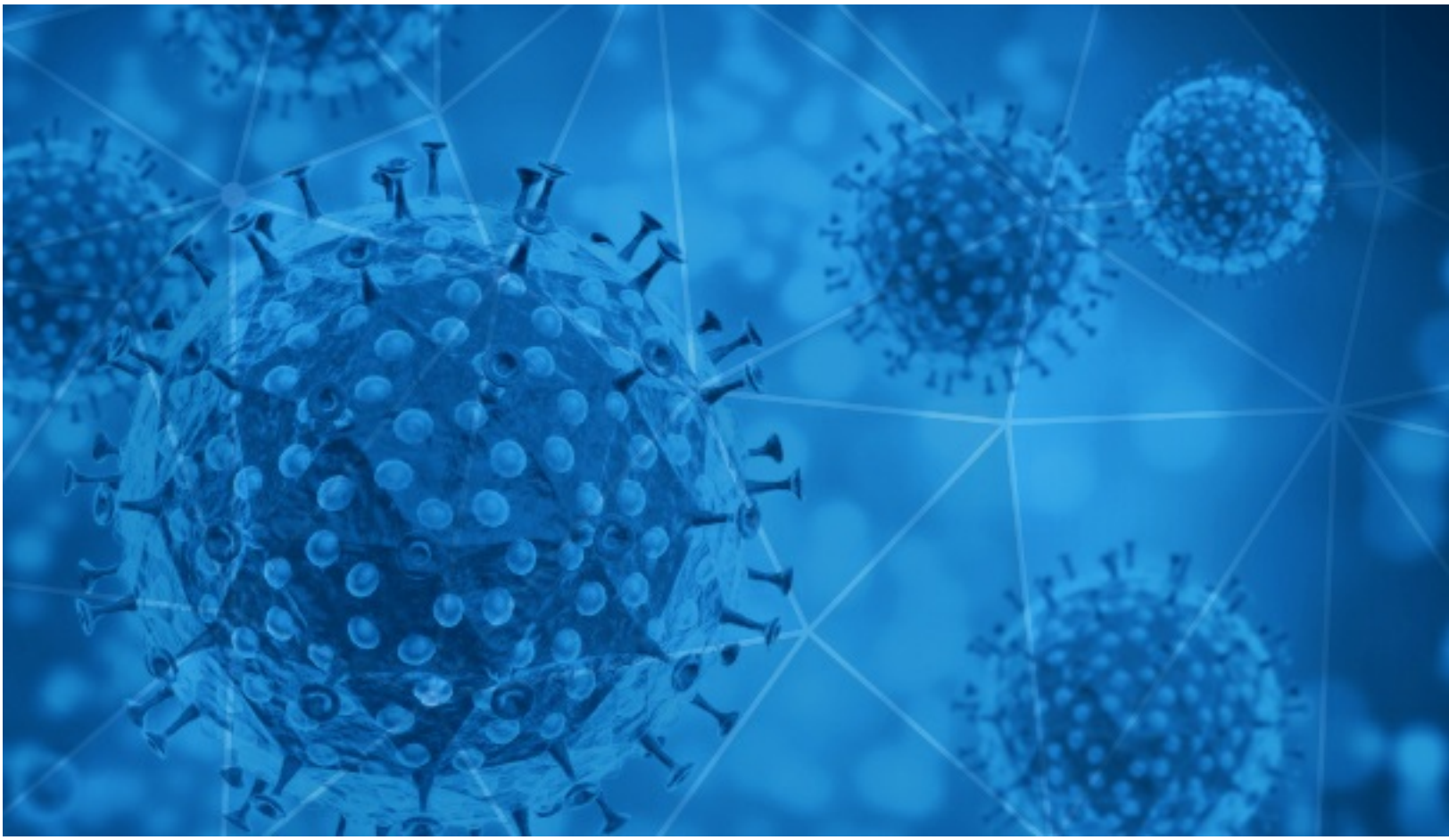
RiskIQ i3:

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

2020-11-26



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 2020-11-25 to 2020-11-26. During this period, RiskIQ analyzed 40,196 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,630 unique subject lines observed during the reporting period. The spam emails originated from 2,275 unique sending email domains and 4,599 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	10499
COVID-19 RELIEF PAYMENT!!!	5972
The Corona Letter: A mutation that made the virus more contagious	2365
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	827
Covid19_Relief (HMRC) - You are eligible for a grant.	592
Contactless infrared body temperature thermometer defeat Coronavirus	559
Re: Defeat Coronavirus, non contact fever alarm device	557
4 must have insurance policies during COVID-19	410
Re: Corona virus Protection Pills.Order confirmation	354
Protégez-vous du Covid avec SOLUGERM France	346
Precios IMPACTO / Productos COVID 19	337
Happy Thanksgiving! Caregiver Support Expansion, Soldiers' Angels Holiday program, COVID-19 Clinical Trials	335
SBA COVID Relief Payroll Protection Program	311
Re: COVID-19 RESPONSE FUND	307
covid-19 vaccines	303
Mi seguro insumos covid 19 protege a tu familia	300
Safety measures to stay protected against COVID-19	295
- $850,000.00 USD COVID-19 GRANT :	291
Fight COVID-19□ With $100 Gift Card!	281
Goossens: ‘Sneltests in ziekenhuizen, testcentra, bij huisarts en op school’ - Waarom Trump zich niet langer tegen de machtsoverdracht verzet - Meghan Markle maakt bekend dat ze miskraam had - De langgerekte lijdensweg van de corona-adviesorganen -...	247
Avoid COVID with this "touchless" infrared thermometer	241
Re: Digital signage solution for Covid-19	241
COVID-19	240
ANTI-COVID "Touchless" Thermometer. Laser tech let's you take their temp from a distance!	227
United Nations 2020 Covid-19 Compensation Payment.	223

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	10501
hearts-foundations.com	5976
timesofindia.com	2365
keyable.net	1116
gmail.com	1095
163.com	652
securesuite.uk	592
energyinspectorsbenefits.com	468
126.com	396
outlook.com	393

Top-15 IPs Sending COVID Spam

203.94.67.129	5976
113.116.207.198	1116
194.146.26.58	466
212.227.254.175	459
95.173.196.206	404
103.225.52.175	357
67.219.150.138	354
103.225.55.219	348
103.225.52.65	327
103.225.52.236	326

Top-15 Countries Sending COVID Spam

JP	10706
US	8257
LK	5976
IN	3554
CN	2546
GB	1180
FR	1012
DE	885
--	669
KR	516

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

Apply For An Affordable Loan at 4%!F(MISSING)or COVID-19 support	24
Apply For An Affordable Loan at 4% For COVID-19 support	16
[pmarc] Invite for a virtual event to release the report on 26 November at 3.30pm to 6pm, "Life in the time of Covid-19: Mapping the impact of Pandemic on the lives and education of children in India	15
NUEVA FORMACION COVID PARA EMPRESAS	6
Veritas ofrece conocer la respuesta ante el COVID-19 en función de la genómica	4
La relazione pericolosa Covid - malattie neurologiche e i progressi della ricerca su Alzheimer al centro del Congresso Nazionale della Società Italiana di Neurologia	3
Organico aggiuntivo O.M. n. 83/2020 ? ?Organico COVID? MONITORAGGIO URGENTE ? TRASMISSIONE DATI.	2
Fw: Positive case Covid-19.	2
TZ - Covid-19 má na světovou ekonomiku větší dopad než velká finanční krize před 12 lety. I pro rok 2021 tak musí firmy počítat s propadem poptávky a opožděnými platbami faktur	2
Webinar "Doing Business in Japan, Covid-19 challenges and opportunities"	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: 133,750
Domains with Potential Mail Servers: 2,621
Email-Capable Domains and Hosts: 50,938
Live Hosts and Domains Not Parked: 46,120

Mobile Apps

Apps in Official Stores: 473

by Store

Apple	238
Google	220
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,801

by Store Type:

Hybrid	932
Secondary	810
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1