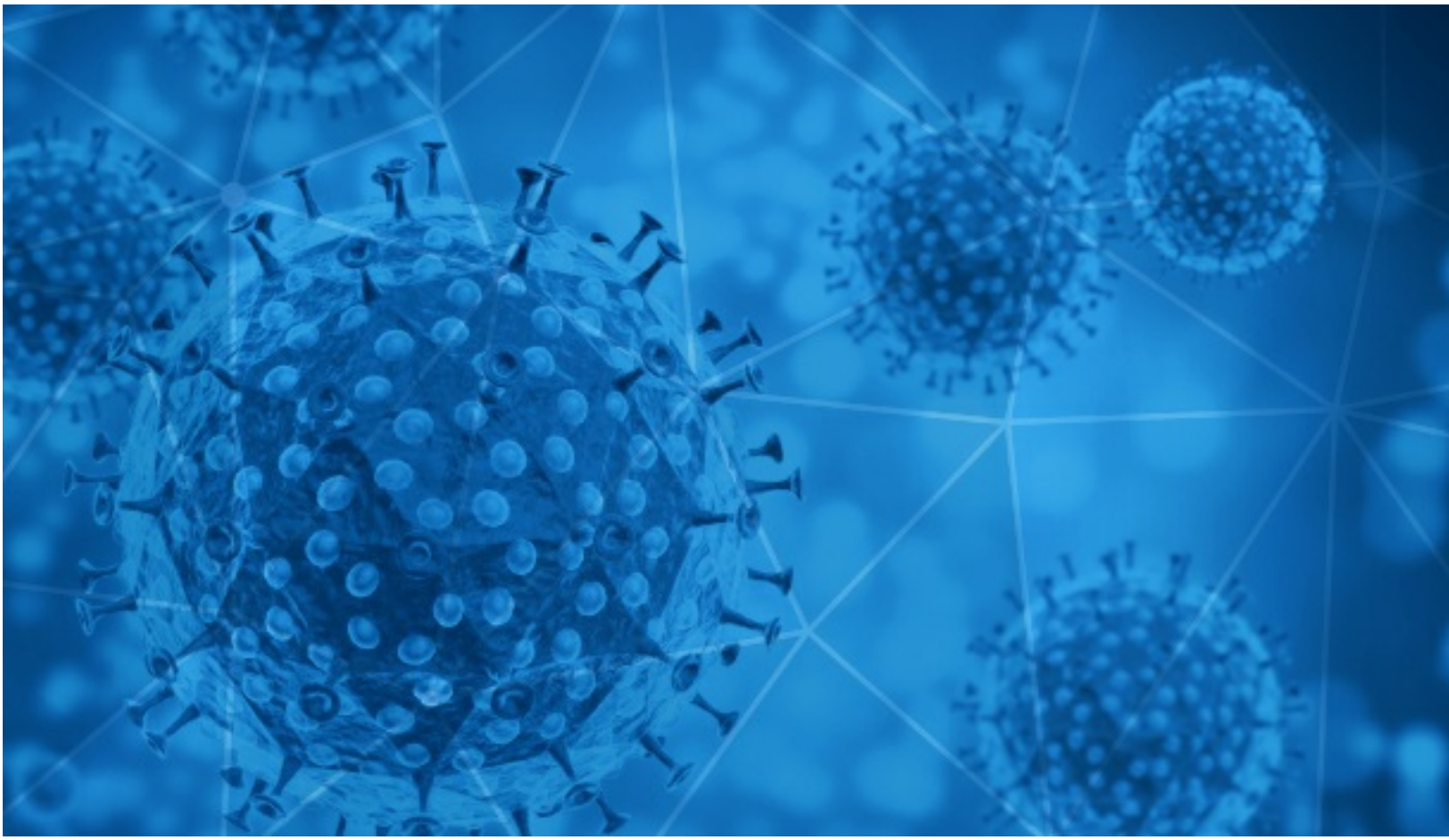
RiskIQ i3:

