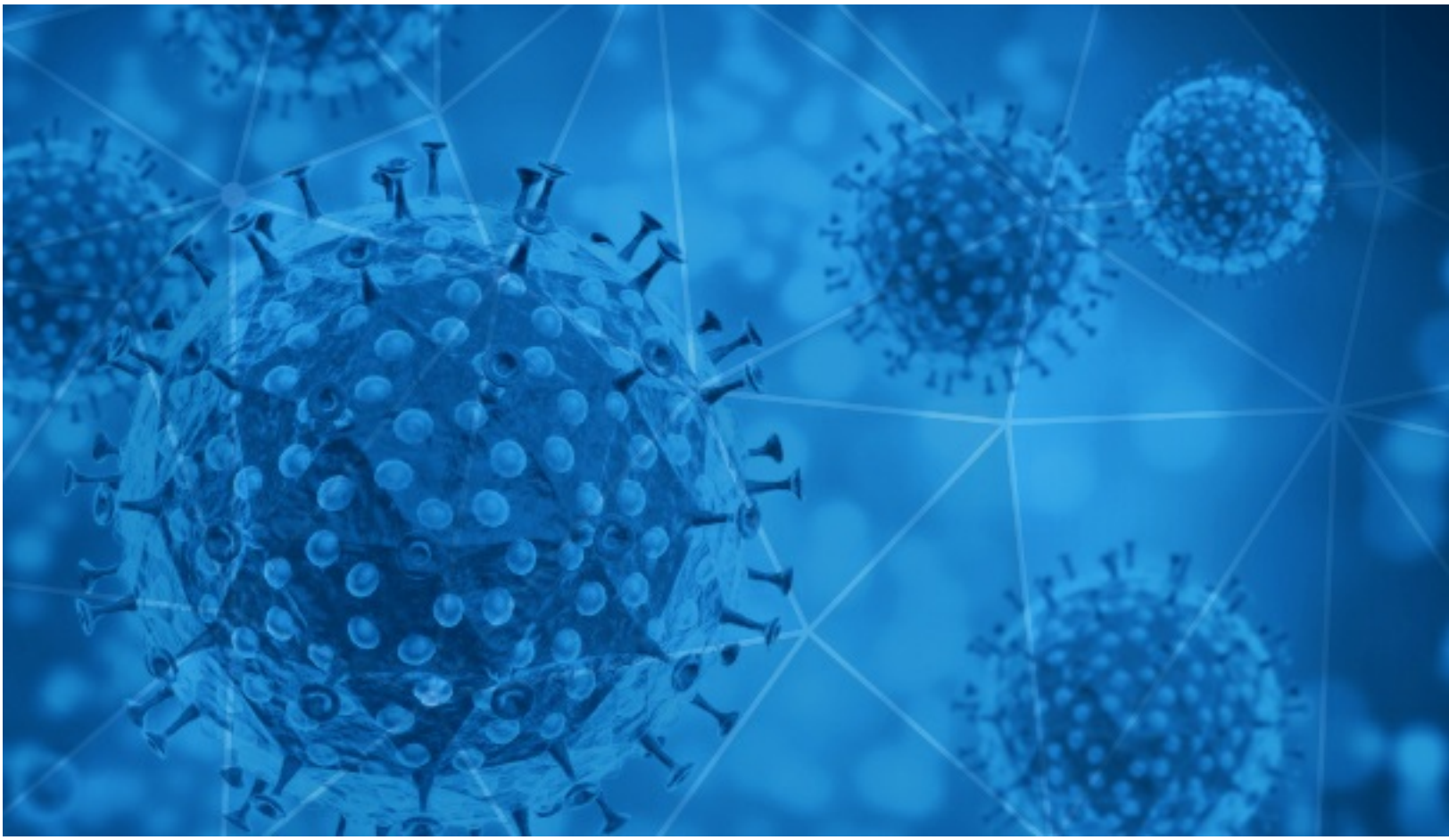
RiskIQ i3:

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

2020-06-08



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 2020-06-07 to 2020-06-08. During this period, RiskIQ analyzed 31,517 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,639 unique subject lines observed during the reporting period. The spam emails originated from 1,190 unique sending email domains and 2,848 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: What should hospitals charge from Covid patients?	3711
Elija su Kit de PROTECCION Covid19	1670
COVID-19 Financial UPDATE!	1581
AID TO NAVIGATE COVID-19	1537
BANNED GOODS DUE TO COVID 19 PANDEMIC	1264
COVID-19-Responder	941
Covid19- Compensation Payment Notice.	912
Rencontrer des femmes (édition Corona)	806
Mamparas de proteccion contra el coronavirus	789
Mamparas de proteccion COVID19	760
CORONAVIRUS RELIEF FUND (CRF) 2020	616
Elija su Kit de protección Covid19	607
GrooveSell is now Free. Because of COVID-19, it's free for life.	596
Insumos - Protección COVID 19	525
Compilation of Important Announcements webhosted for CA Members, Students & ICAI Employees in the wake of Coronavirus COVID-19	436
COVID-19 - Custom Projects | Mobile Application | SEO !! -etc [REDACTED_DOMAIN]	424
Test COVID-19 Aprobados por el ISP	358
Protectores Faciales . Anti Covid 19	348
POST CORONA LOAN OFFER	301
Korea Trend News-COVID19-2	273
Re: COVID-19 Financial Relief Funds for you	237
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	226
STAY SAFE CORONA-VIRUS (COVID 19) IS REAL!!!	224
COVID-19 Response Fund	198
Re: Surgical & Medical Mask for Coronaviruse / China Qualified	177

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	3711
gmail.com	2625
outlook.com	2295
frontsight.com	1880
trendingtopic.cl	1670
platinumfinance.info	1581
countermail.com	1549
ex.ua	1537
163.com	1371
gov.org	1263

Top-15 IPs Sending COVID Spam

209.123.15.146	1875
101.200.184.113	1537
133.167.123.176	1068
175.107.198.38	941
91.143.80.127	912
5.199.131.165	806
207.38.83.40	652
82.80.49.148	616
51.77.33.44	585
51.38.159.218	492

Top-15 Countries Sending COVID Spam

US	7779
IN	4287
CN	3942
FR	2530
DE	2473
AR	1804
JP	1256
PK	941
ES	817
IL	644

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

MEDIA RELEASE [Learn, play, and earn: Access Bank's COVID-19 message to children]	5
Imprtant - post-coronavirus	3
circolare 20.2020 bonus Covid	3
[editors--peacevoice] submission: op-ed: COVID-19, stress, conflict, mindfulness, meditation, compassion	2
PLANILHA COM A PROGRAMAÇÃO DE NOVAS DESPESAS COVID-19 SESAP RN	2
Covid-19 Related Products Price List	2
COVID-19 SONRASI NORMALLEŞME SÜRECİ ARAŞTIRMASI	2
Camilo Lagos y alta cifra de fallecidos por Covid-19: "Hace dos meses llamábamos al gobierno y a la sociedad a parar el país para no quedarnos sin país"	2
INTERNATIONAL CANCER SURVIVORS DAY 2020: COVID-19 AS A WAKE-UP CALL	2
Protocole 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: 103,534
Domains with Potential Mail Servers: 2,669
Email-Capable Domains and Hosts: 39,631
Live Hosts and Domains Not Parked: 41,409

Mobile Apps

Apps in Official Stores: 287

by Store

Apple	166
Google	113
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 644

by Store Type:

Hybrid	391
Secondary	225
Affiliate	28

Blacklisted Mobile Apps: 19

by Store Type:

Secondary	18
Official	1