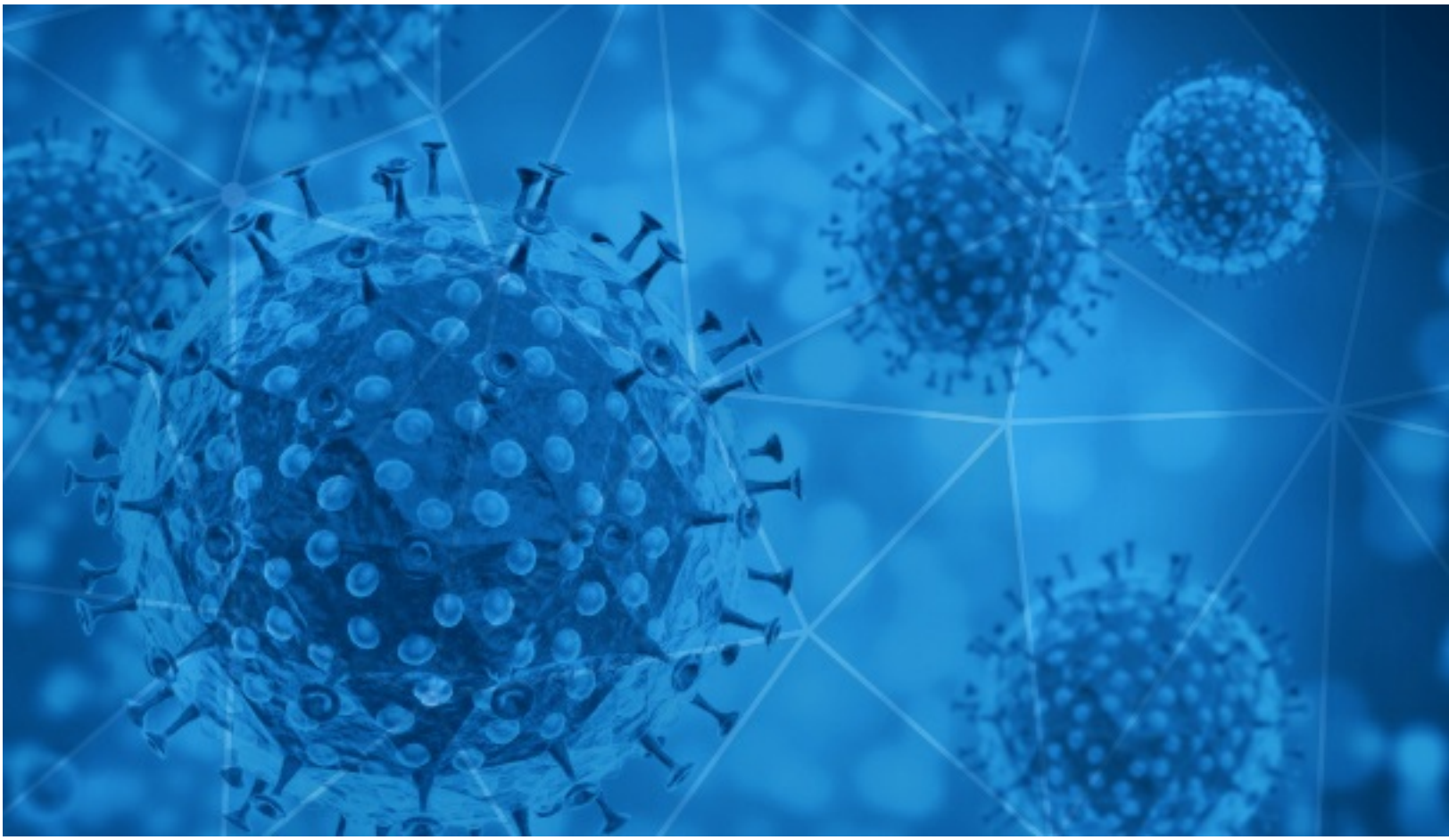
RiskIQ i3:

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

2020-06-01



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 2020-05-31 to 2020-06-01. During this period, RiskIQ analyzed 31,579 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,989 unique subject lines observed during the reporting period. The spam emails originated from 2,233 unique sending email domains and 4,874 unique SMTP IP Addresses. Analysts identified 6 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Antibody tests are back	3149
Test Rapido Covid 19	2107
Last Chance: COVID19 Offer -85%	1550
COVID-19 Financial UPDATE!	1393
Miracle Corona Cash Gifted By The Universe (YES!)	1125
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	1016
Standard Bank COVID-19 Payment Relief Funds Approved	741
Coronavirus Relief,	567
Re: COVID-19 Financial Relief Funds for you	527
WARNING! COVID-19 Patient Near You..	518
Protejase del Covid-19, Productos Certificados	508
Covid-19!!!	488
(COVID-19) DONATION	483
Sale Masks , Corona Virus test Kit,Ventilator machine and Protective Clothing with quality certificates.	349
Covid 19 Wohltätigkeitsfonds	334
HELP USE THIS FOR COVID-19	321
Mamparas de proteccion COVID19	314
Mamparas de proteccion contra el coronavirus	296
Covid Cash Cow $1,500+ Weekly	278
COVID-19 EMERGENCY DELIVERY OF YOUR CONSIGNMENT BOX TODAY.	241
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO ANTE EL COVID19	241
Desinfección para prevenir el COVID-19 - proteja su hogar, oficina y comercio	218
Order Number:COVID19REF	215
Covid19 Relief Business Loan support	212
Re: Medical Mask for Coronaviruse	211

- CONFIDENTIAL -

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmail.com	3486
timesofindia.com	3150
trendingtopic.cl	2147
126.com	1818
yellowpagescloud.net	1605
163.com	1579
platinumfinance.info	1393
outlook.com	1226
mainfestationmagicnewkj.us	1125
standardbank.co.za	741

Top-15 IPs Sending COVID Spam

80.211.76.14	1260
142.11.230.52	1125
51.77.33.44	985
119.122.88.96	780
82.222.61.135	741
51.77.33.39	583
192.254.176.196	567
207.38.83.48	538
85.114.7.186	527
51.38.159.218	492

Top-15 Countries Sending COVID Spam

US	7963
CN	4796
IN	3636
FR	3095
IT	1881
DE	1319
AR	902
TR	897
RU	676
EC	592

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

COVID-19 Update	5

Top-15 Subjects Containing doc/xlsx Files

Financial Accounting Impact of COVID-19- An In-depth Look at IFRS	49
Invitación Encuesta Salarial ElEmpleo 2020 | Capitulo Especial Covid-19	5
COVID POSITIVE REPORTING	2
05.29.2020 TeamAmerica Hotel Closures_Extensions_Updates_Covid19_No14	1
LAPORAN COVID 19 SELENDANG 2	1
Press Release: LetsGetChecked Debuts FDA EUA-Authorized At-Home Coronavirus (COVID-19) Sure-track Test - Order #52227611	1
Mise à jour données Post Covid 19	1
Bonificación ayuda Covid19	1
Parish Pastoral Update- Parish Priest- Covid 19- 31 May 2020	1
5/31/ Update Coronavirus cases data	1

- CONFIDENTIAL -

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: 101,445
Domains with Potential Mail Servers: 3,033
Email-Capable Domains and Hosts: 38,506
Live Hosts and Domains Not Parked: 41,132

Mobile Apps

Apps in Official Stores: 280

by Store

Apple	163
Google	109
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 597

by Store Type:

Hybrid	354
Secondary	215
Affiliate	28

Blacklisted Mobile Apps: 19

by Store Type:

Secondary	18
Official	1