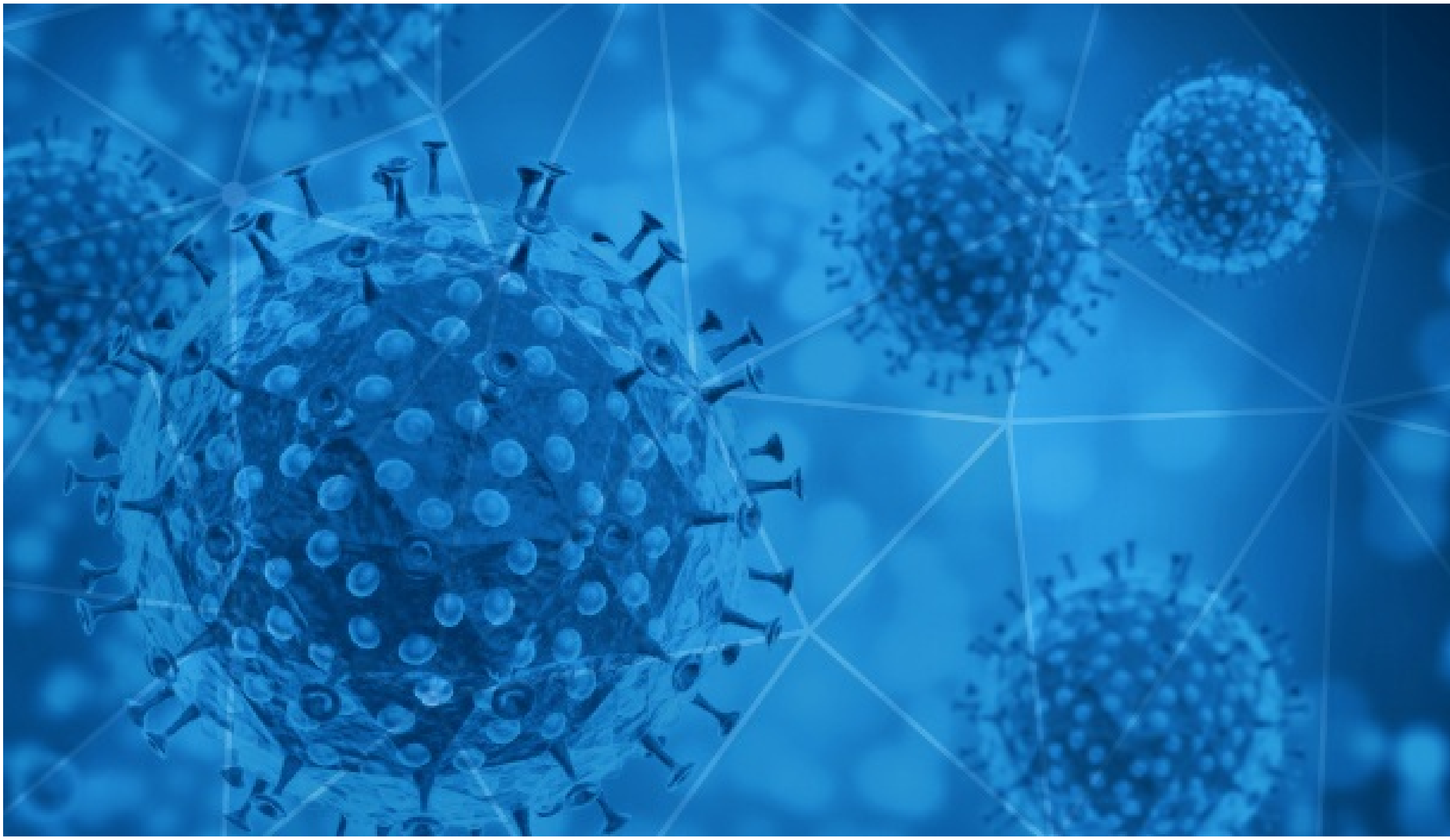
RiskIQ i3:

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

2020-09-04



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 2020-09-03 to 2020-09-04. During this period, RiskIQ analyzed 16,862 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,350 unique subject lines observed during the reporting period. The spam emails originated from 1,366 unique sending email domains and 2,923 unique SMTP IP Addresses. Analysts identified 43 emails which sent an executable file for Windows machines.

