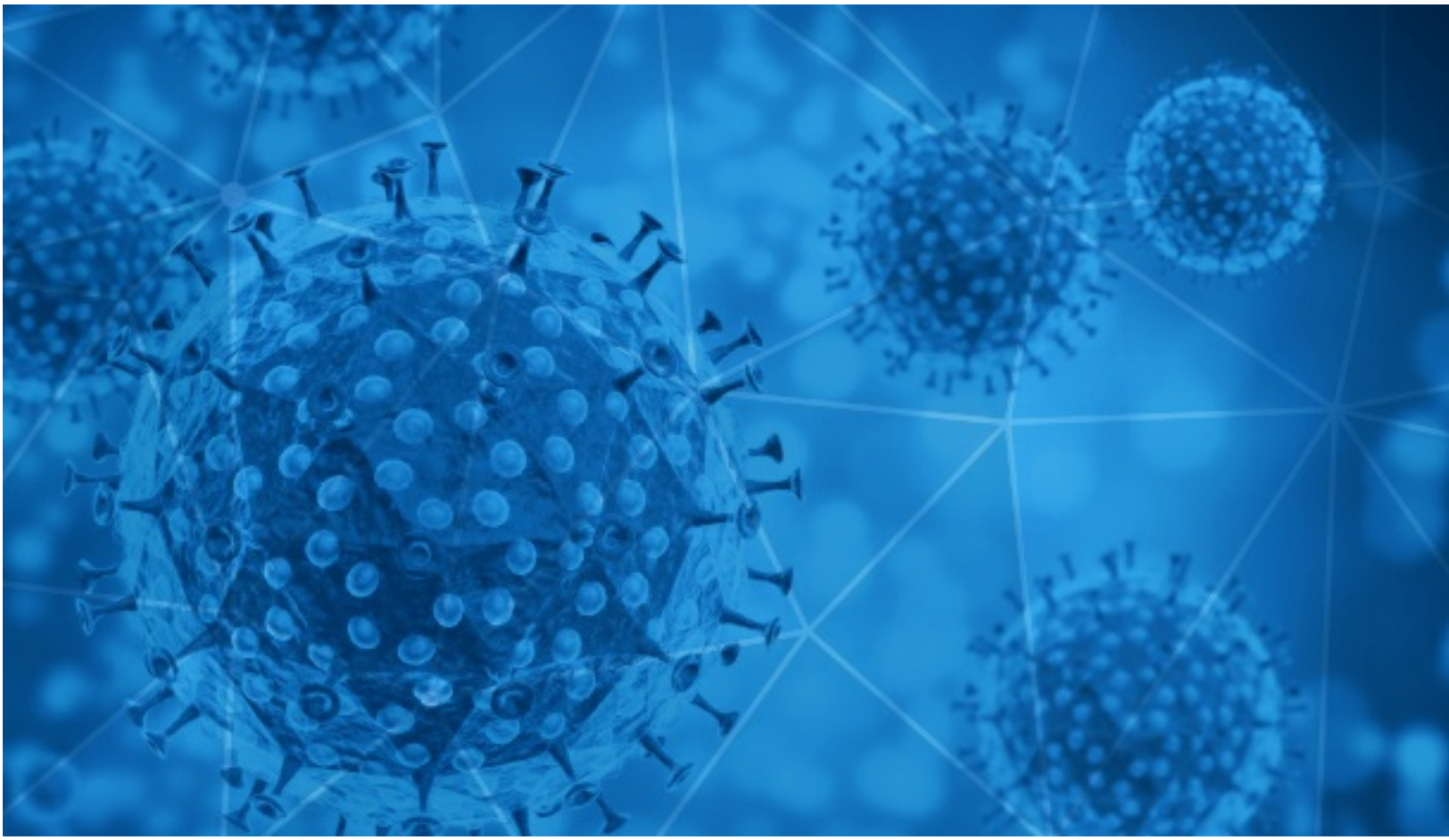
RiskIQ i3:

