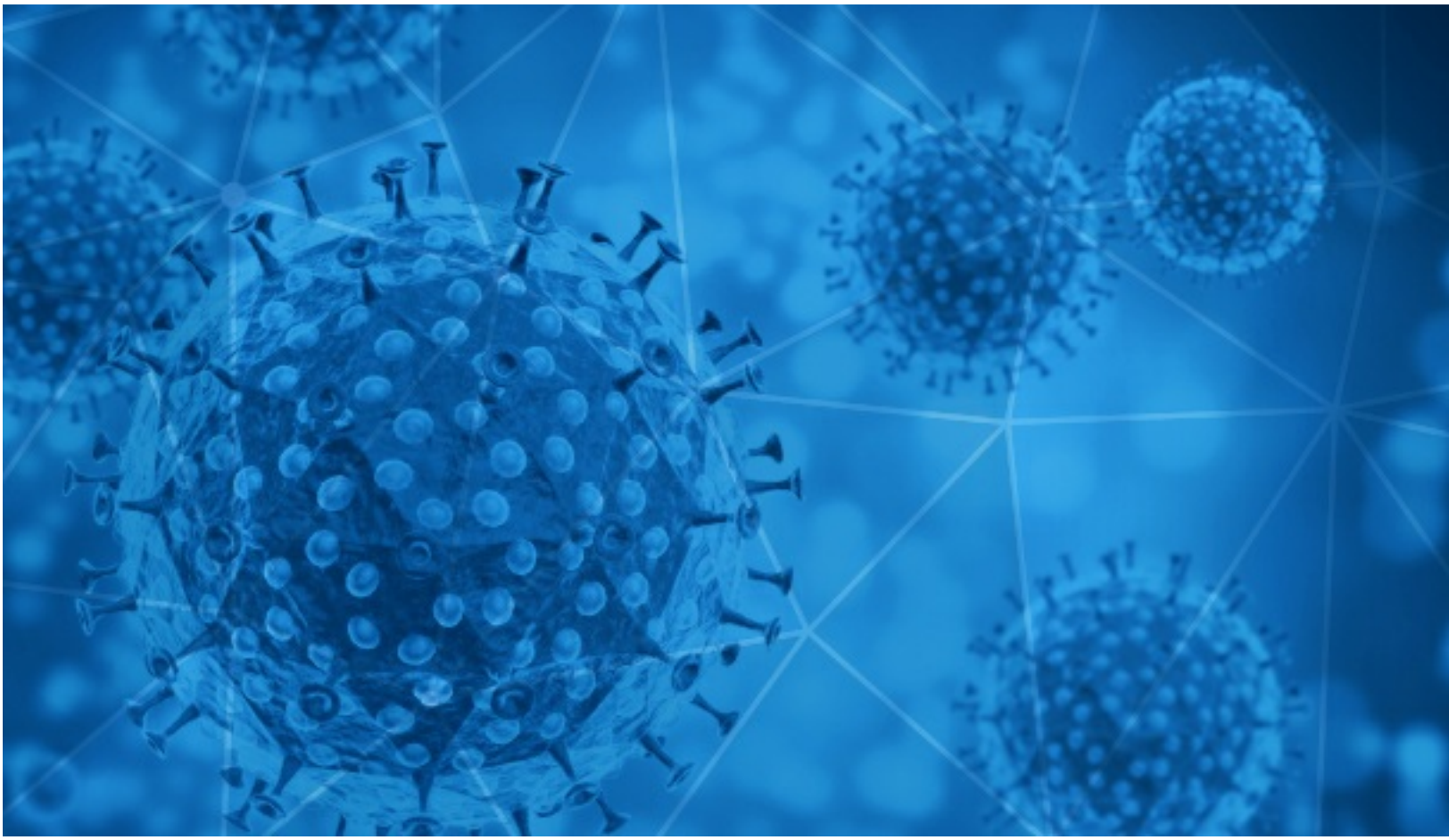
RISKIQ®

RiskIQ i3:

