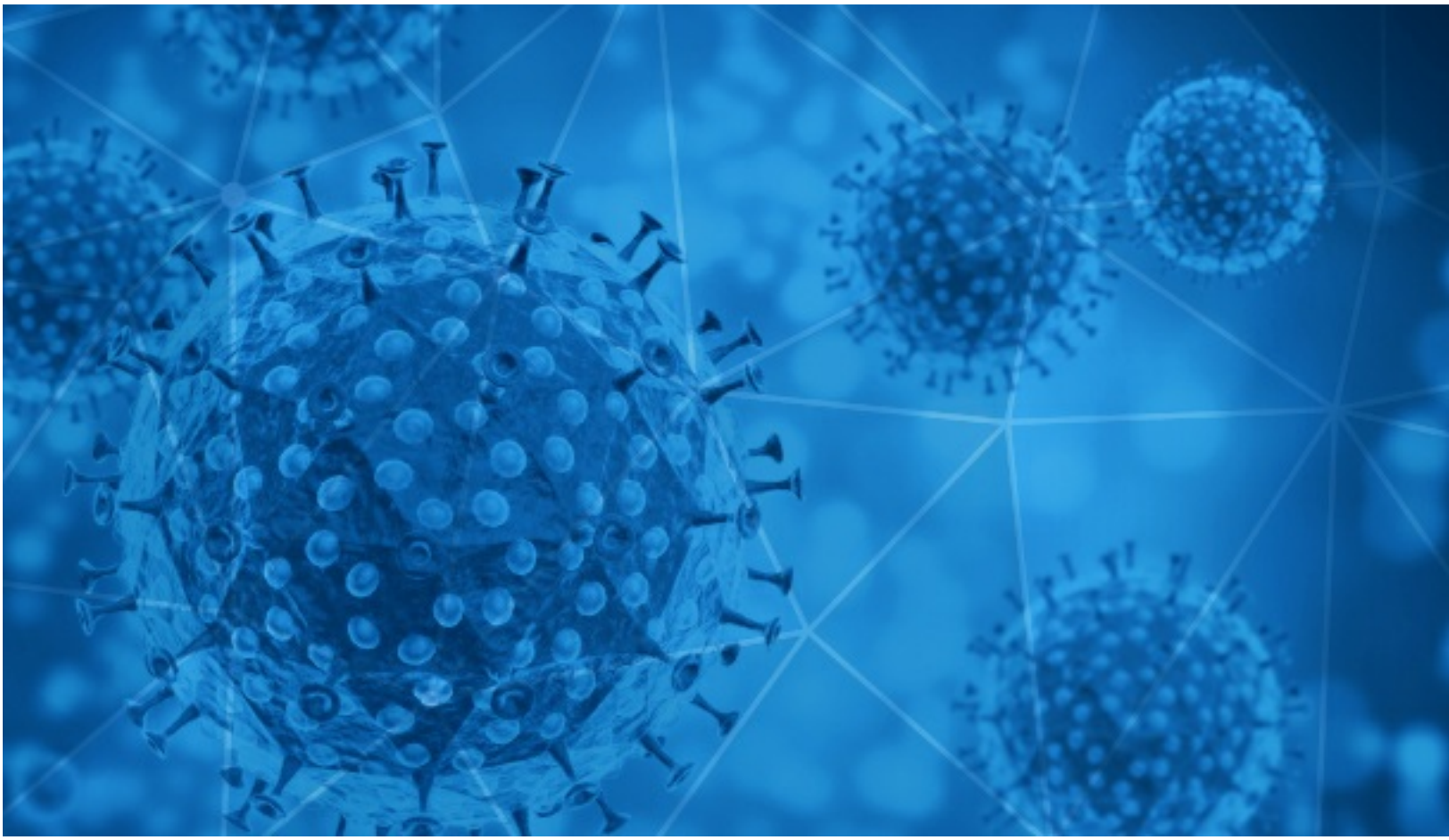
RISKIQ®

RiskIQ i3:

