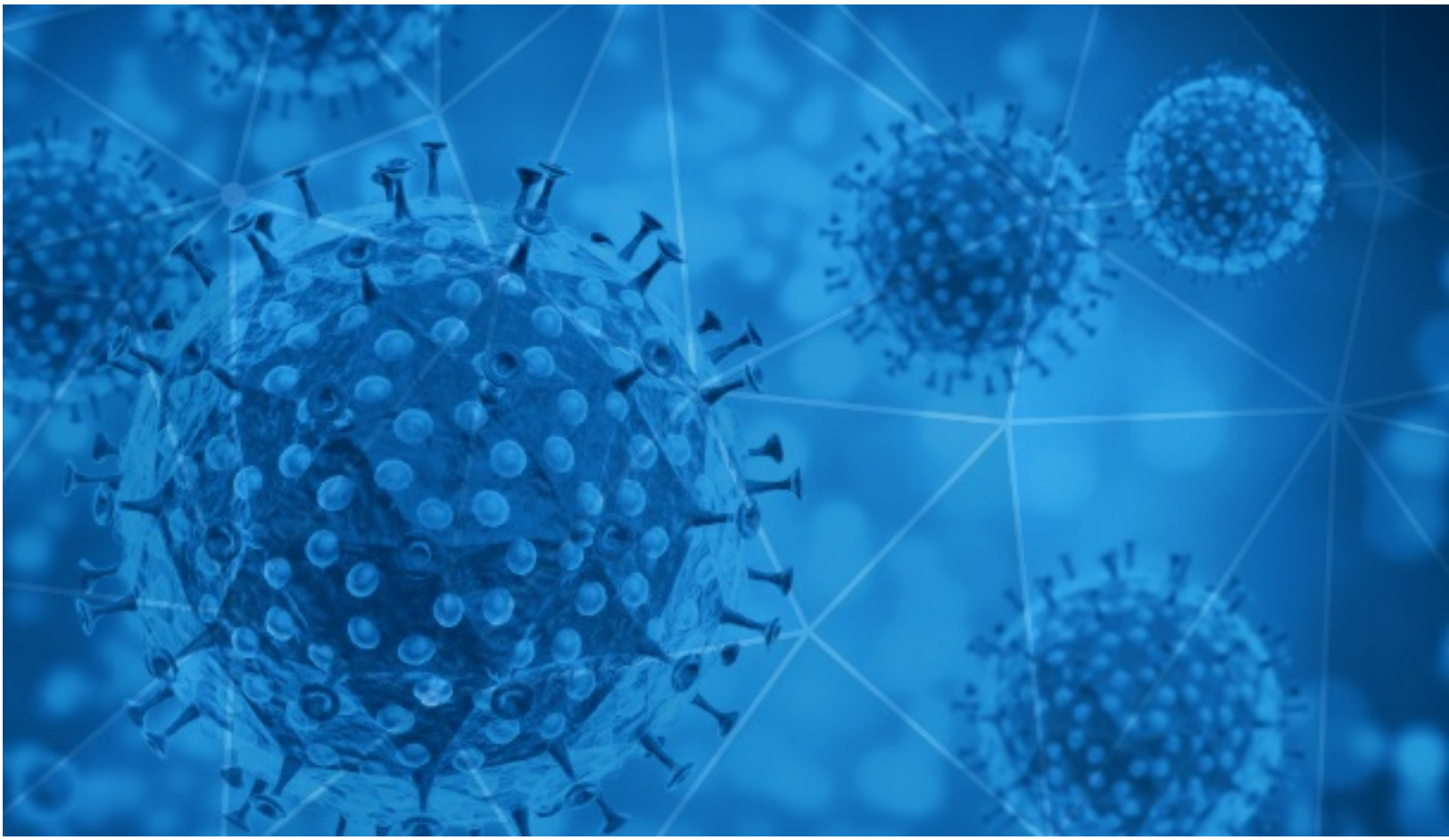
RiskIQ i3:

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

2020-07-21



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 2020-07-20 to 2020-07-21. During this period, RiskIQ analyzed 36,149 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,501 unique subject lines observed during the reporting period. The spam emails originated from 2,764 unique sending email domains and 3,435 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

