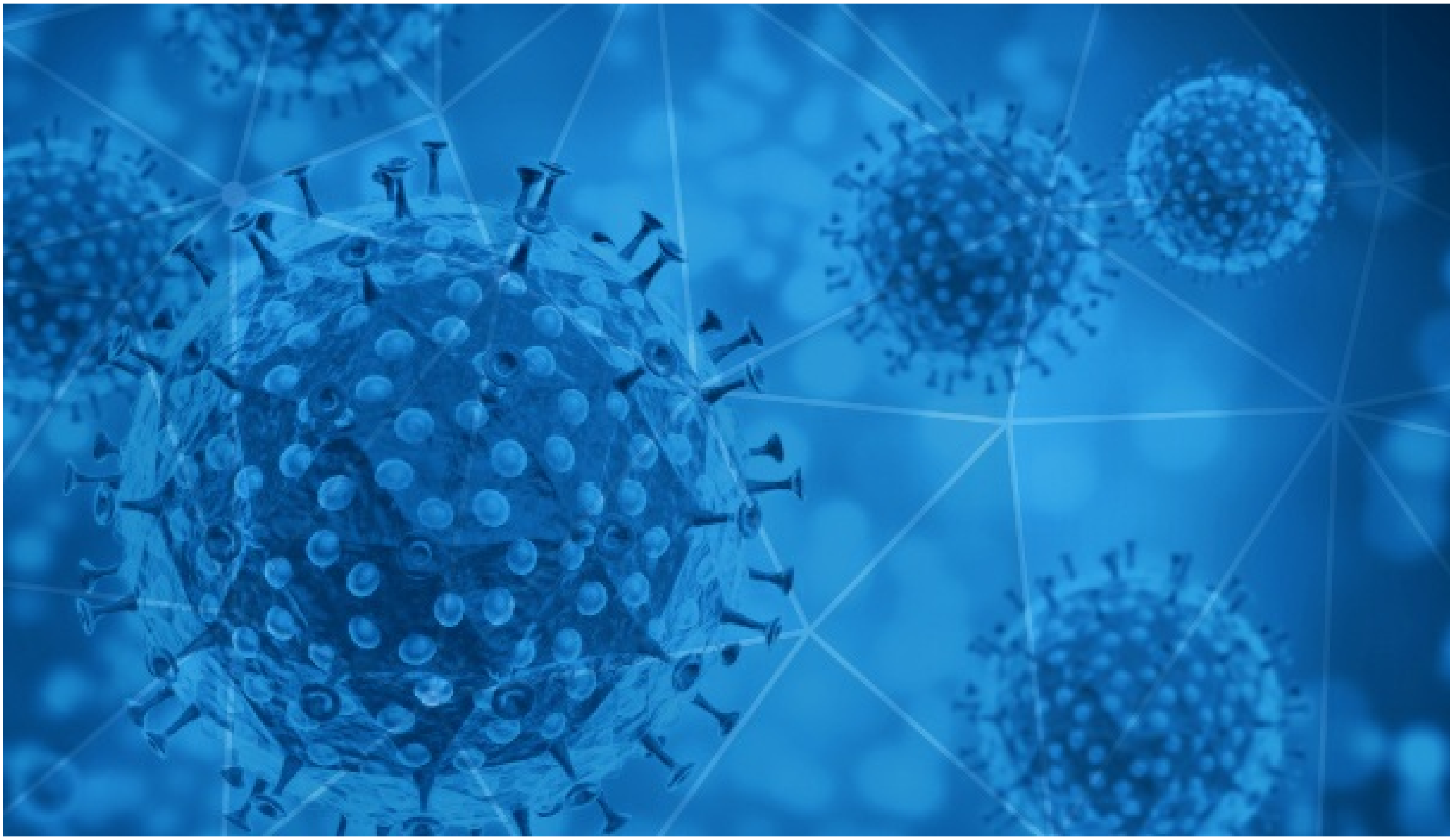
RiskIQ i3:

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

2020-11-20



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 2020-11-19 to 2020-11-20. During this period, RiskIQ analyzed 79,050 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,525 unique subject lines observed during the reporting period. The spam emails originated from 2,214 unique sending email domains and 4,722 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

