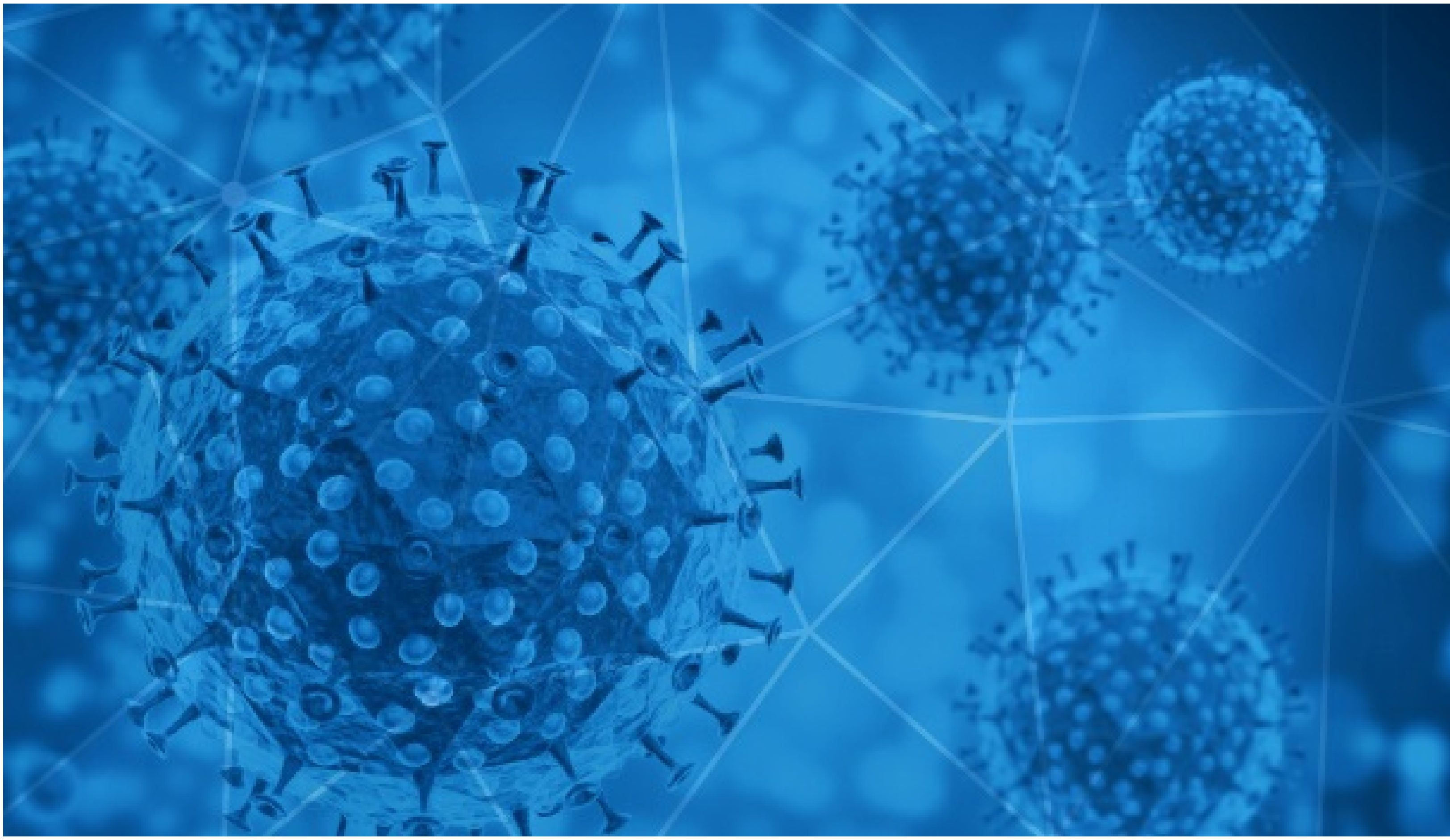
RiskIQ i3:

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

2020-10-05



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 2020-10-04 to 2020-10-05. During this period, RiskIQ analyzed 40,230 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,024 unique subject lines observed during the reporting period. The spam emails originated from 857 unique sending email domains and 2,609 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□□	19803
The Corona Letter: Why tests don't tell you about intensity of Covid	4503
Hope you are safe during this Covid-19 period?	1482
Arrived during this Covid-19 period,	1390
Shibuya's Annual Halloween Event Goes Virtual Due to the Coronavirus - Sankaku News	997
Limpieza y desinfeccion COVID 19	533
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	367
Re: Personal & Business Relief (COVID-19)	330
Register Now For The Webinar On Job Opportunities Post COVID-19	320
COVID-19 KILLED ANTHONY	299
COVID -19 RELIEF FUND	281
SwipeBlue to defeat Trump and end Covid	274
President Trump's positive COVID test changes EVERYTHING!!	232
Re: Re: Covid-19 acrylic shield	200
Vandenbroucke 'zeer ongerust': ‘We moeten aantal contacten beperken’ - Lachaert: ‘De Wever heeft zwaar geblunderd op historisch moment’ - Hoe een coronagolf de entourage van Donald Trump overspoelde - Lieven Annemans, de geluksprofessor die niet kan…	199
Re: Covid-19 Protective acrylic sneeze guards	196
Fundo de socorro da OMS Covid 19	191
Re: Covid-19 Charity Donation	191
Re: Covid-19 acrylic protect shield	184
Let’s fight together to get through the COVID-19	175
COVID-FONDS VERFÜGBAR	164
Re: Hand wash with 75% alcohol, keep away from Covid-19	162
Re: keep away from Covid-19	155
Your COVID-19 Test Results	154
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products).	144

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

epc-store.com	19808
timesofindia.com	4504
gmail.com	4261
yeah.net	1048
sankakucomplex.com	997
126.com	987
tutanota.com	533
cmbmutualfunds.com	361
enlinea.cl	355
timesjobs.com	320

Top-15 IPs Sending COVID Spam

38.117.65.152	2872
208.100.24.254	997
103.225.52.25	599
103.225.52.158	549
103.225.54.249	531
103.225.54.214	513
103.225.55.30	493
103.225.54.95	475
103.225.55.99	430
103.225.55.180	408

Top-15 Countries Sending COVID Spam

JP	19858
US	7160
IN	4802
CN	2822
AR	554
DE	535
BE	475
PL	364
PH	361
FR	359

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

ANC Weekly COVID-19 Reports	29
How did COVID-19 affect the financial performance of MENA’s telecom operators and groups?	4
COVID -19 DUTY SCHEDULE OF DNB/CPS RESIDENTS	2
Bol. Loc. 3954/2020 “Impulsa IMSS programa “Alimentamos tu cuerpo y tu corazón, no estás solo” dirigido a pacientes con COVID-19”	1
COVID/School/Monday	1
IZJAVA COVID-19 (Gibalne urice z MIGI-jem)	1
covid protocol 20-21 fysieke stageuren en NLA's	1
Buletin de presa 04.10.2020 + comunicat actiuni prevenire COVID 19	1
RECEBIMENTO DE KIT COVID19	1
CONSOLIDADO DE LLAMADA CASO COVID-19	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: 127,816
Domains with Potential Mail Servers: 2,821
Email-Capable Domains and Hosts: 48,405
Live Hosts and Domains Not Parked: 72,276

Mobile Apps

Apps in Official Stores: 444

by Store

Apple	226
Google	203
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,521

by Store Type:

Hybrid	837
Secondary	629
Affiliate	55

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1