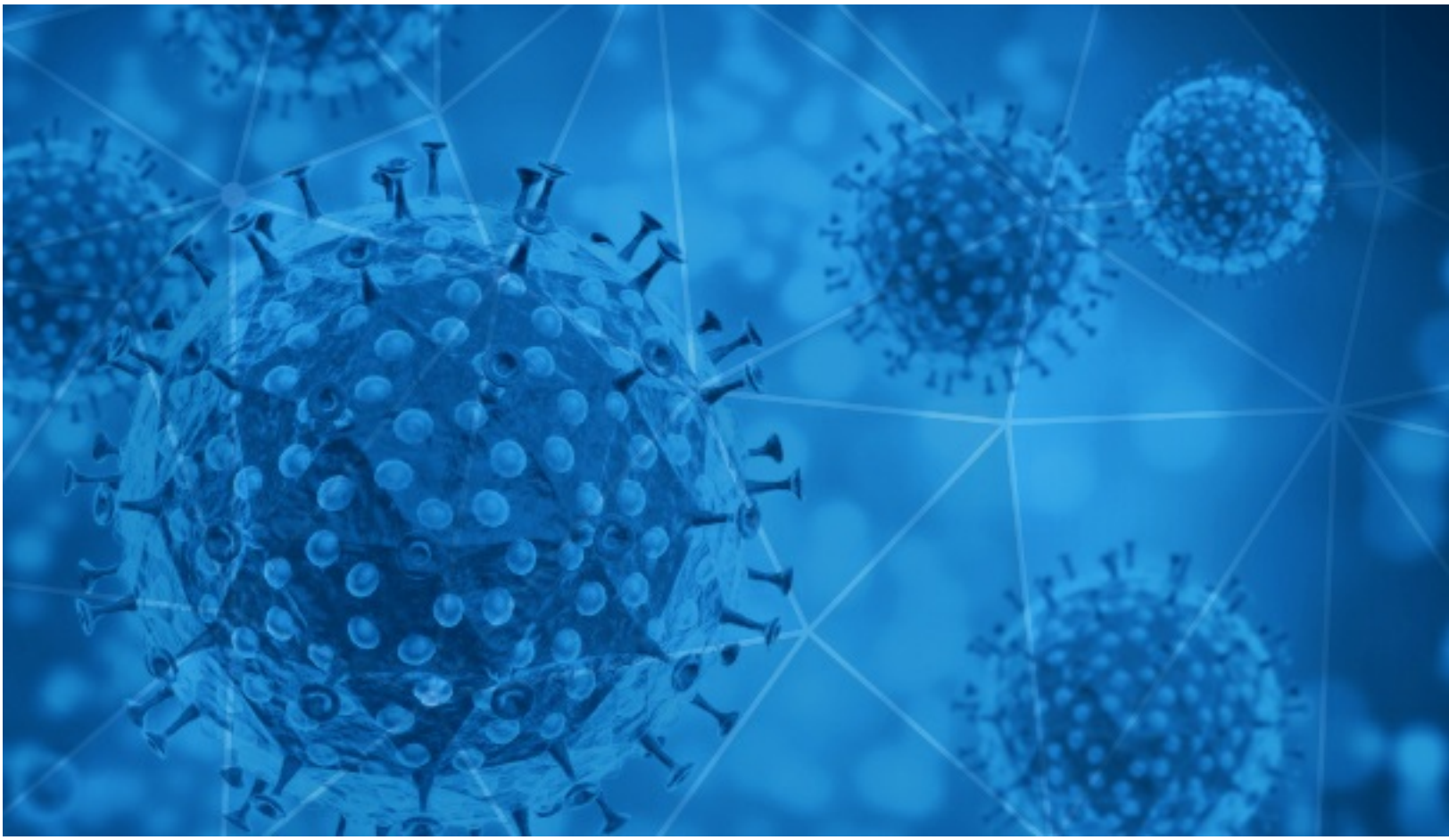
RISKIQ®

RiskIQ i3:

