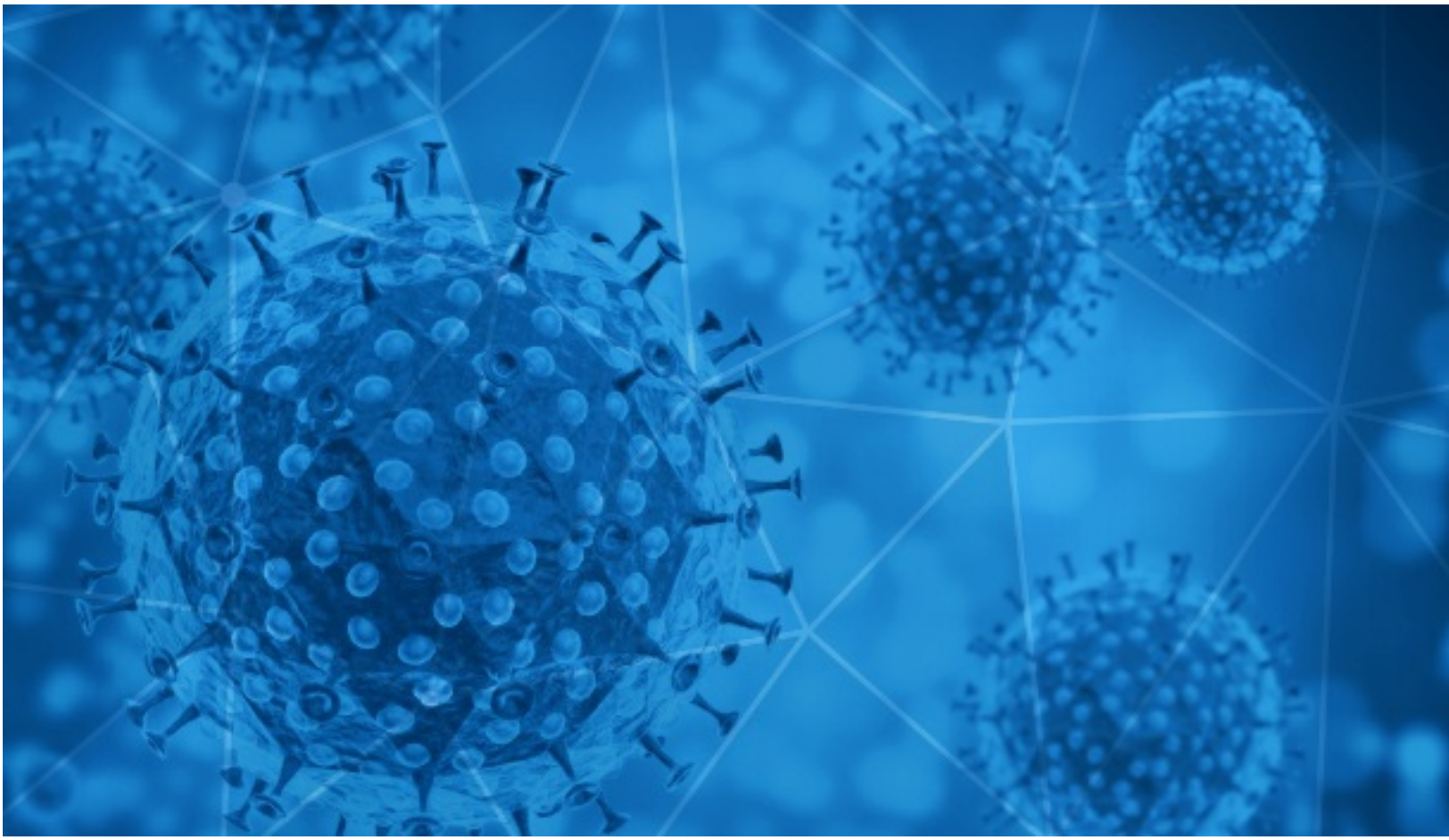
RiskIQ i3:

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

2020-10-08



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 2020-10-07 to 2020-10-08. During this period, RiskIQ analyzed 47,054 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,254 unique subject lines observed during the reporting period. The spam emails originated from 2,191 unique sending email domains and 4,829 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	17730
The Corona Letter: The virus may be infecting our dreams	4109
Fundo de socorro da OMS Covid 19	1012
Limpieza y desinfeccion COVID 19	804
AuraAir: Único Filtro que Elimina el Covid-19 llegó a Chile	792
Test de deteccion rapida COVID19	606
Test rapido para la deteccion del Coronavirus	602
COVID-19 KILLED ANTHONY	571
Covid-19 Rapid Test Kits	524
Protection from Coronavirus and other diseases	420
How to Sell Effectively (Post Covid-19)	412
Covid-19 Cash Support für Sie	365
Last Call! Don't forget to do Covid Antibody IgG + IgM test at Rs 750 only | Appointments are available.	350
0ferta test rápidos COVID 19	342
Test Rápido Covid-19 Segunda Generación - 10.000 Un Entrega Inmediata	336
$500.000,00 USD Covid -19 Financial Relief Funds!	332
OECD Responses to (COVID-19) Fund	291
Incontri online in Italia (no corona)	289
Coronavirus JobKeeper Payments Scheme	258
Mamparas de proteccion COVID19	256
Mamparas de proteccion contra el coronavirus	253
The digital twin that's been helping Vedanta steer out of the crisis | How Indian IT is leveraging analytics to respond to Covid-19	225
Join the Bowser Administration for a Community Leader Telephone Townhall on Coronavirus	221
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	216
Covid 19 Splash/Benefit Promotions	213

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	17732
timesofindia.com	4111
gmail.com	2575
tutanota.com	2521
126.com	786
yeah.net	769
auraairchile.cl	716
tiscali.co.uk	666
sinosa.co.za	524
claimintl.com	492

Top-15 IPs Sending COVID Spam

181.239.232.86	1144
194.113.89.65	1012
103.225.54.16	651
103.225.54.217	547
103.225.53.124	541
103.225.54.207	523
217.69.162.183	492
103.225.55.118	491
3.7.230.6	482
103.225.55.84	476

Top-15 Countries Sending COVID Spam

JP	18135
US	7809
IN	4932
CN	2805
AR	2686
DE	1564
CA	1300
--	1234
GB	988
FR	761

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

PHHS 10 07 2020 End of Day COVID 19 Summary	7
PHHS 10 06 2020 Daily COVID 19 Incident Summary	7
Immunity Certification : Rapid Antibody Test Kits for Covid19	4
WEBINAR COVID-19 SPA Pubbliche, P.A. e PPP: partenariato pubblico-privato e per l'innovazione 14/10/20	3
Fisioterapeutas da UFPR estudam como ventilação mecânica pode auxiliar no tratamento de Covid-19	3
NP-Minsa envía más de 83 toneladas de suministros médicos a regiones para reforzar la lucha contra la Covid-19	2
covid 19 Payments	2
I: Survey GITMO Covid 19 - Proposta	2
Công văn 97 Về việc triển khai công điện hỏa tốc phòng chống dịch Covid-19	2
2.8% DEI NATI DA MADRE POSITIVA HA CONTRATTO IL COVID-19: I PRIMI DATI DEL REGISTRO SIN AL XXVI CONGRESSO NAZIONALE	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: 128,193
Domains with Potential Mail Servers: 2,812
Email-Capable Domains and Hosts: 48,532
Live Hosts and Domains Not Parked: 72,240

Mobile Apps

Apps in Official Stores: 444

by Store

Apple	225
Google	204
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,540

by Store Type:

Hybrid	841
Secondary	643
Affiliate	56

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1