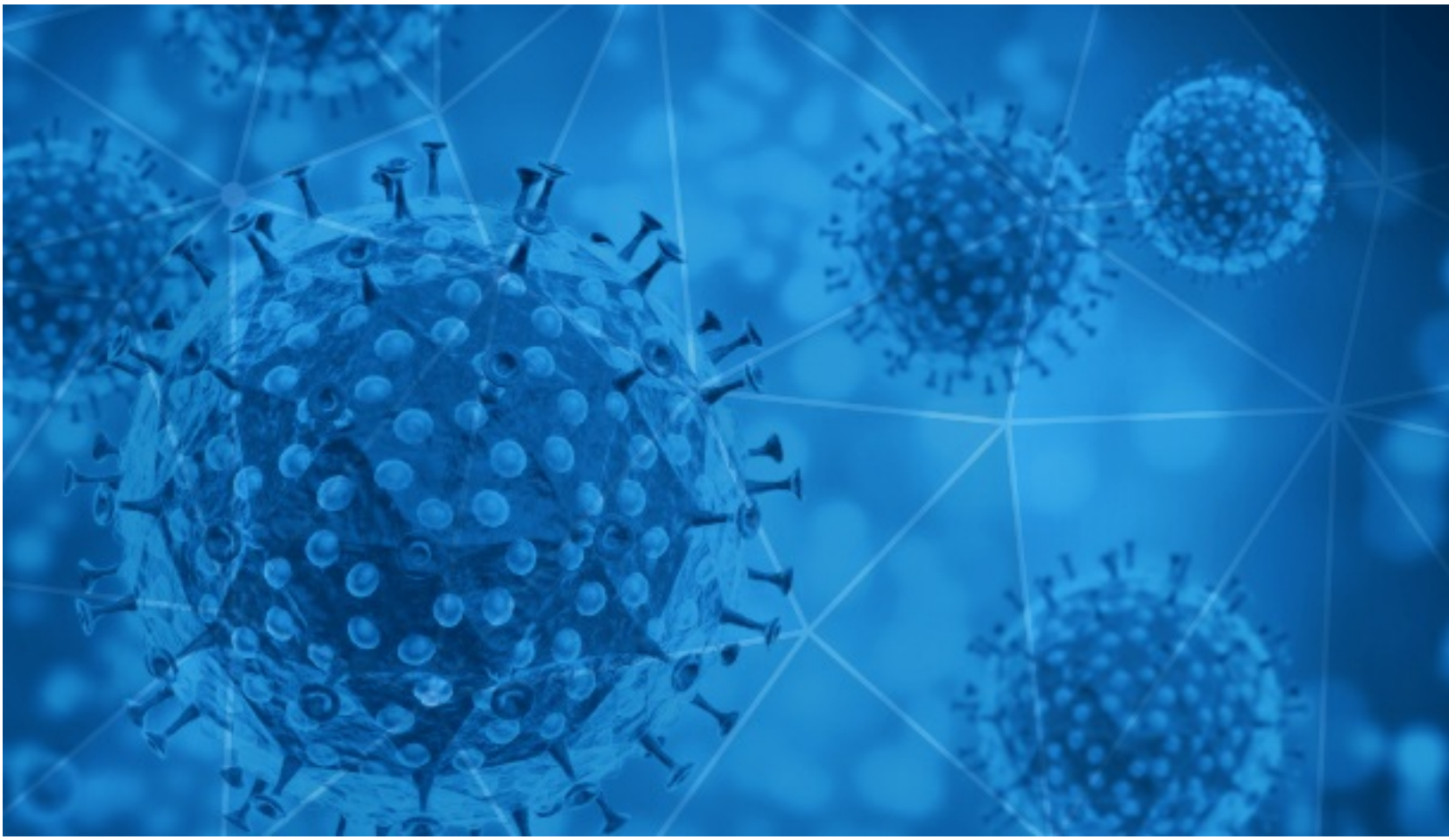
RiskIQ i3:

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

2020-06-09



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 2020-06-08 to 2020-06-09. During this period, RiskIQ analyzed 43,570 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,384 unique subject lines observed during the reporting period. The spam emails originated from 2,610 unique sending email domains and 4,950 unique SMTP IP Addresses. Analysts identified 82 emails which sent an executable file for Windows machines.