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

2020-07-31



RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

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

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 2020-07-30 to 2020-07-31. During this period, RiskIQ analyzed 42,954 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,077 unique subject lines observed during the reporting period. The spam emails originated from 1,920 unique sending email domains and 4,189 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

U.S. coronavirus deaths top 150,000, what to know about the NBA's return today, and more from Apple News	3883
The Corona Letter: Testing has been ramped up but…	1435
YOU ARE LUCKY WINNER OFPALLIATIVE PROMO OF COVID19	1233
PyMEs contra el COVID19	852
- Covid-19 Coronavirus: how to protect yourself	764
Covid 19 Wohltätigkeitsfonds	472
COVID-19 And Your Credit Health	420
Will COVID-19 Impact Your Credit Scores?	412
Protect Scores During Coronavirus	390
Cabinas para la prevencion del coronavirus?	351
Herman Cain DEAD from coronavirus +LAPD run by ‘SWAT Mafia’ + Trump suggests DELAYING 2020 election	350
ARCO Dual Detector de Temperatura y Metales - Covid-19	332
PRODUCTOS DE PROTECCION COVID 19	331
Productos Covid 19 - Entrega Gratis RM	320
Como volver a la actividad post coronavirus?	314
COVID-19 EMERGENCY DELIVERY OF YOUR CONSIGNMENT BOX TODAY.	305
Re: Hay que adaptarnos a la situacion Covid-19	302
Soluciones para la prevencion del covid19	295
□ - SII- Emergencia de salud Covid-19 38193	290
Re: Nos adaptamos a la nueva situacion Covid-19	283
July 2020 User Feedback & COVID-19 Survey	279
Re: Estamos adaptados a la situacion Covid-19	273
Let’s fight together to get through the COVID-19	267
Re: Tenemos que adaptarnos a la situacion Covid-19	266
Solución contra Covid-19: Medición de temperatura sin contacto	265

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

cl.jooble.org	11665
insideapple.apple.com	3883
countermail.com	1812
gmail.com	1440
timesofindia.com	1437
dpt-awardprize.com	1233
stone.com.br	1045
hotmail.com	650
eastical.cyou	621
digisol.top	597

Top-15 IPs Sending COVID Spam

150.109.54.114	1233
45.118.134.118	1038
201.231.83.188	920
50.3.78.149	621
50.3.78.139	584
201.231.19.222	521
201.134.139.73	504
201.231.83.114	370
167.99.239.38	331
50.255.39.220	311

Top-15 Countries Sending COVID Spam

US	13136
CA	10856
DE	4616
CN	2606
AR	2133
IN	1786
SG	1136
FR	725
GB	633
MX	595

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Fw: COVID-19 STAY AT HOME COMPENSATION	1

Top-15 Subjects Containing doc/xlsx Files

IBTCI Baghdad office-PMSP-IMEP Coronavirus Daily	9
NP. Cruz Roja se apoya en Microsoft Power BI para mostrar la transparencia de su plan Cruz Roja RESPONDE frente a la COVID-19	4
COVID-19 RELIEF FUNDING	3
RE: 2020 COVID-19 Essential Supply Delivery Completion File.xlsx	2
IBTCI COVID-19 Bi-weekly Meeting Agenda (Programs)	2
Re: CA209-8TT - Paquete Covid-19 3 / Varela	2
España ha registrado 22 mascarillas durante el COVID19	2
[editors--peacevoice] submission: op-ed: Margaret Mead, anthropology, civilization, Conflict Transformation, healing and helping, COVID party, Elinor Ostrom, tragedy of the commons	2
People Leadership Amid COVID-19 Virtual Conference	2
Texas School-Based Oral Health Programs and COVID-19	2

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

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: 116,976
Domains with Potential Mail Servers: 2,869
Email-Capable Domains and Hosts: 44,150
Live Hosts and Domains Not Parked: 65,566

Mobile Apps

Apps in Official Stores: 361

by Store

Apple	190
Google	162
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 933

by Store Type:

Hybrid	599
Secondary	295
Affiliate	39

Blacklisted Mobile Apps: 23

by Store Type:

Secondary	20
Official	2
Hybrid	1