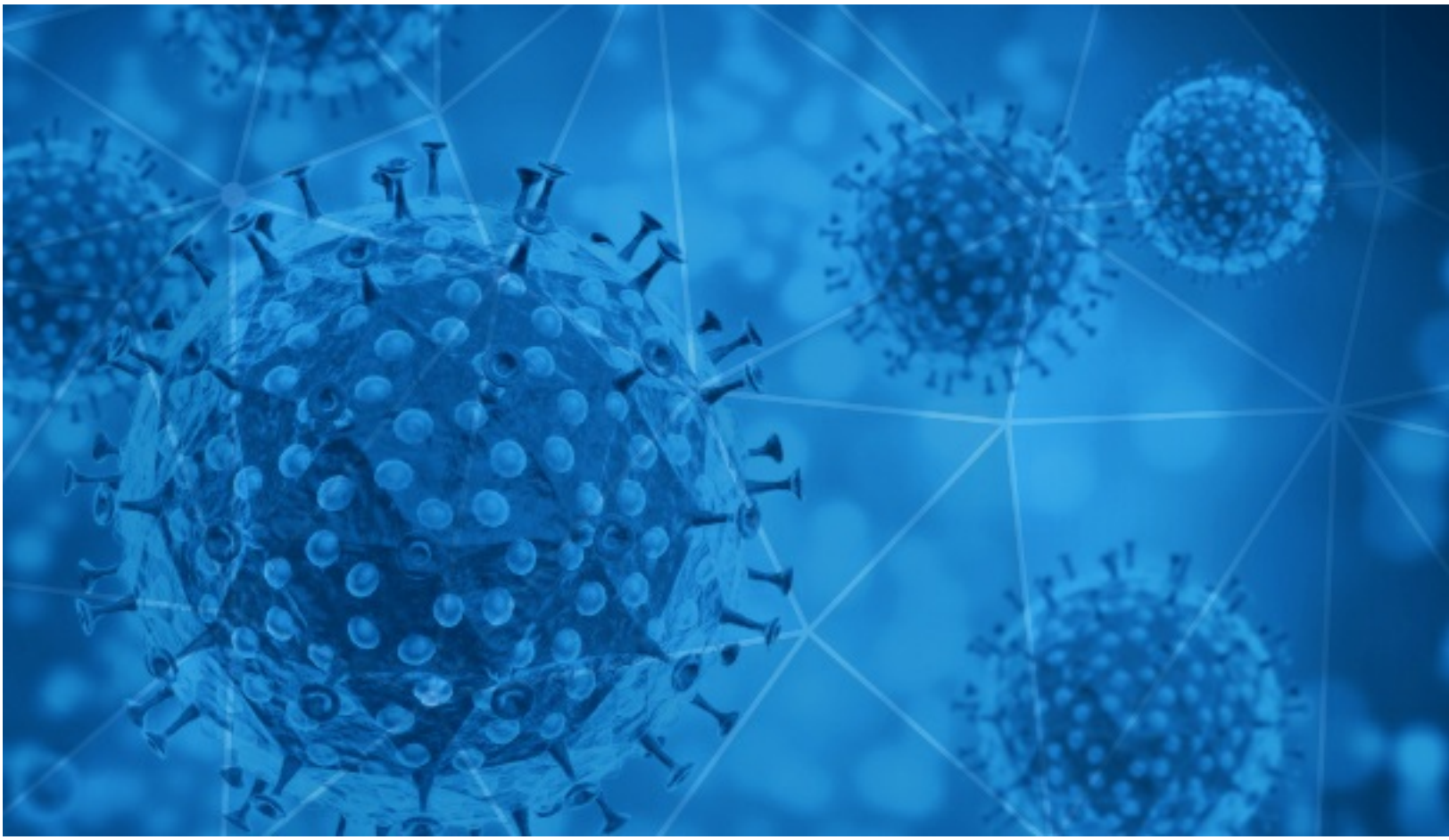
RiskIQ i3:

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

2020-11-02



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 2020-11-01 to 2020-11-02. During this period, RiskIQ analyzed 49,502 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,925 unique subject lines observed during the reporting period. The spam emails originated from 1,109 unique sending email domains and 2,979 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□	22737
The Corona Letter: How long does immunity last?	5145
Gestión de riesgos y auditoría en tiempos de covid19	2066
Coronavirus (Covid19) Bailout Fund	1449
Safety measures to stay protected against COVID-19	1138
Re: Personal, SME & Business Relief (COVID-19).	1071
Agevolazione Flyingmailers per l'Emergenza COVID-19 | Fai sapere che ci sei!	853
Proteja su negocio de COVID19 y ofrezca seguridad a sus clientes	673
Test rapido para la deteccion del Coronavirus	672
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	436
ATALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID -19	422
Triple test para COVID19 de deteccion rapida	375
Ingresaron TEST COVID19 de deteccion rapida	347
Precio test covid19	338
Test rapidos de covid19 aprobados por ANMAT	329
COVID 19 : Continuer de vous être utile	328
COVID-19 PANDEMIC RELIEF FUND	284
Re: Covid-19 acrylic protect shield	276
COVID-19 Asesoramiento contable para tu empresa	247
Just Confirm your Covid Antibody appointment at Rs 750 only and get relaxed.	239
ATENCION COVID-19 Estudio Contable, Legal e Impositivo para tu negocio	234
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	232
Corona - private/betriebliche Veränderung?	231
La Nueva Forma De Trabajar En Tiempos De Coronavirus Rentabilizando Tu Voz	227
Evite el coronavirus en su negocio	216

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

epc-store.com	22742
timesofindia.com	5146
walla.co.il	3432
focazen.com	2073
gmail.com	1665
bknegaraindonesia.com	1449
icicliprulife.com	1138
126.com	1091
cmbmutualfunds.com	1071
flyingmailers.com	853

Top-15 IPs Sending COVID Spam

201.231.19.208	1891
190.247.240.56	1540
45.5.200.6	1449
85.17.15.45	853
103.225.54.218	731
103.225.54.157	646
103.225.55.231	572
103.225.52.16	523
103.225.52.245	510
103.225.54.219	507

Top-15 Countries Sending COVID Spam

JP	22840
IN	6598
US	4741
AR	3973
CN	2737
BR	1485
PH	1070
NL	968
DE	927
FR	812

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

ANC Weekly COVID-19 Reports	29
ASSÍNCRONA - VÍDEO MEDB92 – História da Medicina Tema: A História do Cuidado nas vítimas das epidemias: Isolamento, Quarentena, Rede de Apoio, relacionando com a covid-19.	2
Covid: Colletti (M5s), ritardi su pianificazione, serve commissione d'inchiesta	2
Tanzschule Ayda : Elternbrief zu Corona Pause	2
Fwd: COVID-19 - October 31, 2020	1
WG: Corona-Pandemie und Mannlich-Gymnasium	1
AISLAMIENTO DE PERSONAL POLICIAL POR COVID-19	1
SANITA' E TRASPORTI: ANCHE NEL MOLISE IL COVID METTE A NUDO IL DISASTRO DEL GOVERNO FASCIO- LEGHISTA REGIONALE E DEL GOVERNO CENTRALE I LOCKDOWN CAUSATI DAL DISATRO DI SANITA' E TRASPORTI, LI PAGHINO I PADRONI, NON I LAVORATORI, I DISOCCUPATI, LE PARTITE	1
RV: CUESTIONARIO COVID-19	1
RE: With COVID-19 Infection on a rise get the Training to Help Combat the rise now Free.	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: 131,273
Domains with Potential Mail Servers: 2,689
Email-Capable Domains and Hosts: 49,801
Live Hosts and Domains Not Parked: 46,207

Mobile Apps

Apps in Official Stores: 467

by Store

Apple	235
Google	217
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,676

by Store Type:

Hybrid	881
Secondary	736
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1