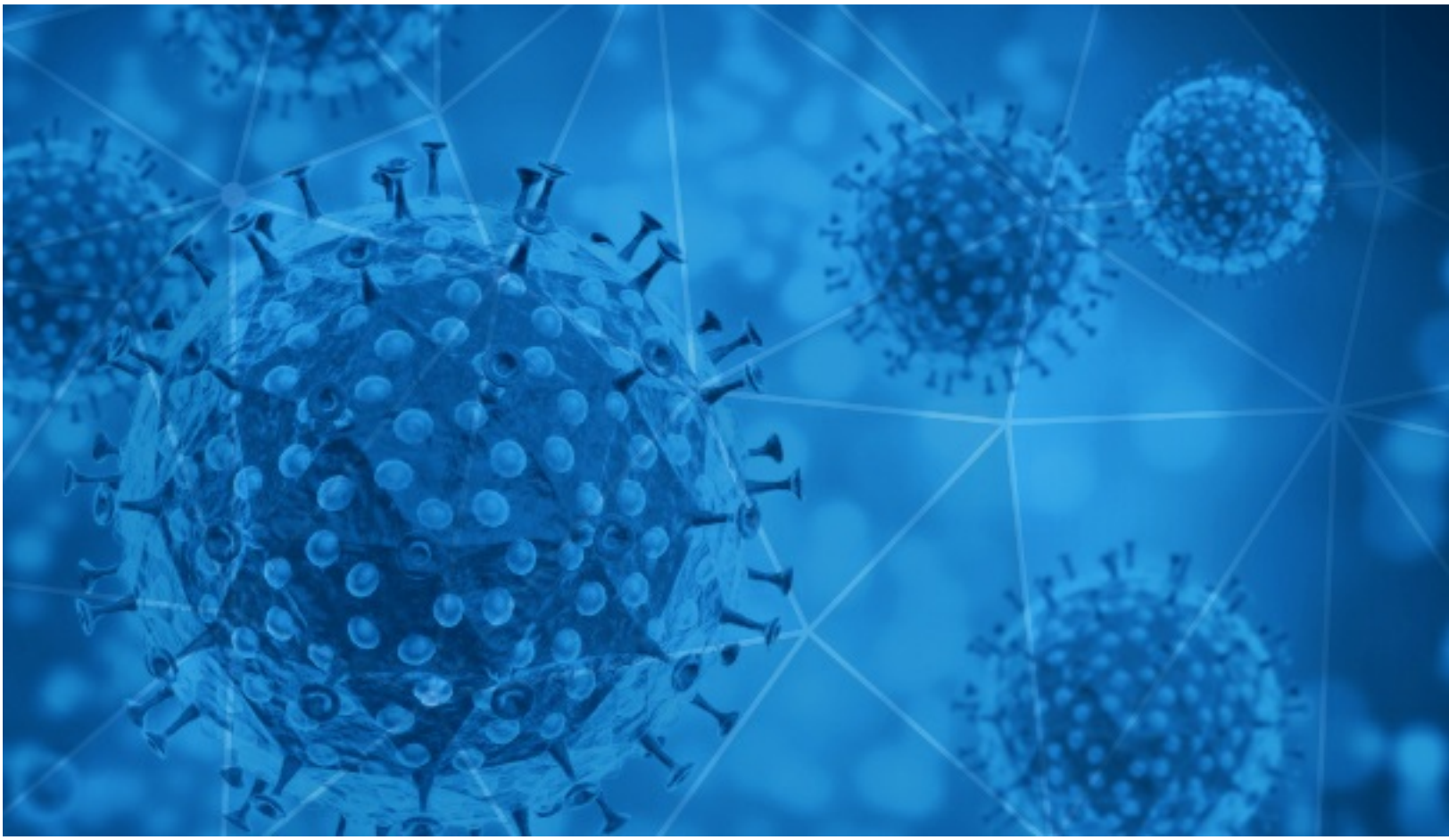
RiskIQ i3:

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

2020-07-24



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 2020-07-23 to 2020-07-24. During this period, RiskIQ analyzed 27,499 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,451 unique subject lines observed during the reporting period. The spam emails originated from 2,024 unique sending email domains and 3,804 unique SMTP IP Addresses. Analysts identified 3 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: The cloud over reinfection	2540
RE: COVID-19 Give away	2218
Re: COVID-19 Give away	1226
PyMEs contra el COVID19	1152
ATTIVATO credito d'imposta sugli acquisti DPI COVID	857
United Nations Covid-19 Palliative/Financial Support/Congratulations.	467
18..VITAL INFORMATION ABOUT COVID 19	386
Cabinas para la prevencion del coronavirus?	370
Soluciones para la prevencion del covid19	357
Test Covid - Entrega inmediata	325
COVID-19 - Website Design / Mobile Application / SEO 100%!R(MISSING)esults Guaranteed - [REDACTED_DOMAIN]	305
Como volver a la actividad post coronavirus?	304
Oferta !!! Protector Facial Covid-19	289
COVID-19 - Website Design / Mobile Application / SEO 100% Results Guaranteed - [REDACTED_DOMAIN]	285
Where the Covid-19 billions are hidden	266
United Nations Covid-19 Palliative/Financial Support/Congratulations.	262
Productos de Sanitizacion y prevencion Covid-19	260
COVID-19 - Website Design / Mobile Application / SEO 100%!R(MISSING)esults Guaranteed - [REDACTED_DOMAIN]	244
NUEVOS Productos Graficos Prevención COVID	229
Fwd:Credito Covid-19 Aprobado.	225
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	224
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	214
COVID-19 Chinese protective products	205
Contagem regressiva | Evento gratuito e certificado | Congresso Digital COVID-19 - Repercussões Jurídicas e Sociais da pandemia.	203
COVID-19 - Website Design / Mobile Application / SEO 100% Results Guaranteed - [REDACTED_DOMAIN]	202

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

onet.eu	3444
timesofindia.com	2542
gmail.com	2541
countermail.com	2183
126.com	1123
163.com	1096
sicurezzanews.it	857
citromail.hu	642
oab.com.br	400
comunidadempresarial.cl	371

Top-15 IPs Sending COVID Spam

103.141.137.241	3444
190.247.242.33	1461
223.74.106.137	583
69.90.78.162	461
82.135.19.130	459
200.252.130.219	399
82.135.19.131	398
177.75.112.18	386
142.93.6.221	370
119.139.137.219	367

Top-15 Countries Sending COVID Spam

US	6185
IN	3967
--	3751
CN	2491
AR	2480
DE	1386
CA	1199
BR	989
FR	612
ZA	502

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	3

Top-15 Subjects Containing doc/xlsx Files

PPE items against Covid-19	6
SME Companies Tax Planning, Incentives & Benefits Post Covid-19 I 29-30 July 2020	3
Follow - Up: July's COVID-19 Informational Call & Unity in Community	3
COVID-19 - Human Rights Violation on Religious Minority Group	3
Transporte sostenible toma fuerza en Colombia en tiempo de covid-19	2
COTIZACION KIT DE PCR EN TIEMPO REAL PARA NUEVO CORONAVIRUS (COVID-19)	2
IMSS Boletín 499.- Investigadores del IMSS participan en 3 de las 4 propuestas enviadas al CEPI para el desarrollo de una vacuna contra el COVID-19 (LINK DE VIDEO Y FOTOS)	2
IIT Kharagpur Media Invite: Web Launch of 'Novel Technology for COVID-19 Rapid Test' on Saturday, 25th July 2020	2
Buscan el 61% de las empresas mejorar su plan de beneficios a raíz del Covid-19	2
RV: “PLAN PARA LA VIGILANCIA, PREVENCION Y CONTROL DE COVID-19 EN EL TRABAJO” MUNICIPALIDAD DISTRITAL DE JOSE LEONARDO ORTIZ	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: 115,990
Domains with Potential Mail Servers: 2,840
Email-Capable Domains and Hosts: 43,831
Live Hosts and Domains Not Parked: 65,518

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