We Produce Covid-19 (Face Mask,Isolation Gown,Head/Shoe/Sleeve Cover,Vinyl Gloves ,PE Gloves,Apron)	4292
TIMES TOP10: India's deadliest week of Covid	2972
Re : Re: COVID-19 Give away	2703
Re: COVID-19 Give away	2015
Worried about your bills due to COVID-19?	1843
The Corona Letter: When price caps start hurting businesses…	1816
{COVID-19} □□□□□□□□□□□□□□□□□	1321
PyMEs contra el COVID19	875
Covid-19-Hilfsfonds	659
Redeem COVID-19 Financial Relief Funds Today redacted@threatwave.com,	607
Japanese Arcades Exerting Utmost Coronavirus Caution - Sankaku News	568
Alertan nuevos sintomas: 15 minutos para saber si eres positivo o negativo de COVID-19	551
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	537
Re: How do we purchase after the COVID-19?	415
Epp, Termómetros, Test Covid19 y Test de Drogas	336
Como volver a la actividad post coronavirus?	333
Productos Covid 19 - Entrega Gratis RM	333
Test Rapido Covid 10.000 CLP	321
Cabinas para la prevencion del coronavirus?	316
Soluciones para la prevencion del covid19	312
United Nations Covid-19 Palliative/Financial Support/Congratulations.	267
COVID-19 - Projects | Website | Mobile Application | E-Commerce | SEO (Results Guaranteed) [REDACTED_DOMAIN]	261
My COVID-19 Donation	252
Re: BT earbuds/ How to do the purchase after COVID-19?	232
Zombie Land Saga Stage Play Rescheduled Because of Coronavirus - Sankaku News	222

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

onet.eu	4718
protonmail.com	4292
gmail.com	3178
bounce.indiatimes.com	2972
countermail.com	1836
timesofindia.com	1821
163.com	1676
toyotacarrr.com	1321
sankakucomplex.com	790
fnbcorporate.co.za	620

Top-15 IPs Sending COVID Spam

103.141.137.241	4718
216.223.71.246	4292
190.247.226.151	1013
113.116.70.198	858
162.243.55.70	801
208.100.24.254	790
92.198.23.110	607
181.46.136.165	537
201.231.5.19	472
223.73.108.112	460

Top-15 Countries Sending COVID Spam

US	7435
IN	5692
--	4842
CA	4829
CN	2446
AR	2418
JP	1702
DE	1383
FR	855
AU	650

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

PHHS 7 20 2020 COVID 19 End of Day Summary	6
GlobalSurg-CovidSurg Week study: invitation	2
IMPACTO DA PANDEMIA COVID-19 NO SONO DOS PORTUGUESES É MAIOR JUNTO DAS MULHERES	2
NP_Expertos señalan la urgencia en la protección de los pacientes con demencia y la continuidad de los estudios clínicos en el marco de la pandemia de la COVID19	2
COVID-19 E DANNI NEUROLOGICI: ATTENZIONE SÌ MA NIENTE ALLARMISMI. La SIN fa chiarezza sul NeuroCovid: possibilità di conseguenze remote e non dimostrate	2
Re: Briefing to SIDS PRs on the World Bank Group COVID-19 Response and Recovery (1 July 2020, 1:00 pm – 2:15 pm)	2
Boletim Diário COVID-19 - 20/7/2020 - 10h00	2
PERAK COVID-19 TRAINING FOR INDUSTRY & SECTOR STAFF	2
COVID-19 RELIEF FUNDING	2
En México, se cancelan más 15 mil cirugías por semana debido a la pandemia por Covid-19	1

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: 115,380
Domains with Potential Mail Servers: 2,821
Email-Capable Domains and Hosts: 43,639
Live Hosts and Domains Not Parked: 64,919

Mobile Apps

Apps in Official Stores: 351

by Store

Apple	187
Google	155
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 902

by Store Type:

Hybrid	575
Secondary	289
Affiliate	38

Blacklisted Mobile Apps: 22

by Store Type:

Secondary	19
Official	2
Hybrid	1