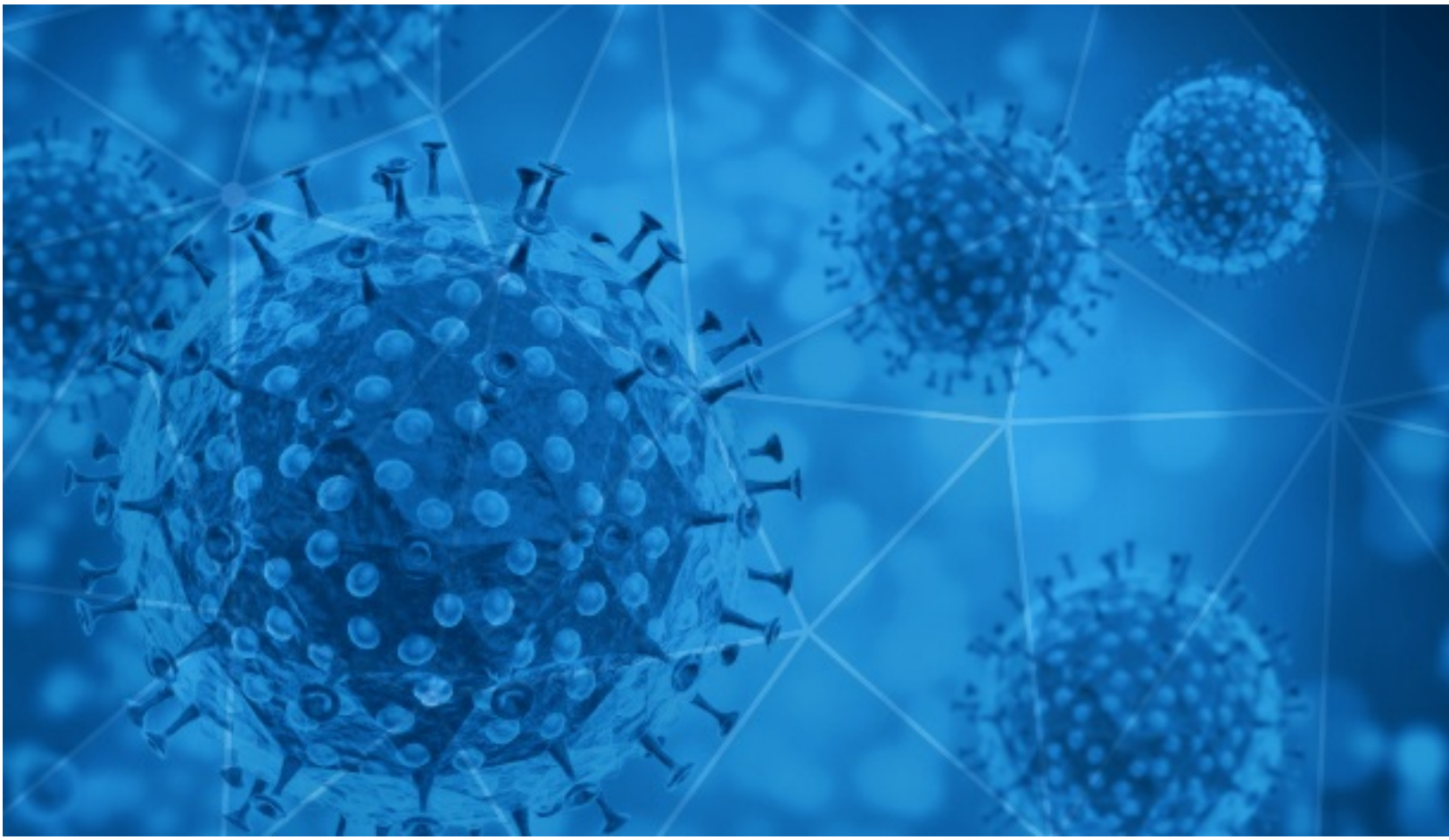
RiskIQ i3:

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

2020-06-25



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 2020-06-24 to 2020-06-25. During this period, RiskIQ analyzed 67,638 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,994 unique subject lines observed during the reporting period. The spam emails originated from 2,940 unique sending email domains and 5,933 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	23435
The Corona Letter: Pandemic has hit the children hard	3320
Redeem COVID-19 Financial Relief Funds Today	2003
Minimice el Riesgo de contagio del Coronavirus - Validacion Biometrica	1900
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	1256
Sistema de detección Térmico Contra Covid-19	945
URGENT ORDER (COVID 19 RUSH HOUR.)	904
Empresas responden, empiezan a hacer pruebas de COVID-19 a empleados	856
Implacable contra el COVID-19 AMONIOX	750
Re:Zuberi Finance SA Droogte / Covid-19-verligtingprojek	708
COVID-19 / DONATION FOR YOU	647
Donations Ref # LJR/020-113377/EUS- You have been Chosen for our COVID-19 Donation	589
Beneficios y Alternativas Legales para Empresas en tiempos de Covid-19	583
Ofertas COVID-19	552
Protección contra el COVID-19 - Te ofrecemos el mejor precio del mercado - ENTREGA INMEDIATA	543
The United Nations/covid-19 palliative rehabilitation scheme	534
Covid Holistic	490
Mamparas de proteccion COVID19	444
Mamparas de proteccion contra el coronavirus	431
Credito fiscal COVID para innovacion	425
Cabinas para la prevencion del coronavirus?	416
Evita el Covid19 en tu lugar de trabajo	413
Soluciones para la prevencion del covid19	411
Test Rapido Covid-19 Mascarillas e Insumos	403
Como volver a la actividad post coronavirus?	368

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	23441
gmail.com	3883
timesofindia.com	3320
countermail.com	3268
126.com	2038
fnb.co.za	2004
sopytecchile.com	1901
163.com	1465
seekscanenchile.com	945
inok-tm.com	904

Top-15 IPs Sending COVID Spam

80.66.193.60	2003
167.99.191.76	1900
159.65.80.166	945
103.207.38.18	904
46.23.1.40	758
159.89.80.159	749
201.231.19.221	708
103.225.54.213	706
119.122.88.25	664
212.227.254.175	647

Top-15 Countries Sending COVID Spam

JP	23722
US	13399
IN	5076
CN	3995
AR	3451
CA	2721
--	2373
GB	2085
DE	1861
VN	1198

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

CORONA VÃRUS PRODUZIDO EM LABORARIO- VEJA A MATERIA	4
CILTSA Covid-19 Information videos for the workplace	4
PEOPLE'S WATCH ANDHRA PRADESH Oklahoma War On Covid-19 and $2Tn US Healthcare Savings	3
Inteligencia Artificial: combinación de algoritmos que salva vidas frente a la pandemia de Covid-19	2
Fwd: tamponi covid	2
Sale!!! New Covid Safety Kits with custom imprint option as low as $3.28 per kit - 3-5 day lead time for non-logod- from GreatSunrise06172020.docx	2
Coronavirus (COVID-19) Information Update Resident Communication: 'Green Phase'- Wednesday, June 24, 8:00 AM	2
IMSS Boletín 422.- A nivel nacional, más de 10 mil 500 personas no derechohabientes reciben atención médica en clínicas y hospitales del IMSS por COVID-19 (LINK DE VIDEO)	2
IMSS VERSIÓN ESTENOGRÁFICA Y AUDIOS. Intervenciones del Jefe de la División de Proyectos Especiales del IMSS, Dr. Felipe Cruz Vega, durante sesión de preguntas y respuestas conferencia informe diario de COVID-19, Palacio Nacional	2
POST COVID-19 SPECIAL B2B RATES	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: 108,950
Domains with Potential Mail Servers: 2,747
Email-Capable Domains and Hosts: 41,712
Live Hosts and Domains Not Parked: 46,899

Mobile Apps

Apps in Official Stores: 301

by Store

Apple	170
Google	123
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 751

by Store Type:

Hybrid	460
Secondary	257
Affiliate	34

Blacklisted Mobile Apps: 20

by Store Type:

Secondary	19
Official	1