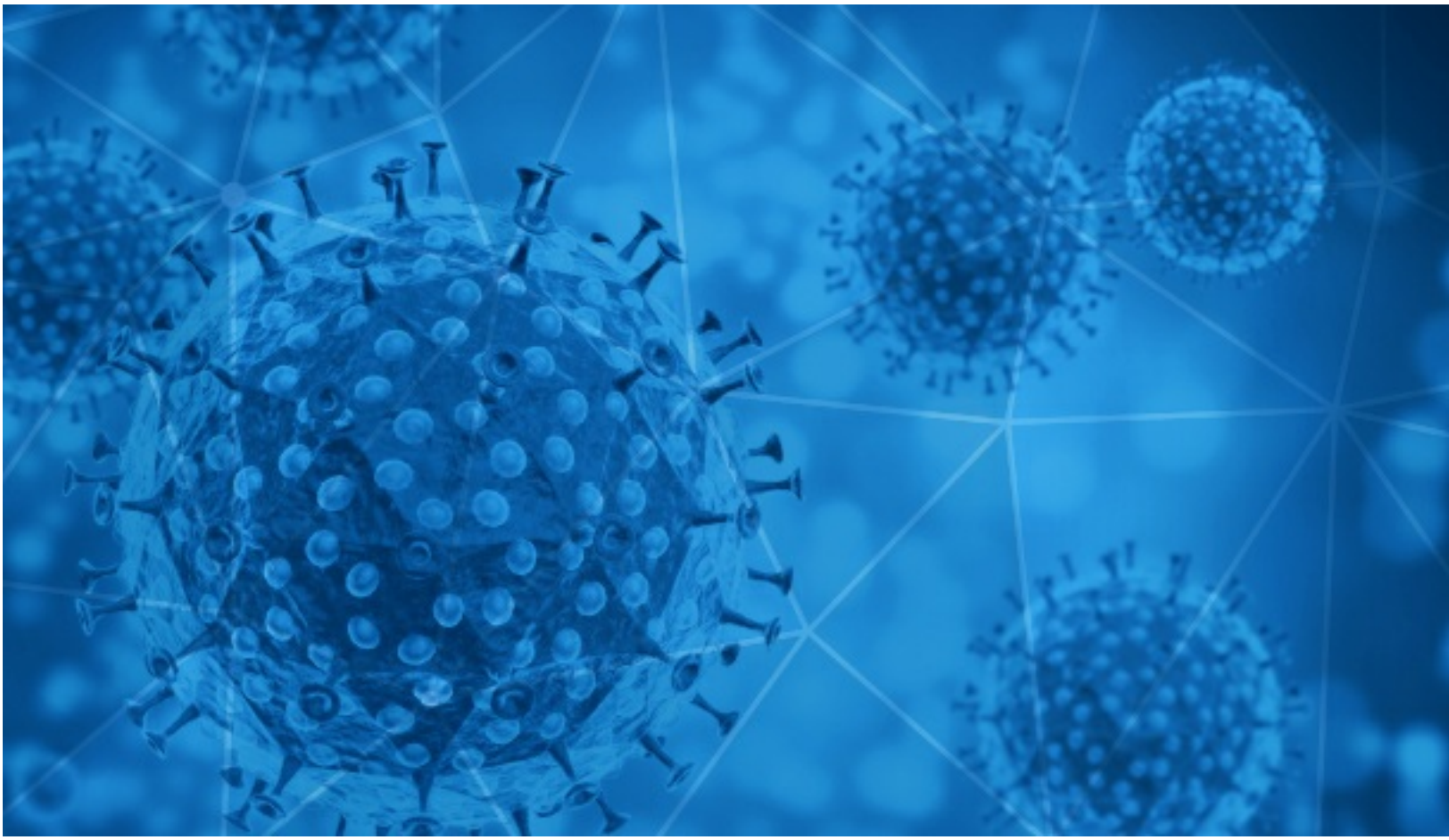
RiskIQ i3:

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

2021-03-30



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 2021-03-29 to 2021-03-30. During this period, RiskIQ analyzed 3,708 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 766 unique subject lines observed during the reporting period. The spam emails originated from 496 unique sending email domains and 761 unique SMTP IP Addresses. Analysts identified 2 emails which sent an executable file for Windows machines.