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

2020-07-03



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 2020-07-02 to 2020-07-03. During this period, RiskIQ analyzed 56,058 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,621 unique subject lines observed during the reporting period. The spam emails originated from 2,812 unique sending email domains and 4,927 unique SMTP IP Addresses. Analysts identified 30 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	21410
My COVID-19 Donation.	2510
The Corona Letter: How bad was June worldwide?	2404
MICROSOFT CORONAVIRUS RELIEF FUND	1375
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	1271
Implacable contra el COVID-19 AMONIOX	1175
Oferta Test Rápidos COVID-19, Mascarillas, Alcohol Gel y Amonio Cuaternario.	1066
APLICACIÃN PRUEBAS RÃPIDAS COVID-19: CÃ³mo funcionan y cÃ³mo se aplican	657
COVID-19 SPENDE FÜR SIE	611
Sistema de detección Térmico Contra Covid-19	534
Rencontrer des femmes (édition Corona)	523
High-quality Disposable Medical Kit, which are reliable products protecting from COVID-19	492
Insumos de Protección COVID-19	483
Test Rápido COVID-19	445
Steunfonds (COVID-19)	419
Caretas anti Covid-19	406
D.L. Hughley Unknowingly Spread COVID-19 To His SON & Entire Team {VIDEO} I Should’ve Killed U Bch**	404
IMF COVID-19 DSP	332
Korea Trend News-COVID19(4)	327
COVID-19 - Custom Projects | Mobile Application | SEO !! -etc [REDACTED_DOMAIN]	286
Re: Supply Protection products against COVID-19	259
Minimice el Riesgo de contagio del Coronavirus - Validacion Biometrica	258
Long Lasting and Eco-Friendly Disinfectant to Fight Covid19…	250
Re: keep away from Covid-19	228
COVID-19 RELIF FUNDS OF £5,950 million	214

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	21412
gmail.com	5366
timesofindia.com	2404
126.com	1748
163.com	1354
outlook.com	1337
serviciosrentables.cl	1175
correosmasivos.cl	1066
tecnologia-organizacional.com	658
zohomail.eu	570

Top-15 IPs Sending COVID Spam

187.174.101.179	2510
45.237.96.13	1375
119.122.89.94	1271
159.89.80.159	1175
51.38.133.70	788
150.254.241.245	644
159.65.80.166	534
5.199.131.165	523
103.225.55.27	483
103.225.54.166	453

Top-15 Countries Sending COVID Spam

JP	21568
US	9975
CN	3231
IN	3187
MX	2529
DE	2069
FR	1922
--	1602
GB	1428
PL	809

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

New Order Project/Covid	18
Fwd: New Order Project/Covid	5
VOTRE DEMANDE DE REPORT COVID 19 - WAFA IMMOBILIER	3
METERIALS EQUIPMENT NEEDED/COVID	2
TR: VOTRE DEMANDE DE REPORT COVID 19 - WAFA IMMOBILIER	1

Top-15 Subjects Containing doc/xlsx Files

BHP – obowiązki pracodawcy i pracownika w dobie Covid 19	7
Inteligencia Artificial: combinación de algoritmos que salva vidas frente a la pandemia de Covid-19	4
Covid-19 Related Products Price List	3
Inteligencia Artificial:combinación de algoritmos que salva vidas frente a la pandemia de Covid-19	3
VOTRE DEMANDE DE REPORT COVID 19 - WAFA IMMOBILIER	3
Covid Health Screening Questionnaire	3
“Customer First Marketing” é a grande tendência na era pós COVID-19	2
APLICATIVO INFRAESTRUCTURA COVID 19	2
NdP_Binance Charity dona a España 15000 trajes protectores y 31200 mascarillas frente al COVID-19	2
Accu-Tell® COVID-19 IgG/IgM Rapid Tests & VTM/VTM-N Virus Collection and Transport Kits	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: 111,528
Domains with Potential Mail Servers: 2,792
Email-Capable Domains and Hosts: 42,224
Live Hosts and Domains Not Parked: 54,160

Mobile Apps

Apps in Official Stores: 313

by Store

Apple	174
Google	130
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 835

by Store Type:

Hybrid	524
Secondary	275
Affiliate	36

Blacklisted Mobile Apps: 20

by Store Type:

Secondary	19
Official	1