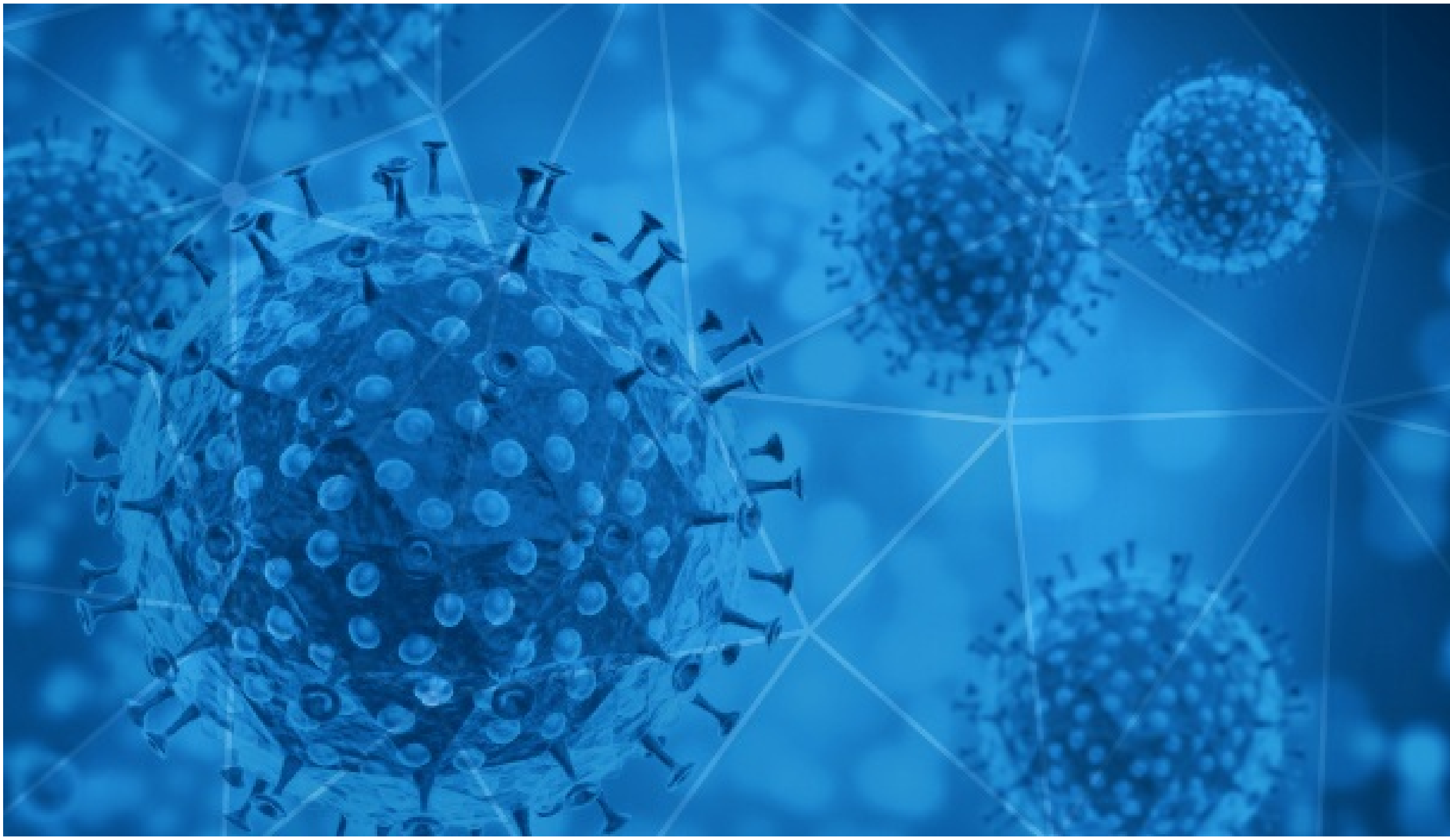
RiskIQ i3:

