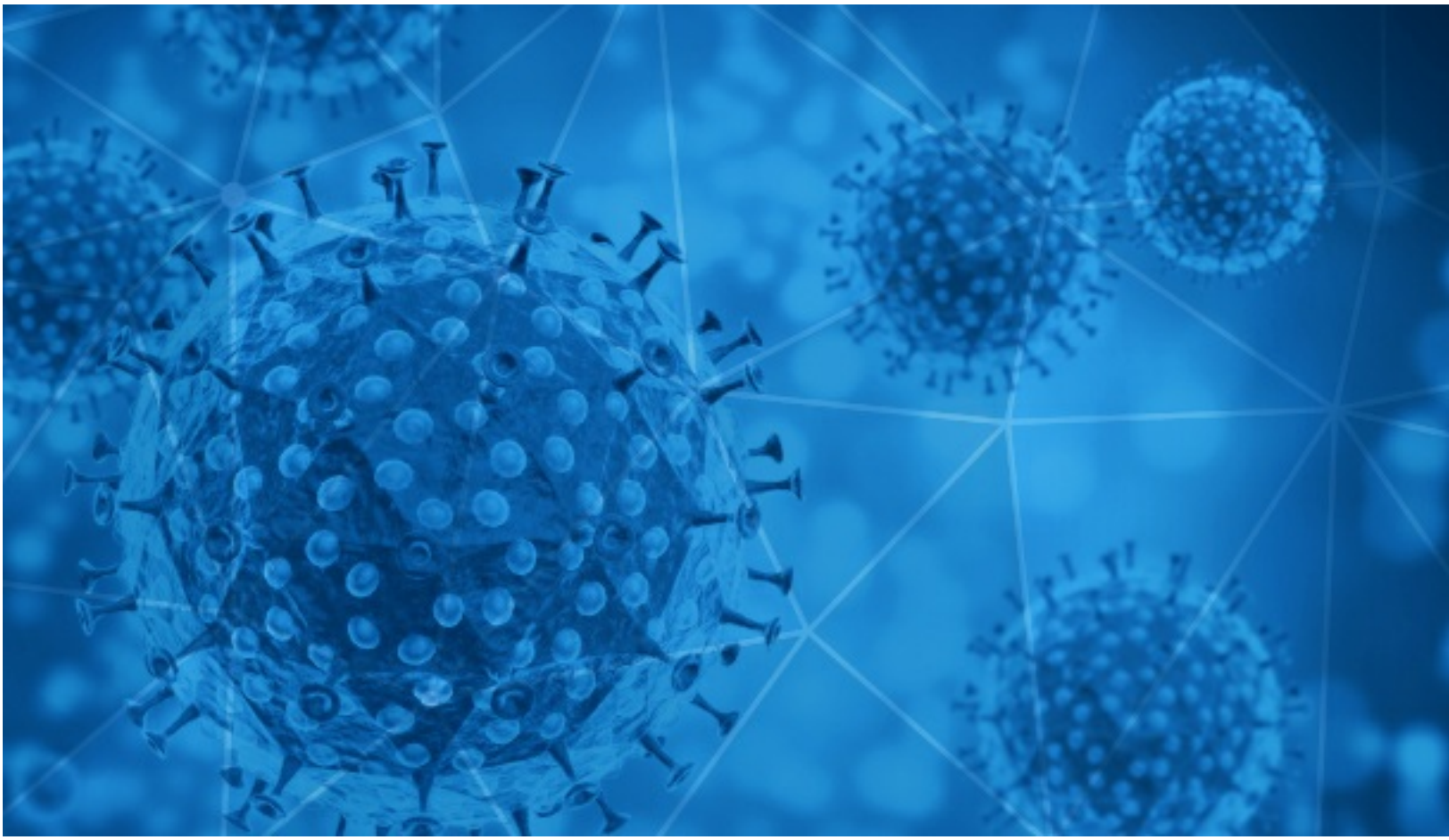
RiskIQ i3:

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

2020-06-10



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 2020-06-09 to 2020-06-10. During this period, RiskIQ analyzed 27,624 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,223 unique subject lines observed during the reporting period. The spam emails originated from 2,053 unique sending email domains and 3,673 unique SMTP IP Addresses. Analysts identified 2 emails which sent an executable file for Windows machines.