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

2020-07-14



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 2020-07-13 to 2020-07-14. During this period, RiskIQ analyzed 43,205 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,397 unique subject lines observed during the reporting period. The spam emails originated from 1,909 unique sending email domains and 3,723 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

COVID-19 Update: We are open and now offering Free Virtual Consultations	14367
Test Rapido Covid 10.000 CLP	4707
The Corona Letter: The many risks of the pandemic	2361
PyMEs contra el COVID19	980
Seguridad Sanitaria Frente al COVID-19	684
Re: How do we purchase after the COVID-19?	619
Covid-19 Financial Update	592
Evita el Covid19 en tu lugar de trabajo	534
Mantene tu lugar de trabajo libre de covid19	510
Implacable contra el COVID-19 AMONIOX	481
Kashi's display of hope amid Covid crisis is inspiring, says PM; Addresses India Global Week in London...More in the newsletter!	412
Redeem Your redacted@threatwave.com SBSA-COVID-19-Financial Relief Today	371
Test Rápidos Covid Entrega Inmediata	344
Productos de Sanitizacion y prevencion Covid-19	343
COVID protective gear in stock!	312
Test Rapido COVID 19	304
Productos Prevención Covid-19	294
Let’s fight together to get through the COVID-19	276
IMF COVID-19 DSP	266
Control de Acceso y Temperatura Covid	260
Re: covid-19 protect products we can provide	248
CONGRATULATIONS!!! You Won COVID19 PALLIATIVE ($1.5M)	225
Caretas Faciales anti Covid	215
Re: keep away from Covid-19	207
Congresso Digital Covid-19 é assunto na revista Justiça & Cidadania. Confira!	204

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

wikimedia.org	14367
trendingtopic.cl	5103
timesofindia.com	2362
countermail.com	2024
163.com	1638
gmail.com	1365
correosmasivos.cl	684
126.com	628
webapcode.live	592
serviciosrentables.cl	481

Top-15 IPs Sending COVID Spam

51.77.33.39	1988
51.77.33.43	1021
51.38.159.218	817
51.38.157.47	643
113.116.118.59	643
51.77.33.44	634
45.95.171.91	592
190.247.254.36	566
190.247.243.10	533
164.90.181.158	481

Top-15 Countries Sending COVID Spam

US	9718
FR	7315
JP	3841
BR	3664
IN	3143
AU	2810
CN	2759
AR	2250
DE	1302
--	1152

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

PPE items against Covid-19	9
Fwd: Measures to be taken to contain Covid 19	3
Precizări de presă privind confirmarea unor noi cazuri de infectare cu COVID-19 în rândul turiștilor români aflați în Republica Elenă	3
TALLER GRATUITO VIRTUAL SOBRE AGUA LIBRE DE COVID-19 Y OTROS VIRUS PATÓGENOS - ALADYR	3
COVID-19 RELIEF FUNDING	2
COLUMNA ATREVERSE O MORIR NO HAY PUNTOS MEDIOS PARA LA INDUSTRIA BANCARIA EN TIEMPOS DE COVID	2
Vuelta a la normalidad pos-COVID-19 en pacientes oncológicos	2
Coronavirus/ COVID-19 UPDATE: WE ARE NOW OPEN!	2
COVID 19 LINE LIST	2
Invitation as Speaker to Community Reliance and Response efforts in Handling COVID19' Workshop	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: 114,445
Domains with Potential Mail Servers: 2,800
Email-Capable Domains and Hosts: 43,370
Live Hosts and Domains Not Parked: 66,588

Mobile Apps

Apps in Official Stores: 332

by Store

Apple	178
Google	145
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 884

by Store Type:

Hybrid	560
Secondary	286
Affiliate	38

Blacklisted Mobile Apps: 21

by Store Type:

Secondary	19
Hybrid	1
Official	1