Top-25 Subjects

Jack Ma joins Africa CDC in online medical exchange session on COVID19	6690
AID TO NAVIGATE COVID-19	3706
The Corona Letter: The added cost of unlocking urban India	3153
Elija su Kit de PROTECCION Covid19	2447
Cursos En Linea - Sobre Proteccion al Empleo Modificaciones a la Ley Covid19	1812
{COVID-19} □□□□□□□□□□□□□□□□	1545
Products for COVID-19	801
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	756
COVID-19 - Custom Projects | Mobile Application | SEO !! -etc [REDACTED_DOMAIN]	750
BANNED GOODS DUE TO COVID 19 PANDEMIC	710
The COVID-19 Response Fund	468
Insumos Protectores Covid-19 Despachos a Todo Chile	443
Mamparas de proteccion contra el coronavirus	397
Mamparas de proteccion COVID19	341
3 minutes to fight COVID	324
Six high-paying jobs to watch out in the times of COVID-19	316
Korea Trend News-COVID19-2	227
Evite Covid 19, Soluciones de Acceso, Asistencia, Casino y Más	225
Covid-19 read and reply my bequest	203
Charter Air Service/Fast Air service/Mask /Covid-19 test/Medical equipment	199
Covid-19 RBI Relief Package on Working Capital Advances Deferment of Interest for March 2020	198
Elija su Kit de protección Covid19	191
How COVID-19 is impacting your local housing market 2020 Top Performing Realtors Near You	174
Ley de Contrataciones del Estado Elaboración de Requerimientos Covid-19	164
Productos de proteccion Anticovid	161

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

service.alibaba.com	6690
ex.ua	3710
timesofindia.com	3246
gmail.com	2771
trendingtopic.cl	2447
proteccionalempleoleycovid19.com	1812
toyotacarrr.com	1545
163.com	1294
126.com	1102
outlook.com	789

Top-15 IPs Sending COVID Spam

101.200.184.113	3710
207.154.221.139	1812
51.38.159.218	877
95.211.208.25	782
209.123.15.146	765
133.167.123.176	611
51.77.33.43	588
142.11.209.110	468
119.122.90.135	462
51.77.33.39	460

Top-15 Countries Sending COVID Spam

CN	13653
US	7156
IN	5394
FR	3309
DE	2820
JP	2632
NL	1098
AR	926
CA	695
GB	675

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

REQUEST FOR QUOTE// COVID-19 CIVIL RELIEF PROJECT, CANADA	69

Top-15 Subjects Containing doc/xlsx Files

PROTEGE A TU EMPRESA FRENTE AL COVID	12
NdP El intercambio de casas multiplica su demanda por 10 tras la crisis del Covid-19 y se consolida como nuevo modelo turístico	11
MEDIA RELEASE [300 Naira is the average amount spent on helping a person a day – BeatingCoronaAfrica breaks down Nigeria's COVID-19 interventions]	5
Covid-19 Related Products Price List	4
2020-05-14_Corona_Meldung Notbetreuung_eingeschränkter Regelbetrieb_Bereich FBBE.xlsx	3
COVID 19- INTERNAMIENTO HOSPITAL ANTONIO LORENA	3
PEOPLE'S WATCH ANDHRA PRADESH Telegraph Editorial to PM Letter, Mega Bungling & Covid19	2
PRESENTATION BY MR. MANOJ BHATT - Webinar on "nCOVID 19: Impact on and Future of Indian Economy"	2
Fwd: V/v hướng dẫn lập hồ sơ đề nghị hỗ trợ người dân gặp khó khăn do đại dịch Covid-19	2
NP. NUEVA APLICACIÓN DE MINDFULNESS COMO HERRAMIENTA DE APOYO A LA GESTIÓN EMOCIONAL DEL COVID-19	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: 103,535
Domains with Potential Mail Servers: 2,673
Email-Capable Domains and Hosts: 39,631
Live Hosts and Domains Not Parked: 41,390

Mobile Apps

Apps in Official Stores: 288

by Store

Apple	166
Google	114
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 648

by Store Type:

Hybrid	393
Secondary	227
Affiliate	28

Blacklisted Mobile Apps: 20

by Store Type:

Secondary	19
Official	1