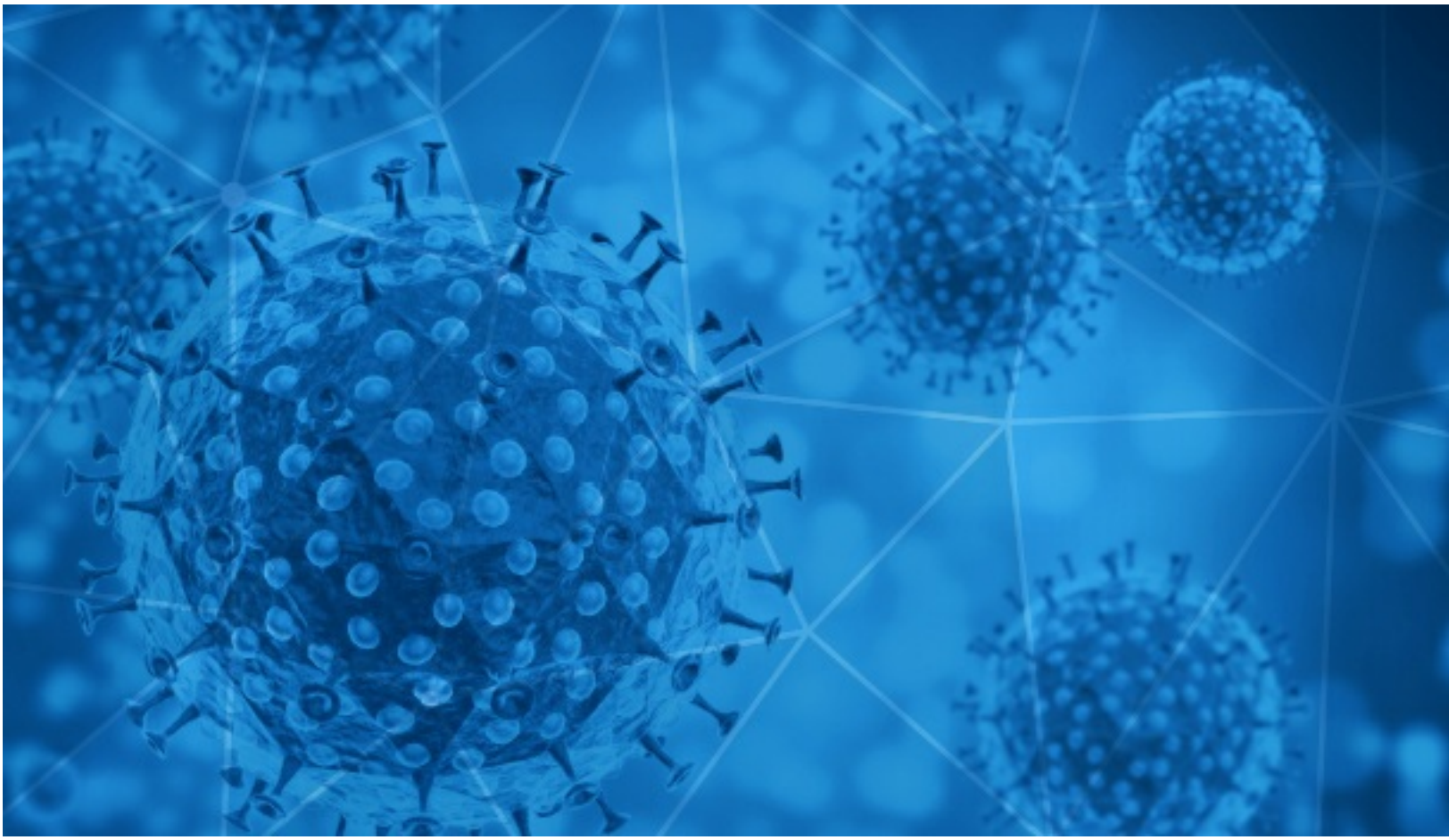
RiskIQ i3:

