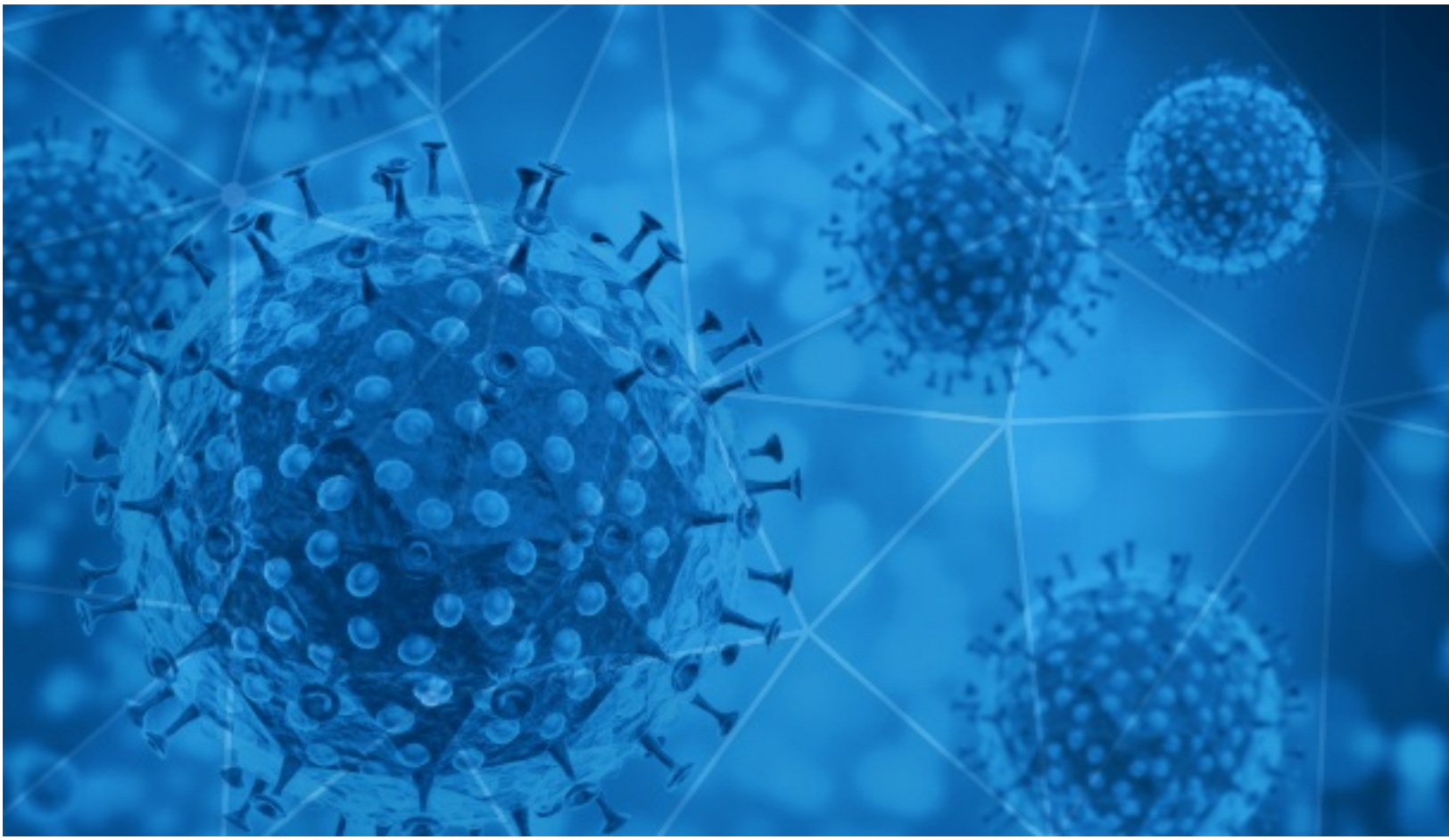
RiskIQ i3:

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

2020-07-15



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 2020-07-14 to 2020-07-15. During this period, RiskIQ analyzed 36,290 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,825 unique subject lines observed during the reporting period. The spam emails originated from 1,840 unique sending email domains and 3,985 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	12574
The Corona Letter: Covid treatments and India's challenges	2378
DPI linea fase3 covid-19 protezione e igiene	836
Re: How do we purchase after the COVID-19?	726
PyMEs contra el COVID19	627
COVID protective gear in stock!	610
Control de Acceso y Temperatura Covid	557
Test Rapido Covid 10.000 CLP	543
Covid-19-Hilfsfonds	352
Productos Covid 19 - Entrega Gratis RM	312
IMF COVID-19 DSP	307
Re: covid-19 protect products we can provide	274
Productos de Sanitizacion y prevencion Covid-19	267
Caretas Faciales anti Covid	253
1...VITAL INFORMATION ABOUT COVID 19...	247
Productos disponibles Covid	246
Re: Estamos adaptados a la situacion Covid-19	238
Re: Hay que adaptarse a la nueva situacion Covid-19	229
Re: Nos adaptamos a la nueva situacion Covid-19	225
Re: Tenemos que adaptarnos a la situacion Covid-19	222
Re: Hay que adaptarnos a la situacion Covid-19	221
Re: Nos tenemos que adaptar a la situacion Covid-19	218
Re: Your Covid-19 Economic Relief Payment !	211
Re: Estamos adaptados a la nueva situacion Covid-19	211
Let’s fight together to get through the COVID-19	210

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

toyotacarrr.com	12578
timesofindia.com	2380
163.com	1674
gmail.com	1295
stone.com.br	1051
trendingtopic.cl	855
sicurezzanews.it	836
countermail.com	816
126.com	589
tidair.com	509

Top-15 IPs Sending COVID Spam

187.108.198.226	980
103.225.52.236	639
103.225.54.74	522
82.135.19.130	472
223.73.108.89	441
113.116.118.59	383
113.118.173.77	381
103.225.53.198	377
82.135.19.131	364
202.90.240.33	352

Top-15 Countries Sending COVID Spam

JP	13095
US	5118
DE	3111
IN	2687
CN	2607
FR	2075
BR	1093
AR	1051
CL	810
ES	693

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Οδηγοί για την πρόληψη/περιορισμό του δεύτερου κύματος covid -19 σύμφωνα με τις οδηγίες του συστήματος υγείας (ΠΟΥ)	1

Top-15 Subjects Containing doc/xlsx Files

CORONA Raksha Policy by IFFCO TOKIO	4
Corona Kavach from IFFCO TOKIO	3
anefp lanza la campaña 'Sé responsable. Cuídate' apelando al autocuidado responsable como clave para luchar contra los rebrotes de la COVID-19	2
PR _ Medallion Associates _ Institutional investors can offer fresh boost to real estate investments post Covid-19 _ English	2
Пожертвовали плазму крови на $83 млрд для лечения COVID-19. В ответ - репрессия прав человека. Ю. Корея. Пресс-релиз, фото.	2
Parent Letter COVID 19 14 July 2020	2
NdP_Legionelosis, cuando la Covid-19 se mira al espejo	2
A global increase of shelf stable milk demand since COVID-19 pandemic - Zaki Group launches locally produced liquid dairy in SIG Combibloc Obeikan's family size combidome	2
Fwd: COVID-19: Zimbabwe entry requirement	1
NP SANTALUCÍA lucha contra la brecha digital provocada por el 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: 114,623
Domains with Potential Mail Servers: 2,805
Email-Capable Domains and Hosts: 43,405
Live Hosts and Domains Not Parked: 66,608

Mobile Apps

Apps in Official Stores: 333

by Store

Apple	177
Google	147
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 889

by Store Type:

Hybrid	565
Secondary	286
Affiliate	38

Blacklisted Mobile Apps: 22

by Store Type:

Secondary	19
Official	2
Hybrid	1