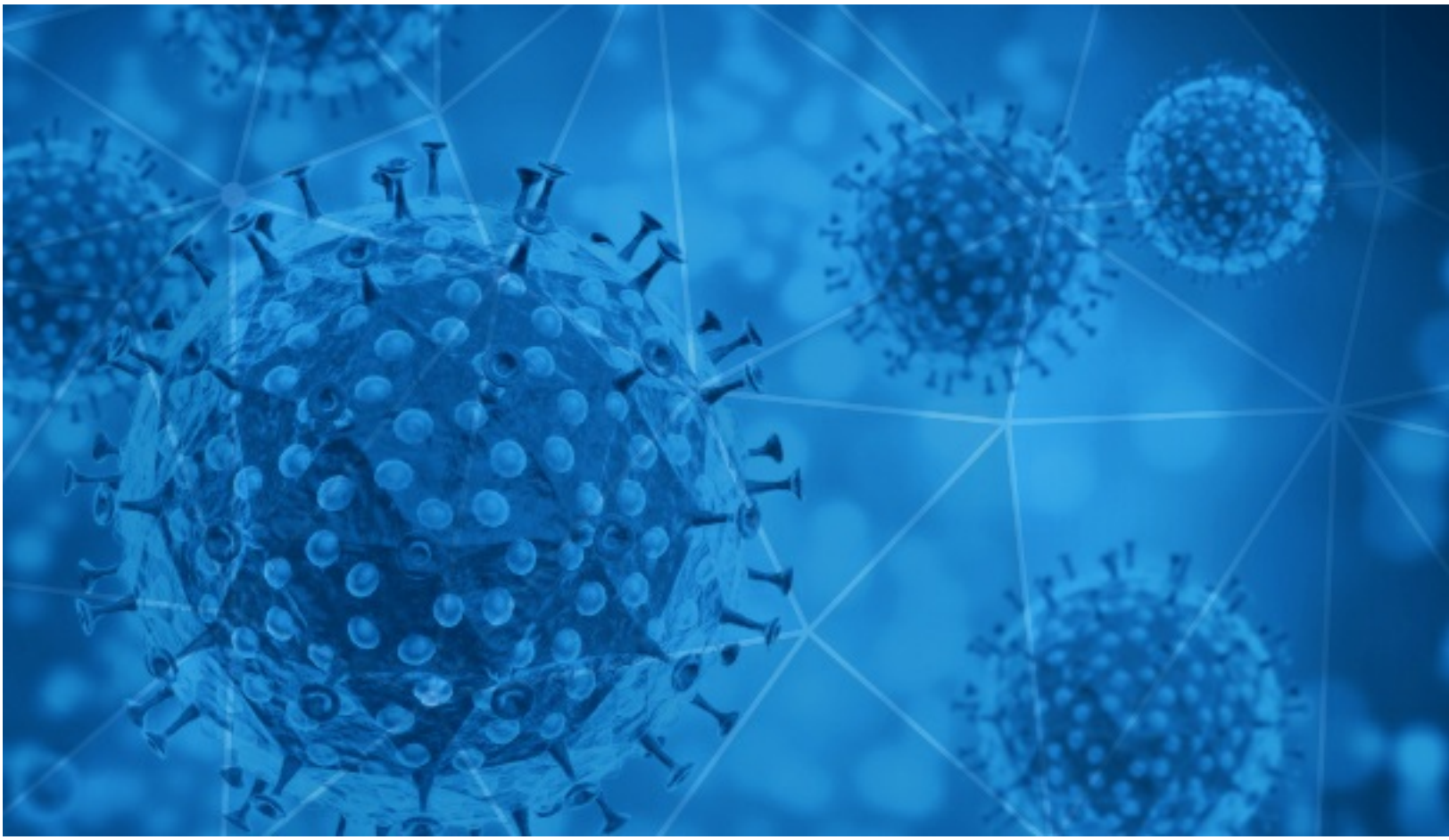
RiskIQ i3:

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

2020-12-21



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 2020-12-20 to 2020-12-21. During this period, RiskIQ analyzed 37,409 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,643 unique subject lines observed during the reporting period. The spam emails originated from 1,038 unique sending email domains and 2,328 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	19504
The Corona Letter: Had Covid? Vaccines are good for you too	4613
Tamar Braxton Explains Suicide Attempt{VIDEO}Chaos aboard United flight as passenger with COVID dies	1291
COVID FUNDS	1191
Herzliche Glückwünsche!!! Sie haben die Helping Hand Covid-19 Compensation gewonnen	572
Ingresaron TEST COVID19 de deteccion rapida	534
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	517
COVID Cases Still Rise, Stock Up ON KN95 Masks While Supplies Last	466
Respuestas gerenciales para el post Covid19	457
Oportunidad de Cumplimiento de Ley de SST y Plan COVID-19	388
Let’s fight together to get through the COVID-19	263
New "Faster Spreading" Strain of Corona Virus Found	245
Covid-19 Update	230
Politie valt binnen op familiefeest - Hoe gevaarlijk is gemuteerd coronavirus? - Waarom je nu moet investeren in goud	226
Chase Update / Covid-19 Important Notice	206
Help the world's response to Covid-19 with the most protective mask on the market.	204
Wearing a KN95 mask is your best defense against coronavirus	199
!You have won covid-19 palliative award fund €950.000,00 Euro!	183
Re: covid-19 touch monitor	174
Covid-19 Donation	168
COVID 19 RELIEF GRANT	161
Re:covid-19 touch monitor	145
Re: Digital signage solution for Covid-19	135
Mutatie coronavirus opgedoken in ons land - Alle coronacijfers gaan verkeerde kant uit - "Mijn kaalheid schrikt mannen af, maar ik wilde kindje"	132
PACK DESINFECCIÓN COVID-19 CON DESPACHO GRATIS	98

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	19506
timesofindia.com	4614
gmail.com	1965
caribbeanfever.com	1291
hhwwo.org	572
grupolylsalud.com	534
consons.com.cn	517
greigerseptic.com	466
walla.co.il	457
126.com	454

Top-15 IPs Sending COVID Spam

103.99.1.130	1191
103.225.52.3	568
164.163.56.11	550
181.239.232.123	533
103.225.52.183	486
103.225.53.80	468
194.146.36.163	466
190.247.223.105	457
103.225.55.144	422
103.225.53.195	420

Top-15 Countries Sending COVID Spam

JP	19555
US	5680
IN	4625
AR	1597
VN	1202
CN	1050
BE	583
--	523
GB	390
NL	343

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

ANC Weekly COVID-19 Reports	33
TEUTEUGA O POLOAIGA O LE COVID19- Aso 20 Tesema 2020	8
Your Covid- 19 relief payments	4
Cs N. 321 - Covid-19: Speranza, "Servono decisioni uniformi a livello Eu"	3
NV COVID-19 UPDATE 12/20	2
Covid-19 Outbreak at Tudor Lodge	1
Vollzug IfSG/Covid-19 (CVD)	1
NdP SNI: Industria del turismo y gastronomía requiere de medidas urgentes que le permitan reactivarse post COVID-19	1
FW: Informatie van de GGD Hollands Noorden voor de positief geteste Covid-19 patiënt / Registratienummer: 140337	1
CS N. 320 - Covid-19: Speranza, "Firmata ordinanza per blocco voli da Gb"	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: 137,020
Domains with Potential Mail Servers: 2,624
Email-Capable Domains and Hosts: 52,180
Live Hosts and Domains Not Parked: 47,073

Mobile Apps

Apps in Official Stores: 492

by Store

Apple	245
Google	232
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,924

by Store Type:

Hybrid	985
Secondary	880
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1