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

2020-12-22



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 2020-12-21 to 2020-12-22. During this period, RiskIQ analyzed 48,295 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,055 unique subject lines observed during the reporting period. The spam emails originated from 1,979 unique sending email domains and 4,434 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	16331
Neue Corona Variante ausser Kontrolle.	4494
The Corona Letter: Should we be worried about the new virus variant?	3682
Covid-19 Relief Details	1915
Wack 100 Fights 2 White Men, leaves one Bloody {VIDEO} New mutant Covid strain coming out of the UK	1897
Oportunidad de Cumplimiento de Ley de SST y Plan COVID-19	1440
Dieses Covid-Spezialpaket wird geliefert	1249
Ingresaron TEST COVID19 de deteccion rapida	884
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	759
Beanspruchen Sie Ihr Operation Covid-Paket	526
COVID-19 and the impact on car and auto auctions	526
Covid-19 Donation	513
Let’s fight together to get through the COVID-19	377
Wearing a KN95 mask is your best defense against coronavirus	353
COVID-19 vaccine research studies	314
Offering N95 FACE MASK (3M 1860,1860S, Makrite 9500 N95,N95S,HARLEY, SAMPLING SWAB AND TUBE KITS,Novel Coronavirus (COVID-19) Test ,quick delivery in a couple days	297
Re: Your Order corona vaccine Free	216
!You have won covid-19 palliative award fund €950.000,00 Euro!	208
Respuestas gerenciales para el post Covid19	207
Matchmaking in the time of Covid-19	201
Soy Camila Cid, representante de la marca de alcohol gel Como Te Odio Corona.	201
Stay Protected From COVID19 With KN95 Official Certified Masks	192
Promoción Insumos Covid-19 Especial Para Empresas	186
Essential steps CIOs and CMOs must take together to break silos for e-commerce | 72% of cyberattacks related to COVID-19 coming via fake emails	170
Good Morning, SA | Zikalala has warns on COvid-19 clusters, Gordhan vindicated, News24 coronavirus documentary	158

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	16333
outlook.de	4496
timesofindia.com	3689
xcontrol.it	1970
caribbeanfever.com	1901
aol.com	1788
focazen.com	1440
gmail.com	1061
grupolylsalud.com	884
ecaptcdhorijumaontfourth.com	707

Top-15 IPs Sending COVID Spam

155.254.28.56	1821
51.79.142.8	1504
82.62.149.230	1339
181.239.232.123	861
195.22.157.128	777
103.225.53.252	734
45.141.58.55	730
178.62.255.238	596
5.180.79.138	537
103.225.55.141	536

Top-15 Countries Sending COVID Spam

JP	16490
US	12614
IN	4158
--	3211
FR	2004
IT	1859
NL	1398
AR	1171
CN	1106
GB	713

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

Allarme esperti per pazienti cronici derma e reuma: seguite le raccomandazioni che abbiamo messo a punto per affrontare il Covid 19	4
Salud y el gobierno de Tierra del Fuego trabajaron en la plan operativo de vacunación COVID-19	3
NMDA Coronavirus Briefing - 21.12.2020	2
CONFIRMACION CITA COVID-VEHICULAR	2
Buletin de presa 21.12.2020 + comunicat actiuni COVID19	2
Preses relīze "Apstiprina pirmo vakcīnu pret Covid-19 lietošanai Eiropas Savienībā"	2
Corona: IHK Pfalz gibt neue Hinweise: Erweiterte FAQs zu Novemberhilfen und Dezemberhilfen erschienen ---- Anträge auf Dezemberhilfe voraussichtlich ab Anfang Januar 2021 möglich	2
Curso covid19	1
FW: Covid 19 school update - provisional arrangements	1
RE: Congress Announces Deal on COVID Relief and Spending Bill	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: 137,132
Domains with Potential Mail Servers: 2,623
Email-Capable Domains and Hosts: 52,230
Live Hosts and Domains Not Parked: 47,390

Mobile Apps

Apps in Official Stores: 493

by Store

Apple	245
Google	233
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,926

by Store Type:

Hybrid	986
Secondary	881
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1