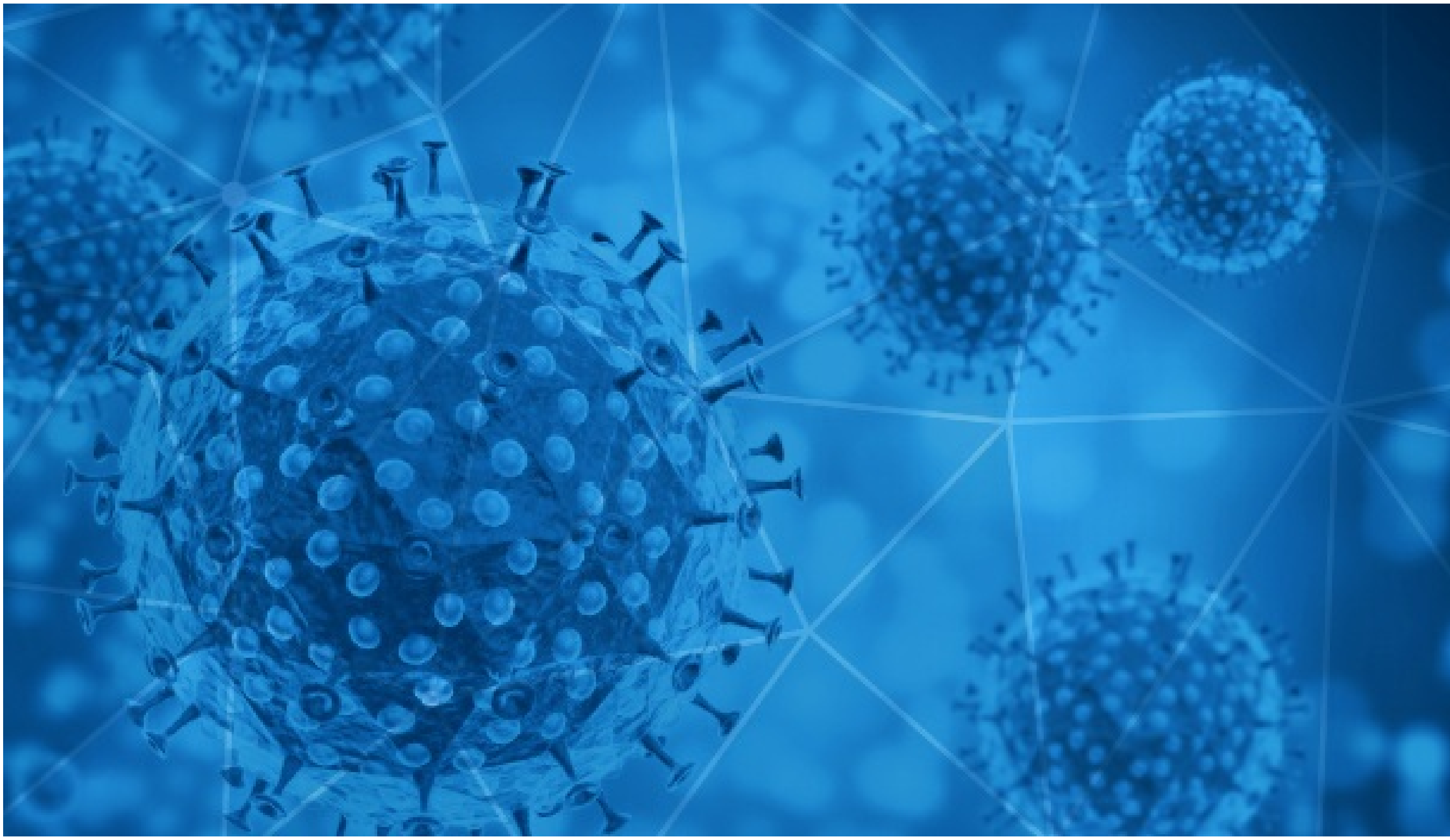
RiskIQ i3:

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

2020-07-28



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 2020-07-27 to 2020-07-28. During this period, RiskIQ analyzed 34,381 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,445 unique subject lines observed during the reporting period. The spam emails originated from 1,772 unique sending email domains and 3,489 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Does testing negative really mean recovery?	2416
PyMEs contra el COVID19	1654
COVID-19 Protection Products - Update	1374
Making money during the covid!	781
MICROSOFT COVID-19 RELIEF FUND - GLOBALGIVING	560
My COVID-19 Donation	529
Covid Victims Compensation	514
COVID Mafia Exposed	395
Let’s fight together to get through the COVID-19	350
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	340
Soluciones para la prevencion del covid19	309
Como volver a la actividad post coronavirus?	308
Importante reportar resultados positivos y negativos COVID-19	294
Cabinas para la prevencion del coronavirus?	281
Productos Covid 19 - Entrega Gratis RM	269
ARCO Dual Detector de Temperatura y Metales - Covid-19	267
Super Promociones Julio - Proteccion COVID-19	263
COVID-19 Lastest News	254
Test Rapido COVID 19	240
Fwd:Credito Covid-19 Aprobado.	216
2020 COVID-19 Scholarships at University of Minnesota + Fordham University – USA + Others	214
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	207
[CND Español - 4191]. 9 cambios que veremos en los hoteles después de la Covid	203
COVID-19 Chinese protective products	200
China Supply Chain of COVID-19	198

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

cl.jooble.org	9820
countermail.com	2552
timesofindia.com	2416
gmail.com	2043
medicproduction.com	1374
163.com	1166
126.com	997
topdigitalad.com	782
microphilanthropies.com	658
trendingtopic.cl	528

Top-15 IPs Sending COVID Spam

180.235.132.241	1374
31.129.170.191	782
190.247.243.54	768
190.247.243.11	615
164.163.167.2	560
201.231.58.171	560
187.174.101.179	526
153.122.116.244	514
223.74.106.137	508
119.139.137.162	349

Top-15 Countries Sending COVID Spam

US	9126
CA	7231
AR	3097
IN	3009
CN	2659
HK	1506
FR	1045
BR	946
DE	920
UA	790

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

NOTICE: COVID 19 State of Emergency Orders Amended 27th July 2020	5
KVNO Praxisinfo: Corona-Test für Reiserückkehrer aus Risikogebieten	5
COVID-19 RELIEF FUNDING	4
corona OPŠTA BOLNICA GORNJI MILANOVAC_ (3).docxIIIIIIIIIIIII.docx	3
Parents Handbook COVID-19	2
FW: August COVID19 Schedule	1
REİS COVID-19 GÜVENLİ ÜRETİM BELGESİ'Nİ ALDI	1
POSITIVOS COVID-19 PENDIENTES POR NOTIFICAR A SIVIGILA	1
GT 28 and COVID	1
Covid Welcome Protocol	1

- CONFIDENTIAL -

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: 116,438
Domains with Potential Mail Servers: 2,855
Email-Capable Domains and Hosts: 43,984
Live Hosts and Domains Not Parked: 65,627

Mobile Apps

Apps in Official Stores: 359

by Store

Apple	190
Google	160
WindowsPhone	8
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 926

by Store Type:

Hybrid	594
Secondary	293
Affiliate	39

Blacklisted Mobile Apps: 23

by Store Type:

Secondary	20
Official	2
Hybrid	1