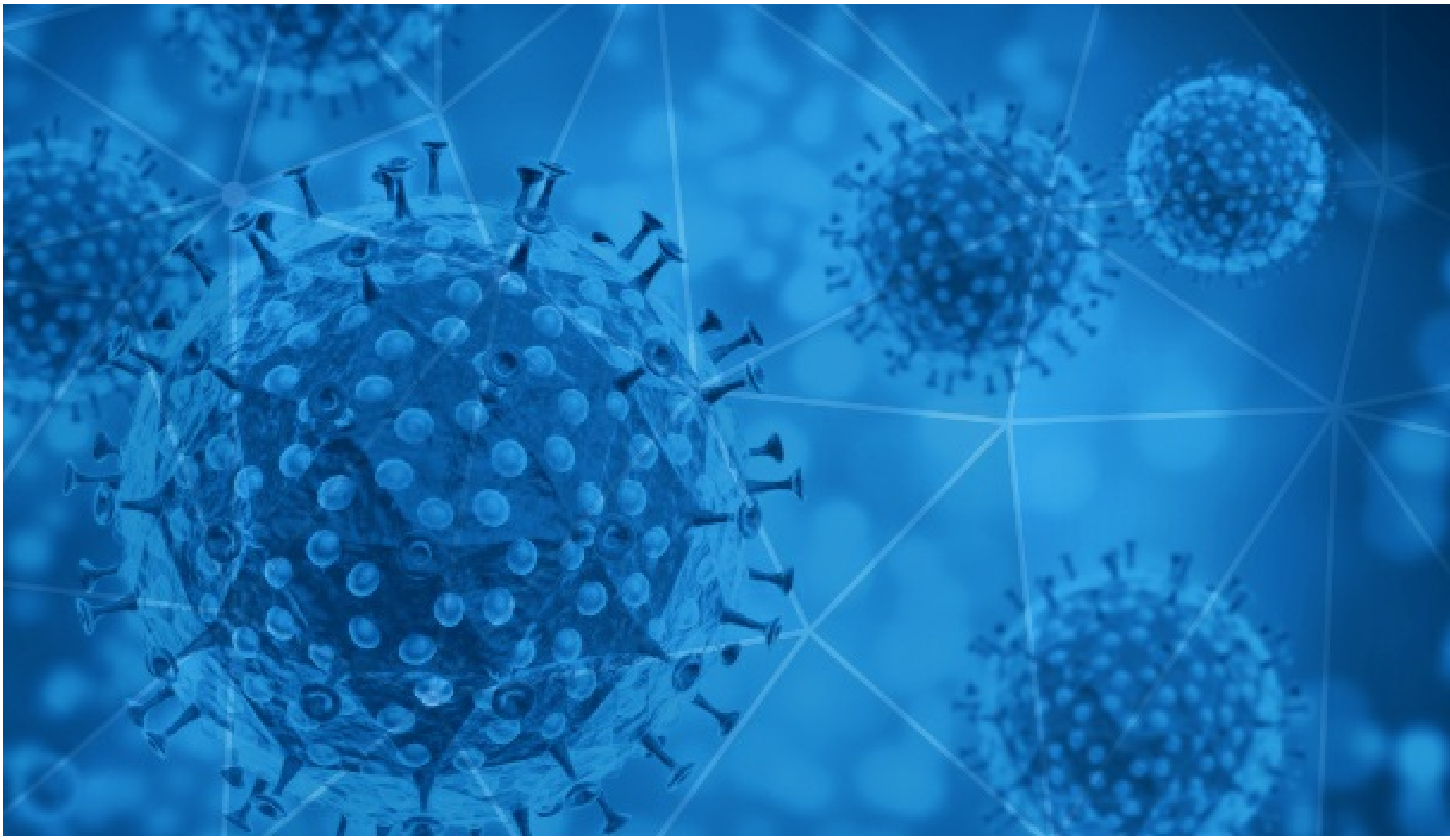
RiskIQ i3:

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

2020-11-23



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 2020-11-22 to 2020-11-23. During this period, RiskIQ analyzed 30,977 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,372 unique subject lines observed during the reporting period. The spam emails originated from 905 unique sending email domains and 2,633 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□	13911
The Corona Letter: Endemic after pandemic?	3304
Covid19_Relief (HMRC) - You are eligible for a grant.	1690
Bonus Covid: Polizza auto da 189€	871
United Nations 2020 Covid-19 Compensation Payment.	736
Re: Digital signage solution for Covid-19	388
Re: Personal, SME & Business Relief (COVID-19)	341
[SPAM] Yahoo/Microsoft Covid-19 Award Fund 2020	341
Vandenbroucke sluit coronaweddenschap af: 'Als het niet lukt, moet u op mijn schieten' - Ouders Mawda: ‘Elke keer als ik de agent zie, heb ik het gevoel dat hij in mijn hart schiet’ - De Croo: ‘Merendeel bevolking in tweede en derde kwartaal 2021…	294
COVID-19 Update: We are open and now offering Free Virtual Consultations	291
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.	275
Smettiamo Covid 19 insieme	262
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	245
Re: Covid-19 acrylic protect shield	244
Detecting COVID-19 From Home Without Pain, Heres How	234
Battered Oyoâs plan for life after covid and more	201
Detecting COVID With All New Pulse Oximeter Up To 70%!O(MISSING)ff	193
Detect COVID-19 Using The Pulse Oximeter- No Pain Or Swabs	192
AWFUL: The States With the WORST Holiday Covid Restrictions	187
Your test for covid is confirmed at Rs.749 only	181
Re: COVID-19 RESPONSE FUND	172
Atencion covid Estudio Contable Legal e Impositivo para tu negocio	168
Re: Covid-19 Disbursement Funds,	156
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	155
Let’s fight together to get through the COVID-19	153

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

epc-store.com	13915
timesofindia.com	3304
securesuite.uk	1690
gmail.com	1210
126.com	878
milliionacres.com	625
cmbmutualfunds.com	444
hotmail.com	351
protonmail.com	329
mail.standaard.be	298

Top-15 IPs Sending COVID Spam

197.81.195.127	1690
103.225.55.187	624
194.146.26.37	610
103.225.52.170	536
103.225.52.64	455
103.225.55.104	407
103.225.53.159	401
103.225.52.159	375
103.225.55.60	348
173.219.81.50	341

Top-15 Countries Sending COVID Spam

JP	14014
IN	3647
US	3354
ZA	1795
CN	1418
FR	935
--	818
IT	599
BE	524
DE	498

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

ANC Weekly COVID-19 Reports	19
CCS/10678 Rebasa Chihuahua las 3 mil defunciones por COVID-19	2
Covid-19, prima causa di morte 2020	2
KORREKTUR: COVID-19 Tagesbericht LGA (Stand 22.11.2020)	2
RV: UCI COVID / CEPILLO DE SUCCION / ADAPTADOR PARA MDI / TRAMPAS PARA EXTRACCION / MUY URGENTE	2
RE: REPORTE COVID-19 RAICA 22.11.2020 (CORTTE: 07.00 HORAS)	2
CDHS Minutes for Wed Nov 25 - 7.30pm & Covid Safe Guidelines	1
[HRC] Corona Challenge 3 (23.11.-06.12.2020)	1
Fwd: RED NEGATIVA COVID	1
COVID POLICY	1

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: 133,423
Domains with Potential Mail Servers: 2,622
Email-Capable Domains and Hosts: 50,805
Live Hosts and Domains Not Parked: 45,572

Mobile Apps

Apps in Official Stores: 474

by Store

Apple	238
Google	221
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,790

by Store Type:

Hybrid	929
Secondary	802
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1