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

2020-11-24



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

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 2020-11-23 to 2020-11-24. During this period, RiskIQ analyzed 20,682 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,792 unique subject lines observed during the reporting period. The spam emails originated from 1,951 unique sending email domains and 4,472 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: How the virus is hurting careers	2336
COVID-19 Update: We are open and now offering Free Virtual Consultations	915
Covid19_Relief (HMRC) - You are eligible for a grant.	760
UV-C-Sterilisationslampe als guter Weg zur Bekämpfung des Coronavirus (covid-19)	440
Safety measures to stay protected against COVID-19	434
Bonus Covid: Polizza auto da 189€	403
United Nations 2020 Covid-19 Compensation Payment.	366
Re: Digital signage solution for Covid-19	331
Mi seguro insumos covid 19 protege a tu familia	320
Vaccin van Oxford en AstraZeneca ‘minstens zeventig procent effectief’ - Opnieuw coviddrama in Gentse woonzorgcentra - Supermarkten vrezen stormloop tijdens eindejaar	268
VENETO: bando per contributi a supporto delle PMI del settore turistico che svolgono attività di agenzie di viaggio e turismo colpite dell'emergenza epidemiologica da COVID-19. Scadenza 9 febbraio 2021.	231
Feedback on Impact of RBI COVID 19 measures on Home Loan	227
COVID-19: Employer support – live webinars	219
[USAB2B02] Covid-19 will be a memory but you will still need to get it done!	207
Let’s fight together to get through the COVID-19	195
Onze reporter verliest beide ouders in vijf dagen tijd aan corona - Proces rond Mawda (2) van start - Zelfs voormalige bondgenoot uit kritiek op Trump	193
Re: Covid-19 acrylic protect shield	190
[USAB2B01] Covid-19 will be a memory but you will still need to get it done!	172
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	166
Covid lockdowns killing the American dream	165
Re: Covid-19 Disbursement Funds,	156
[USAB2B03] Covid-19 will be a memory but you will still need to get it done!	153
COMMONWEALTH/UNITED NATIONS COVID-19 BUSINESS INTERUPTION GRANT SCHEME	140
NCJ Daily - Health Officer Urges Two Weeks of Distance Learning After Thanksgiving. Incumbent Fennell Seems Unlikely to Make Up Votes. Arcata Restaurants Hit by COVID. Supes to Meet Today on Auditor-Controller's Office Concerns.	132
Fwd:W.H.O COVID 19 GLOBAL SUPPORT FUND -EIM PAYMENTS.	129

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	2336
gmail.com	1150
securesuite.uk	760
126.com	724
usab2bmail.com	594
yourbetterofferisherebcustom0ers.com	511
uvclampen.ch	440
iciciprulife.com	434
rtspogresonlreimmkhadkhodar.com	368
protonmail.com	332

Top-15 IPs Sending COVID Spam

197.81.195.127	760
184.175.86.164	594
77.55.217.43	440
212.227.254.175	279
46.254.37.34	231
104.248.10.217	200
124.219.103.225	195
180.164.168.58	166
112.111.163.33	166
219.65.85.34	155

Top-15 Countries Sending COVID Spam

US	6660
IN	3545
CN	1489
FR	850
ZA	801
DE	795
IT	755
BE	682
PL	537
GB	516

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Information contact à risque covid	1

Top-15 Subjects Containing doc/xlsx Files

COVID 19 WEB DIR STREAMING DIGITALIZZAZIONE, DEMATERIALIZZAZIONE, A.I., Big Data, GDPR: processi, competenze, ruolo DPO 1/12/20	19
Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	7
Update on the COVID 19 potential case in Samoa:	5
NDP - La Covid-19 acelera el ‘home-delivery’ de medicación y la telefarmacia - III Encuentro de Expertos en Gestión Sanitaria y Economía de la Salud	5
NOTICE: MEDIA RELEASE: Update on the COVID 19 potential case in Samoa	4
RV: Remito CARTA DE CULMINACION DE CONTRATO TRABAJADORES CAS COVID	2
Fwd: UPDATED Ontario COVID Update Effective November 16th	2
Coronavirus - Comunicato stampa Federconsumatori	2
Fw: PB > Apoio Economia COVID 19 - MPE - LATIN COSMIC - LDA - 514733586	2
NdP HomeExchange vuelve a ceder sus casas a profesionales que luchan en primera línea contra la segunda ola del COVID-19	2

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: 133,532
Domains with Potential Mail Servers: 2,624
Email-Capable Domains and Hosts: 50,852
Live Hosts and Domains Not Parked: 45,886

Mobile Apps

Apps in Official Stores: 474

by Store

Apple	238
Google	221
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,792

by Store Type:

Hybrid	929
Secondary	804
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1