Top-25 Subjects

Covid-19 Cash Support für Sie	1038
Reife Frauen zu Corona-Zeiten treffen	1005
Precios Imbatibles / Productos COVID 19	681
Evite contagios, no al Covid19, Accese, Asistencia biométricos	667
The Corona Letter: Cheap steroids make strong case	550
TCS hiring soon; will start onboarding 40,000 employees | Infosys, TCS, HCL Tech to gain the most benefit in post Covid era	507
Cuidate del COVID19 con nuestros productos	388
ATALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID -19	363
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	360
Precios Rebajados COVID-19	349
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW.	233
Instalación Medidas de Prevención Covid-19 - OFERTA LIMITADA	226
Desinfectamos su ambiente de coronavirus	208
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	206
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	199
Desinfeccion Preventiva Covid19	189
COVID-19 Pandemic - Most valuable financial lessons learnt	188
Eliminar Covid-19	186
Ante el elevado riesgo de contagio por Coronavirus en Perú.	181
Desinfeccion covid19 mediante termoniebla	178
TermoScanner Anti-Covid. Sconti fino al 50 % e pronta consegna. Non abbassiamo la guardia!!!	168
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	167
Prevención Covid-19	163
Re: Personal & Business Funding (COVID-19 Relief) for redacted@threatwave.com.	155
Re: Defeat Coronavirus, non contact fever alarm device	145

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmail.com	2537
126.com	1377
data2web.de	1005
countermail.com	963
sopytecchile.com	667
timesofindia.com	550
techgig.com	507
banestado.cl	488
keyable.net	277
campus4x.cl	265

Top-15 IPs Sending COVID Spam

80.169.245.163	1038
46.20.37.30	1005
46.101.218.158	667
190.247.243.228	631
219.65.84.187	505
185.104.152.200	484
119.122.91.189	295
190.247.241.78	246
113.116.205.126	243
185.235.131.114	233

Top-15 Countries Sending COVID Spam

US	3069
DE	2073
CN	2018
ES	1746
IN	1494
AR	1193
FR	702
CL	621
PL	501
IT	429

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Besplatna distribucija zaštitne opreme Covid-19 (Ministarstvo zdravlja)	19
Covid-19 დამცავი აღჭურვილობის უფასო განაწილება (საქართველოს საზოგადოებრივი ჯანმრთელობის დეპარტამენტი)...	13
Covid-19 დამცავი აღჭურვილობის უფასო განაწილება (საქართველოს საზოგადოებრივი ჯანმრთელობის დეპარტამენტი)	9
****IMPORTANT** Bulk Quote Request-Covid19**	2

Top-15 Subjects Containing doc/xlsx Files

Financial Accounting Impact of COVID-19- An In-depth Look at IFRS	10
[PRESS RELEASE] Katadata x KawalCovid-19 "6 bulan Covid-19 di Indonesia, Kapan Berakhirnya?"	6
Bezpieczne Dziecko 2020/2021 - NNW (w tym COVID-19) + OC bez konieczności zawierania polisy!	4
Zbytek roku bude pro řadu firem kritický, kvůli Covid-19 může být letos až o čtvrtinu více insolvencí	3
Team Educates COVID-19 Action Plan and Available Candidates	2
COVID REFLECTION	1
SOLICITUD DE RESULTADOS DE MUESTRAS COVID 19	1
Covid Travel Restrictions - updated 03 September 2020	1
COVID 19 Line List	1
DEMANDE DE PPSPS COVID-19 : Restructuration EHPAD Richard CONFLANS ST HONORINE - PHASE II	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: 122,776
Domains with Potential Mail Servers: 2,942
Email-Capable Domains and Hosts: 45,561
Live Hosts and Domains Not Parked: 66,861

Mobile Apps

Apps in Official Stores: 410

by Store

Apple	212
Google	183
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,270

by Store Type:

Hybrid	734
Secondary	483
Affiliate	53

Blacklisted Mobile Apps: 27

by Store Type:

Secondary	24
Official	2
Hybrid	1