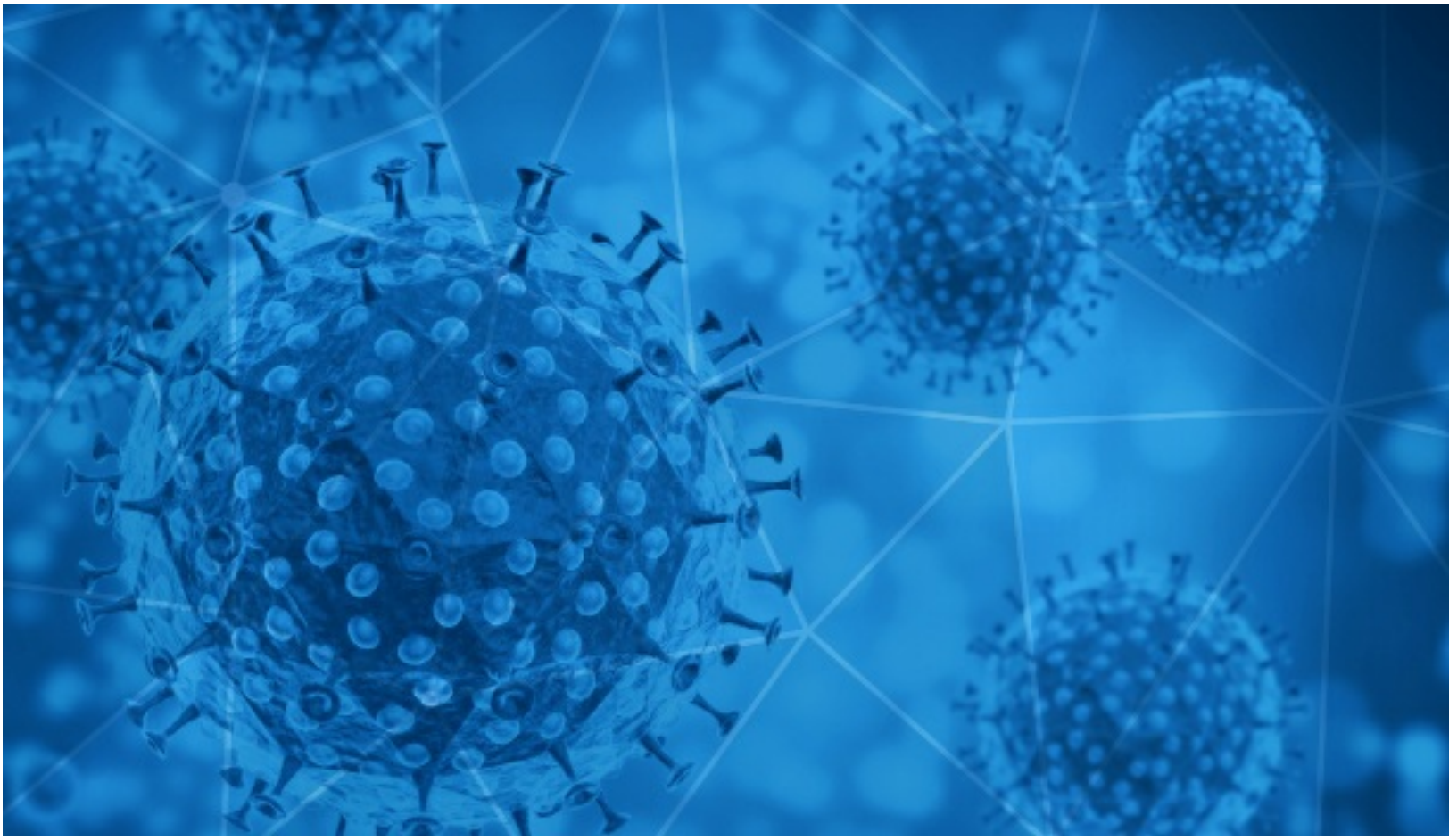
RiskIQ i3:

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

2021-02-17



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 2021-02-16 to 2021-02-17. During this period, RiskIQ analyzed 35,472 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,905 unique subject lines observed during the reporting period. The spam emails originated from 2,072 unique sending email domains and 4,184 unique SMTP IP Addresses. Analysts identified 10 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	12935
The Corona Letter: More virus mutations discovered	3571
Covid19 Relief Fund	1491
LJC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation	971
Better than COVID Vaccine…	725
Últimas medidas Laborales en el entorno Covid 2021□	516
Re: Corona virus Protection Pills.Order confirmation	474
Test zur Erkennung von COVID-19 Antigen und Antikörper zum besten Preis an	420
Lineamientos de salud por Covid-19	396
Mi seguro insumos covid 19 protege a tu familia	374
Últimas medidas Laborales en el entorno Covid	349
Gran Venta Outlet - Productos Covid 19	335
TermoScanner e strumenti DPI Anti-Covid in pronta consegna con sconti oltre il 70% e prezzi a partire da Euro 39,00 + spedizione gratuita. Non Abbassiamo la guardia!!!	300
UN Covid-19 Winning Notificationw	263
Pruebas Rápidas de Alta Precisión para COVID-19	209
Influweb contro il coronavirus	184
COVID LOANS FROM UNITED NATIONS	161
Test Rápido Covid-19 Segunda Generación	153
Re: covid-19 touch monitor	150
Vax diplomacy: 37% doses exported are grants | Post Covid, patients see rise in fungal infection | Covid stress caused more damage to mind than heart	122
Important Information About Your COVID-19 Vaccine Pre-Registration (también en español)	117
Holen Sie sich noch heute Ihren COVID-19 Palliative Support	114
Prueba rápida de Covid-19 en el Movistar Arena ¡Resultado en 1 hora!	112
COVID TASTE RESULT	101
PMI.it - Pensioni, punti deboli del sistema italiano e prospettive post Covid	97

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

giant-pw.com	12938
timesofindia.com	3582
gmail.com	2867
eremitmms.com	971
lifesmils.guru	725
vdocument.net	516
compratest.es	424
gajtek.com	416
expertosenaprendizaje.com	396
public.govdelivery.com	394

Top-15 IPs Sending COVID Spam

59.12.54.10	1483
103.131.245.194	971
195.62.46.11	725
198.20.248.178	475
67.219.150.138	474
103.225.55.233	382
143.110.158.154	373
103.225.54.28	366
103.225.53.179	333
103.225.54.161	318

Top-15 Countries Sending COVID Spam

JP	13204
US	8071
IN	3787
--	1836
KR	1596
IT	962
FR	810
CN	692
DE	554
CA	529

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Pfizer-BioNTech Covid-19 Vaccines update	9

Top-15 Subjects Containing doc/xlsx Files

Planowanie i rozliczanie czasu pracy w 2021 roku oraz w dobie covid-19.	8
Planowanie i rozliczanie czasu pracy w 2021 roku oraz w dobie covid-19	4
PR - Torrestir realiza testes quinzenais de rastreio à COVID-19 aos seus 2.600 funcionários	4
Vandalizzata per la seconda volta la corona ai martiri delle foibe	3
UN Covid 19 Relief fund.	3
Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	3
NP-Hospital Loayza puso en funcionamiento nuevos ambientes de emergencia para pacientes COVID-19	2
IMSS FOTO NOTA.- En tres unidades médicas del IMSS se aplica la vacuna contra COVID-19 a población adulta mayor en la Ciudad de México	2
IMSS FOTO NOTA.- Con séptimo embarque de vacunas contra COVID-19 de Pfizer se cubrirá inmunización a personal de salud: IMSS	2
CCS 11391 Reporte COVID-19: confirman 26 contagios y 5 fallecimientos más	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: 143,997
Domains with Potential Mail Servers: 2,577
Email-Capable Domains and Hosts: 52,332
Live Hosts and Domains Not Parked: 44,316

Mobile Apps

Apps in Official Stores: 514

by Store

Apple	255
Google	242
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,096

by Store Type:

Hybrid	1069
Secondary	960
Affiliate	67

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	26
Official	2
Hybrid	1