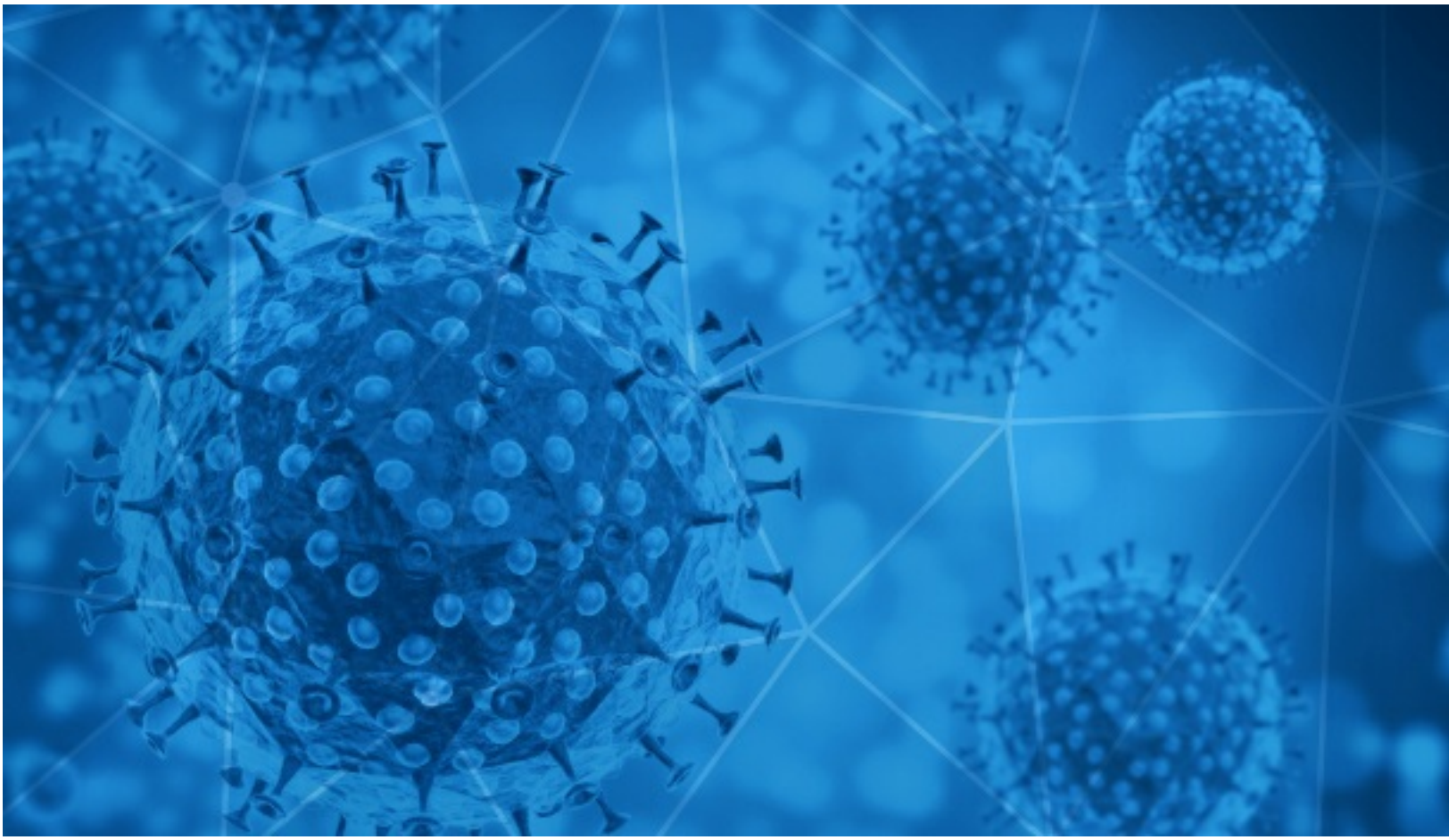
RiskIQ i3:

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

2020-12-07



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 2020-12-06 to 2020-12-07. During this period, RiskIQ analyzed 41,088 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,463 unique subject lines observed during the reporting period. The spam emails originated from 925 unique sending email domains and 3,514 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	19402
The Corona Letter: How the world is rolling out the vaccine	4644
This Has Killed Thousands More People Than Coronavirus 2020	3787
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	1963
Global Pandemic Relief Fund 3 Million Pounds In 2020 Coca Cola Covid-19 Pandemic Relief Award	1743
United Nations 2020 Covid-19 Compensation Payment.	803
Coronavirus COVID-19 and the impact on car and auto auctions	335
Testy kasetkowe na COVID19 - chroń siebie lub firmę - 99% skutecznoci	320
COVID-19 COMPENSATION FUNDS :	319
United Nations 2020 Covid-19 Compensation Payment.	304
Coronaregels nu versoepelen 'compleet onverantwoord’ - Antwerpse politie legt negen lockdownfeestjes stil: 64 personen betrapt - Jongeren filmen hoe leerkracht en leerlinge in de clinch gaan in de klas - Familiedrama in Oost-Vlaanderen: jongeman (26)…	280
Re: Digital signage solution for Covid-19	245
Hızlı Tanı Kiti-Covid 19 CRT	237
Re: COVID-19 - Projects | Website | Mobile Application | E-Commerce | SEO (Results Guaranteed) [REDACTED_DOMAIN]	228
UNITED NATIONS CORONAVIRUS RELIEF FUND (UNCRF)	221
Re: covid-19 touch monitor	213
CRT Covid 19 Hızlı Tanı Kiti	184
Let’s fight together to get through the COVID-19	180
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	170
COVID-19 Update: We are open and now offering Free Virtual Consultations	166
India Means Business : Despite COVID-19, Foreign Direct Investment Doubles in Q2	156
covid-19 pandemic relief fund-(06/12/2020)	134
RE: COVID-19 STIMULUS PACKAGE WORTH $1,500,000.00 USD	123
Got a minute? Tell us your opinion on COVID-19 vaccine.	118
Attn: Claim your COVID-19 Relief Funds	113

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	19407
timesofindia.com	4649
liqrut.cam	3787
hotmail.com	1878
gmail.com	1012
outlook.com	900
ourvaluedcustomer2pjdrewardsrready.com	564
drewardurvalsrreadyourvalue1dcustomerpj.com	472
126.com	458
drewardurvalsrreadyourvalue2dcustomerpj.com	458

Top-15 IPs Sending COVID Spam

193.223.106.166	3787
192.3.136.7	1743
150.95.82.182	1106
103.225.53.219	651
103.225.53.226	623
103.225.55.113	609
103.225.54.69	606
103.225.55.41	455
103.225.53.96	414
103.225.55.189	374

Top-15 Countries Sending COVID Spam

JP	19827
US	5730
IN	4909
--	4434
SG	1251
CN	937
BE	443
GB	418
BR	371
PL	345

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	30
CCS/10782 Rebasa Chihuahua los 40 mil casos confirmados de COVID-19	2
NdP_TrasplantesyCovid-19.docx	2
REPORTE LLAMADAS COVID-19 RED HUANUCO 05/12/20	1
Elternbriefe zu den Corona bedingten Anpassungen für die ZP	1
REPORTE DIARIO DE INSUMOS COVID	1
brq covid 06-12-2020	1
Delim „Radno vreme za vreme Covid 19“ sa vama	1
Fwd: Prueba de antígeno para Covid 19 - Miércoles 09 Diciembre	1
RE: REPORTE COVID-19 RAICA 06.12.2020 (CORTTE: 07.00 HORAS)	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: 134,975
Domains with Potential Mail Servers: 2,611
Email-Capable Domains and Hosts: 51,497
Live Hosts and Domains Not Parked: 45,112

Mobile Apps

Apps in Official Stores: 478

by Store

Apple	240
Google	223
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,864

by Store Type:

Hybrid	967
Secondary	838
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1