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

2020-07-23



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 2020-07-22 to 2020-07-23. During this period, RiskIQ analyzed 28,955 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,650 unique subject lines observed during the reporting period. The spam emails originated from 1,762 unique sending email domains and 3,272 unique SMTP IP Addresses. Analysts identified 11 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	6618
Re: COVID-19 Give away	2248
The Corona Letter: Tracking China's vaccine projects	1858
United Nations Covid-19 Palliative/Financial Support/Congratulations.	1399
PyMEs contra el COVID19	723
COVID-19 : Protectores Faciales	564
Covid Victims Compensation	429
Tamar Braxton Alert & Responsive +Over 1K coronavirus deaths in a day +Unlock your iPhone win no PIN	410
Como Afrontar una Fiscalización de Sunafil En Tiempos de Covid	368
COVID-19 - Website Design & Development / Mobile Application / SEO 100% Results Guaranteed [REDACTED_DOMAIN]	320
COVID-19 - Website Design & Development / Mobile Application / SEO 100%!R(MISSING)esults Guaranteed [REDACTED_DOMAIN]	313
PRODUCTOS DE PROTECCION COVID 19	306
Soluciones para la prevencion del covid19	266
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	262
Cabinas para la prevencion del coronavirus?	249
Como volver a la actividad post coronavirus?	248
Cities Admit COVID Spikes Due to Leftist Protests	245
You are more likely to contract Covid at home	243
Productos de Sanitizacion y prevencion Covid-19	239
MICROSOFT CORONAVIRUS RELIEF FUND (CRF) GLOBALGIVING	214
¡Vuelve a la normalidad! Combate el Covid-19 / Descuentos Imperdibles	203
Latest coronavirus (COVID-19) updates for Companies House customers	184
Grandes nomes confirmados para o I Congresso Digital Covid-19. Últimos dias para inscrição. O evento será gratuito, 100% on-line e com certificação!	182
Alertan nuevos sintomas: 15 minutos para saber si eres positivo o negativo de COVID-19	181
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	167

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	6618
gmail.com	3772
onet.eu	2248
timesofindia.com	1859
countermail.com	1486
trendingtopic.cl	922
163.com	766
126.com	642
caribbeanfever.com	410
acqla.com	368

Top-15 IPs Sending COVID Spam

103.141.137.241	2247
64.225.40.253	1376
190.247.254.96	619
157.119.122.136	514
153.122.116.244	429
190.247.226.222	399
190.247.227.154	357
223.74.106.137	356
157.119.122.39	351
167.99.239.38	305

Top-15 Countries Sending COVID Spam

JP	7256
US	7122
IN	3272
--	2380
AR	1852
CN	1706
FR	1431
GB	486
CA	434
DE	379

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

RE: Payment delayed due to situation COVID-19	10

Top-15 Subjects Containing doc/xlsx Files

COVID-19 RELIEF FUNDING	6
**LIST OF OVERDUE LOAN ACCOUNTS [COVID-19 RELAXATION A/C]	URGENT RECOVERY / RENEWAL REQUIRED**	3
Covid-19 compensation fund	3
NP_ Estación de 'Metro Lavamanos', la petición de KFC a Metro Madrid para cambiar el nombre de la estación de Lavapiés de forma temporal y luchar contra la Covid-19	2
****SMART User Notice - COVID-19 Medical Suspension Absence Recording****	2
Boletim Diário COVID-19 - 22/7/2020 - 10h00	2
PRUEBAS COVID- 19	1
COVID Update July 22	1
Planilha Surtos Covid 19 Atualizada	1
SBI DONATES THREE VENTILATORS TO JP HOSPITAL FOR TREATMENT OF COVID-19 PATIENTS	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: 115,666
Domains with Potential Mail Servers: 2,834
Email-Capable Domains and Hosts: 43,736
Live Hosts and Domains Not Parked: 65,390

Mobile Apps

Apps in Official Stores: 354

by Store

Apple	190
Google	155
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 909

by Store Type:

Hybrid	582
Secondary	289
Affiliate	38

Blacklisted Mobile Apps: 22

by Store Type:

Secondary	19
Official	2
Hybrid	1