Top-25 Subjects

Recuperacion Efectiva de los Subsidios Laborales ante Essalud Post Covid19	740
- Covid Relief Donation -	216
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	181
COVID-19 Update: We are open and now offering Free Virtual Consultations	171
Aktuelle BfArM-Zulassung: Ausreichend lieferbar Coronatestsets	107
YOUR COVID-19 STIMULUS PACKAGE WORTH..	102
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO ANTE EL COVID19	95
Seguro COVID19 para la construccion	95
Re: Covid vaccine is approved for you.	91
Separadores Sanitarios Contingencia COVID / Todo Tipo de Trabajos en Aluminio y Cristal	87
Minister Says His COVID-19 Disappered in 3 Days	81
Refuerza la UNAM laboratorios para evaluacion preclinica de vacunas contra la Covid-19	68
Coronavirus briefing: Novavax vaccine deal	66
Additional Coronavirus Information and Resources	56
Do you Think that the Coronavirus Pandemic Will be Over in 2021?	43
Recuperacion Efectiva de los Subsidios Laborales ante Essalud Post Covid19 -8 y 9 de Abril	35
Canada issuing new guidelines for use of AstraZeneca's COVID-19 vaccine	31
3/29/2021 COVID-19 General Order Re: In-Court Appearances	31
Arma tu kit para tus colaboradores y clientes contra el Covid	30
COVID-19 Grant!	27
Your COVID-19 Test Results	27
COVID-19 Vaccine Appointment	24
Indiana Department of Health invites any Indiana resident age 30 and older to receive the COVID-19 vaccine!	21
Covid19 Relief Fund	19
[SUSPECTED SPAM] COVID-19 Relief Fund	18

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

euroavisos.com	740
gmail.com	485
aiusm.com	217
veq90.xyz	174
ccwtooday.info	155
gmx.net	107
walla.co.il	95
gajtek.com	91
exalumno.pve.unam.mx	68
email3.telegraph.co.uk	66

Top-15 IPs Sending COVID Spam

212.200.239.162	216
91.228.101.43	173
91.228.101.213	155
157.245.42.150	144
142.93.129.38	107
96.86.106.193	102
181.46.136.168	95
67.219.150.138	91
68.183.93.29	77
167.71.188.112	67

Top-15 Countries Sending COVID Spam

US	1878
DE	374
RS	239
CA	234
AR	213
NL	115
FR	102
MX	71
CN	65
--	42

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

FW: Coronavirus: Deuxième prolongation IP Covid-19 | Tweede verlenging SO Covid-19	1
Mandatory Covid-19 vaccination/Form is attached.	1

Top-15 Subjects Containing doc/xlsx Files

CCS 11800 Cambio temporal en Ruta Circunvalación 2 por aplicación de vacuna anti COVID-19	2
Covid Extension notification	2
CORONAVIRUS	1
Paterson Middle Covid-19 Update	1
Cotação urgente covid - Mirante do Paranapanema	1
censo de covid-19 del personal de la Region Sanitaria	1
PLANILLA ACTUAL 2021 DE COVID A SER UTILIZADO	1
COVID Exposure	1
REPORTE DE PERSONAL CON SISTOMAS O SOSPECHAS DE COVID-19 29 DE MARZO DEL 2021 EN CERVECERIA.	1
Envio covid maximiliano	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: 154,050
Domains with Potential Mail Servers: 2,554
Email-Capable Domains and Hosts: 51,305
Live Hosts and Domains Not Parked: 43,486

Mobile Apps

Apps in Official Stores: 519

by Store

Apple	257
Google	245
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,259

by Store Type:

Hybrid	1157
Secondary	1036
Affiliate	66

Blacklisted Mobile Apps: 30

by Store Type:

Secondary	27
Official	2
Hybrid	1