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

2020-10-09



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 2020-10-08 to 2020-10-09. During this period, RiskIQ analyzed 51,028 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,685 unique subject lines observed during the reporting period. The spam emails originated from 2,101 unique sending email domains and 4,659 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	14537
Key moments from the VP debate, 8 unanswered questions about Trump's COVID-19 case, and more from Apple News	4807
The Corona Letter: Can heaters spread the virus?	4007
Check out "Bruse Wane Live Ep 22:Trump, Eminem and Lord Jamar, Nicki Minaj, Tekashi 69 overdose ?, Is Trump's covid diagnosis real ? LL Cool J Disses Kanye West" on Wane Enterprises	1987
Corona virus (Covid19) Bailout Fund	1785
Covid 19 Splash/Benefit Promotions	1297
$500.000,00 USD Covid -19 Financial Relief Funds!	1230
Covid-19 Rapid Test Kits	917
Fundo de socorro da OMS Covid 19	683
Female founders lose ground amid COVID-19	592
Test de deteccion rapida COVID19	513
Test rapido para la deteccion del Coronavirus	483
International (OECD) Responses #COVID-19 Fund	474
La mascarillas FFP2 y KN95, la mejor arma contra el COVID y los más de 10.000 contagios diarios, ¿tienes las tuyas?	364
PROTEZIONE concreta da COVID19 in azienda	341
Mamparas de proteccion contra el coronavirus	314
Mamparas de proteccion COVID19	288
International (OECD) Responses to #COVID-19 Fund	273
La Nueva Forma De Trabajar En Tiempos De Coronavirus Rentabilizando Tu Voz	263
International (OECD) Responses #COVID-19 Fund	263
Protection from Coronavirus and other diseases	256
Protégete RESPONSABLEMENTE Contra el Covid -19 / Los Mejores Precios	215
Test y Tarifa Productos Covid 19 Entrega 24 horas	212
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	201
zwalcz covid - sterylizator powietrza	189

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	14540
insideapple.apple.com	4933
timesofindia.com	4010
gmail.com	2665
waneenterprises.com	1987
tutanota.com	1728
bknegaraindonesia.com	1521
contactyouragentemail.com	1297
claimintl.com	1260
sinosa.co.za	917

Top-15 IPs Sending COVID Spam

168.227.76.6	1785
181.239.232.86	1727
164.163.76.10	1297
3.7.230.6	1170
212.108.220.115	1142
194.113.89.65	683
192.169.7.136	659
67.192.51.27	590
103.225.53.246	507
103.225.55.37	434

Top-15 Countries Sending COVID Spam

US	15757
JP	14838
IN	4259
BR	3140
CN	2077
AR	1786
DE	1445
HU	1177
FR	941
--	933

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

covid 19 Payments	8
WEBINAR COVID-19 Green economy e fonti rinnovabili: decreti attuativi, modelli, ecobonus, cessione del credito 22/10/20	8
WEBINAR COVID-19 Anticorruzione e Trasparenza P.A e partecipate pubbliche: PNA 2019-2021, novità legislative 26/11/20	6
INZ sačinio dodatno COVID-19 Uputstvo za škole, fakultete i vrtiće	5
Invitation to Attend: Employee Engagement in the Time of COVID	4
Hold the Date - Palisades Institute: The Shifting Business Landscape of the Lower Hudson Valley Region due to COVID-19	3
"PLANEAMIENTO TRIBUTARIO EN TIEMPOS DE COVID-19" ¿Como generar ahorros tributarios y liquidez para su empresa?	2
[KYTF:] Ryle Oct 10 Covid forms	2
NP_Beko lanza HygieneShield, la primera gama de electrodomésticos del mercado que elimina más del 99% de las bacterias y virus (incluyendo el coronavirus)	2
[Università di Verona] com.st. L'Europa unisce le forze per combattere il Covid-19	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: 128,507
Domains with Potential Mail Servers: 2,801
Email-Capable Domains and Hosts: 48,564
Live Hosts and Domains Not Parked: 72,523

Mobile Apps

Apps in Official Stores: 446

by Store

Apple	225
Google	206
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,549

by Store Type:

Hybrid	842
Secondary	651
Affiliate	56

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1