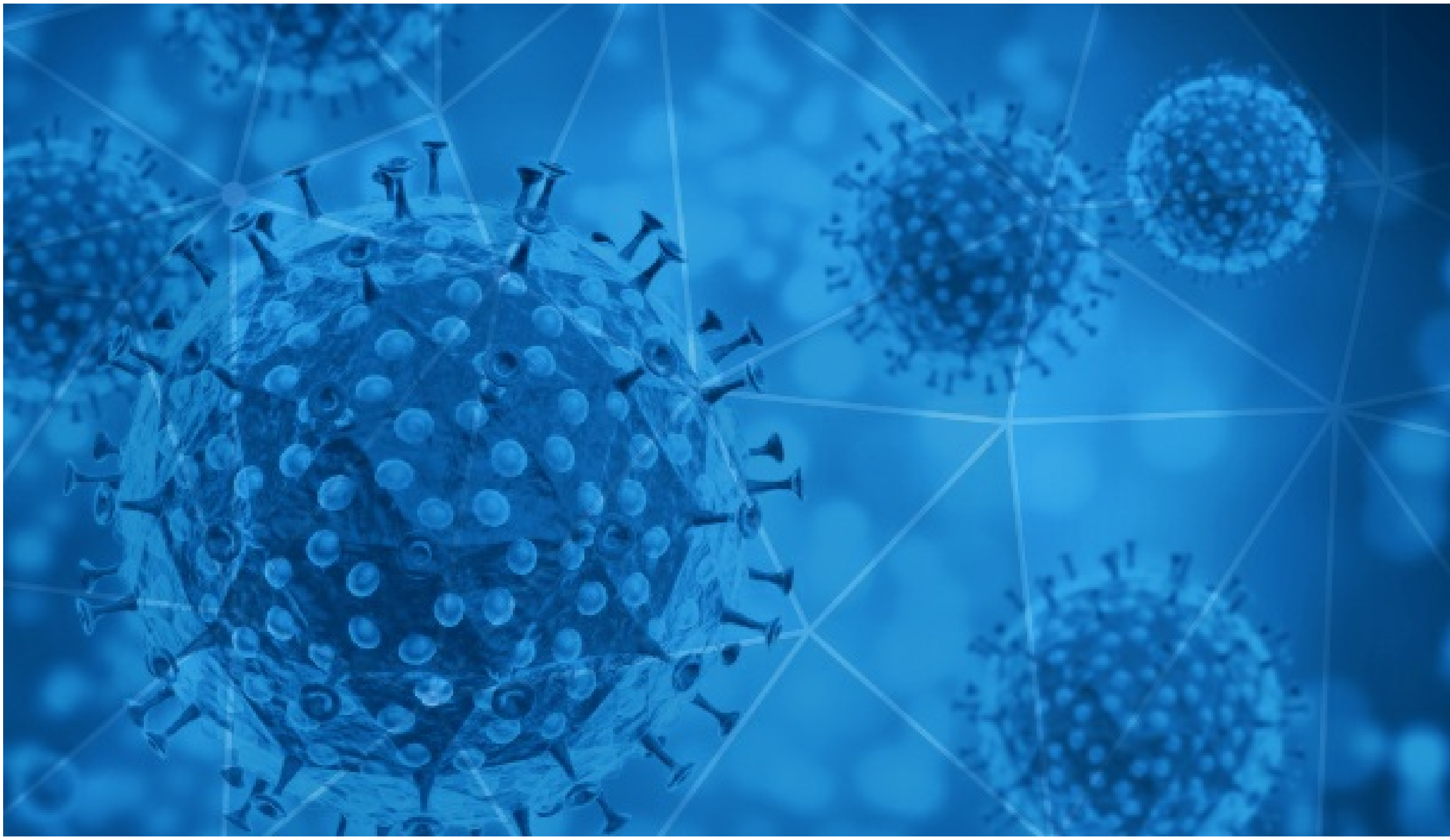
RiskIQ i3:

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

2020-10-06



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 2020-10-05 to 2020-10-06. During this period, RiskIQ analyzed 36,818 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,375 unique subject lines observed during the reporting period. The spam emails originated from 2,037 unique sending email domains and 4,402 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□	14338
The Corona Letter: A test minus scarce reagents	3762
Protection from Coronavirus and other diseases	1297
500.000,00 USD Covid -19 Financial Relief Funds! test	593
Limpieza y desinfeccion COVID 19	501
Covid19 Products	426
Test Rápido Covid-19 Segunda Generación - 10.000 Un Entrega Inmediata	414
Fwd:Credito Covid-19 Aprobado.	374
Liquidacion Final Covid19	369
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	300
500.000,00 USD Covid -19 Financial Relief Funds!	286
COVID-19 KILLED ANTHONY	256
*****SPAM*** COVID-19 COMPENSATION PAYMENT**	255
Az áldozatok kártalanításának jelölése az Egészségügyi Világszervezettol (Covid.19)	236
Revisa si tienes acceso a Credito FOGAPE COVID-19	224
Let’s fight together to get through the COVID-19	173
Van Gucht: "Stabilisatie coronacijfers heeft zich helaas niet doorgezet" - BV's getuigen: "Ik woog amper 41 kilo en werd dik genoemd" - "Trump wordt als proefkonijn behandeld"	172
Coronavirus Job Retention Scheme	143
Coronaproof events organiseren in Gent	143
Re: Personal & Business Relief (COVID-19)	139
Are you confident your retirement portfolio won't be affected by the coronavirus?	137
Re: Covid-19 Protective acrylic sneeze guards	129
Re: Covid-19 acrylic protect shield	128
Corona legt Strukturkrise offen: Das Geschäftsmodell der Industrienation Deutschland ist bedroht	125
COVID -19 RELIEF FUND	122

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

epc-store.com	14343
timesofindia.com	3762
claimintl.com	904
yeah.net	842
126.com	668
gmail.com	638
tutanota.com	598
herculist.com	577
stargoldmedics.com	481
outlook.com	439

Top-15 IPs Sending COVID Spam

143.107.178.200	903
216.87.190.232	576
103.225.52.176	479
103.225.53.128	466
103.225.53.223	439
139.99.133.125	426
103.225.53.99	395
216.87.190.231	375
103.225.52.45	375
190.114.253.218	353

Top-15 Countries Sending COVID Spam

JP	14557
US	6543
IN	3991
CN	2141
BR	952
DE	931
FR	702
BE	694
AR	661
CL	506

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

Press Release: COVID-19 Song, Happy Magic TARAHOROVA Saves Countless life in this Pandemic	8
WEBINAR COVID19 Crisi pandemica, L.40/20, organi sociali: continuità aziendale, adeguati assetti, moratorie 28-29/10/20 4 MODULI	3
MAP Virtual Week debate futuro das empresas na era pós-COVID-19	2
Welcome to GlobalSurg-CovidSurg Week - Period 1	2
IMSS FOTO NOTA.- Desde las Oficinas Centrales del IMSS, se rinde homenaje a fallecidos por COVID-19 y personal de salud en todo el país (LINK VIDEO)	2
COVID Information to Parents	2
Coronavirus - Comunicato stampa Federconsumatori	2
Η ΠΕΡΙΦΕΡΕΙΑ ΠΕΛΟΠΟΝΝΗΣΟΥ ΘΩΡΑΚΙΖΕΙ ΤΑ ΑΘΛΗΤΙΚΑ ΣΩΜΑΤΕΙΑ ΜΕ ΤΟ RAPID TEST COVID19 ΤΗΣ ARATOSMEDICA.	2
La Melatonina bloquea la replicación del virus responsable de la COVID-19	2
[Chsstudents] ADDITIONAL RULES AND REGULATIONS TO MITIGATE THE SPREAD OF COVID 19 IN ALBERT COOK LIBRARY	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: 127,886
Domains with Potential Mail Servers: 2,822
Email-Capable Domains and Hosts: 48,440
Live Hosts and Domains Not Parked: 72,308

Mobile Apps

Apps in Official Stores: 443

by Store

Apple	225
Google	203
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,526

by Store Type:

Hybrid	838
Secondary	633
Affiliate	55

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1