U.S. reaches grim COVID-19 milestone, key takeaways from the NBA draft, and more from Apple News	41399
Governmentâs Darkest Secret sees the light of day due to Coronavirus Situation.	9606
The Corona Letter: Freeze-dried vaccines to the rescue?	2745
COVID-19 Vaccine for Veterans, Free Customer Experience Certificate, Changes to Patient Billing	2317
Detecting COVID From The Comfort Of Your Home	1061
Fastest And Easiest Way Of Detecting COVID From Home	1001
Best Method For Detecting COVID Is Now Here- No Nasal Swabs	970
Re:Produce hand dispenser at the situation of COVID-19	513
Re: Digital signage solution for Covid-19	491
Atencion covid Estudio Contable Legal e Impositivo para tu negocio	433
Precios IMPACTO / Productos COVID 19	327
Mi seguro insumos covid 19 protege a tu familia	320
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	319
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	317
Direct Client hiring for Senior Network Engineer ÃÂ¢ÃÂ¿ÃÂ¿ 12 Months option to hire with end client- Beltsville, MD OR Chicago,IL (Temporarily Remote Due to Covid)	315
YOU ARE TO BENEFIT FROM MICROSOFT COVID-19 INVESTMENT FUND	261
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove...etc.	243
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	233
Aprovecha Productos COVID en Oferta!	213
Let’s fight together to get through the COVID-19	205
Coronavirus will haunt the economy till 2025	203
Re: Covid-19 acrylic protect shield	202
FDA approves first at-home Covid test	196
[Earn Credits] Lost Your Job Because of COVID-19?	183
Re::Your Covid-19 Fund Benefit	165

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

insideapple.apple.com	41448
blessedme.bid	9607
crumbelcookies.com	3032
timesofindia.com	2745
messages.va.gov	2327
126.com	956
yeah.net	816
gmail.com	637
qq.com	616
public.govdelivery.com	481

Top-15 IPs Sending COVID Spam

104.223.153.74	9604
194.116.229.87	3025
113.83.194.40	513
17.32.227.91	340
17.32.227.56	339
17.32.227.82	328
17.32.227.79	327
17.32.227.106	326
17.32.227.87	320
17.32.227.98	319

Top-15 Countries Sending COVID Spam

US	61666
CN	3311
IN	3211
--	3177
FR	953
DE	918
GB	537
AR	480
BE	437
BR	384

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Fwd: NOTE D'INFORMATIONS - ACTUALITES COVID-19	1

Top-15 Subjects Containing doc/xlsx Files

COVID 19 WEB DIR STREAMING SUPERBONUS 110%, ECOBONUS, CESSIONE DEL CREDITO: aspetti contrattuali e finanziari-fiscalità 18/12/20	31
Ocena ryzyka zawodowego (aktualizacja pod względem COVID -19)	8
Fe de erratas_NP: Beko lanza en exclusiva en España la secadora de la gama HygieneShield, que elimina el coronavirus	6
COVID 19 WEB DIR STREAMING SUPERBONUS 110%!,(MISSING) ECOBONUS, CESSIONE DEL CREDITO: aspetti contrattuali e finanziari-fiscalità 18/12/20	3
NP-Minsa distribuyó más de 279 toneladas de suministros médicos para enfrentar la COVID19 a regiones y a Lima Metropolitana	3
Ik deel Opdracht burgerschap vrijheid-solidariteit corona (1)-1 met u	2
I: LAGUNA TRAVEL AGENCY SRL: CAPODANNO 2020/21 "Tour tra le meraviglie di VENEZIA & LE ISOLE DI MURANO, BURANO E TORCELLO" dal 31 Dicembre 2020 al 03 Gennaio 2021 - 03 ESCURSIONI CON GUIDA & GIRO IN GONDOLA - in omaggio Assicurazione Covid-19	2
RE: Suspected positive COVID19 Swap samples heading to NZ	2
Je partage « Consistances_COVID_A_Partir_Du_23_Novembre_2020 » avec vous	2
WG: ver.di Information Corona-Maßnahmen und Kinderbetreuung	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: 133,083
Domains with Potential Mail Servers: 2,625
Email-Capable Domains and Hosts: 50,609
Live Hosts and Domains Not Parked: 45,756

Mobile Apps

Apps in Official Stores: 474

by Store

Apple	238
Google	221
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,758

by Store Type:

Hybrid	923
Secondary	776
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1