Top-25 Subjects

Manifest Corona Cash?	3964
Paneles anti Covid-19 para atención de Público.	1887
AFFORDABLE LOAN OFFER FOR COVID-19.	1057
Jack Ma joins Africa CDC in online medical exchange session on COVID19	894
Insumos Protectores Covid-19 Despachos a Todo Chile	768
Products for COVID-19	758
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	668
COVID-19 - Custom Projects | Mobile Application | SEO !! -etc [REDACTED_DOMAIN]	666
Productos Prevención Covid-19	503
Kits Protectores Reutilizables COVID-19	459
Evite Covid 19, Soluciones de Acceso, Asistencia, Casino y Más	439
Cursos En Linea - Sobre Proteccion al Empleo Modificaciones a la Ley Covid19	377
Riesgos de Lavado de Dinero por el COVID-19	362
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	329
Elija su Kit de PROTECCION Covid19	323
Re: CONGRATULATIONS!!! You Won Bitcoin For Covid 19	320
LOAN RELIEF FOR COVID-19 AFFECTED INDIVIDUAL AND BUSINESSES.	315
COVID 19 Compensation Fund. Open the attached file!!!!!	305
“Plan Protección Covid-19”	250
CONGRATULATIONS!!! You Won Bitcoin For Covid 19	233
COVID-19 / DONATION FOR YOU	207
Campaña Covid 19	187
EXCELENTES MASCARILLAS DE PROTECCIÓN FACIAL COVID-19	186
Mamparas de proteccion COVID19	185
While Media Focuses on Protests, Stunning Coronavirus Update Emerges	184

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

moneyboost.icu	3964
gmail.com	3107
publica20.club	1887
freedommarketinvestments.com	1057
service.alibaba.com	894
126.com	843
insumosprotectorescovid19.com	768
163.com	742
focazen.com	578
aol.com	554

Top-15 IPs Sending COVID Spam

75.75.231.4	3964
160.20.147.106	1887
198.72.105.132	1057
167.99.191.76	768
95.211.208.25	695
119.122.90.135	667
198.211.114.182	498
157.119.122.134	448
101.200.184.113	432
207.154.221.139	376

Top-15 Countries Sending COVID Spam

US	9984
CN	3252
CA	2277
DE	2070
--	1996
NL	1364
FR	1046
IN	1013
AR	965
ES	436

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	2

Top-15 Subjects Containing doc/xlsx Files

Important - Post-Coronavirus	11
Fight against the COVID-19 pandemic	4
Np: El coronavirus impulsa las rebajas online: un 73% de los españoles comprará a través de internet	4
GASOLINERO, PUEDE MINIMIZAR LOS EFECTOS POR EL COVID EN EL TALLER VIRTUAL "LA ERA DE LA COLABORACIÓN EN LAS ESTACIONES DE SERVICIO"	3
TEARFUND C.C.M.P PROVIDED BIBLE STUDY MATERIAL FOR COVID-19 PERIOD.	2
Press Release: FLIR Systems Launches FLIR Screen-EST Software to Improve Skin Temperature Screening for COVID-19 - Order #52231416	2
La 2éme vague du COVID-19 sera économique…	2
Informe Actualizado Semanal COVID-19 Relaciones Laborales 05/06/20 a 11/06/20	2
PR_Sessão clínica online: Insuficiência Cardíaca em tempos de Covid-19	2
Covid-19 Compensation Fund	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: 105,908
Domains with Potential Mail Servers: 2,691
Email-Capable Domains and Hosts: 40,851
Live Hosts and Domains Not Parked: 41,935

Mobile Apps

Apps in Official Stores: 289

by Store

Apple	166
Google	115
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 658

by Store Type:

Hybrid	401
Secondary	229
Affiliate	28

Blacklisted Mobile Apps: 20

by Store Type:

Secondary	19
Official	1