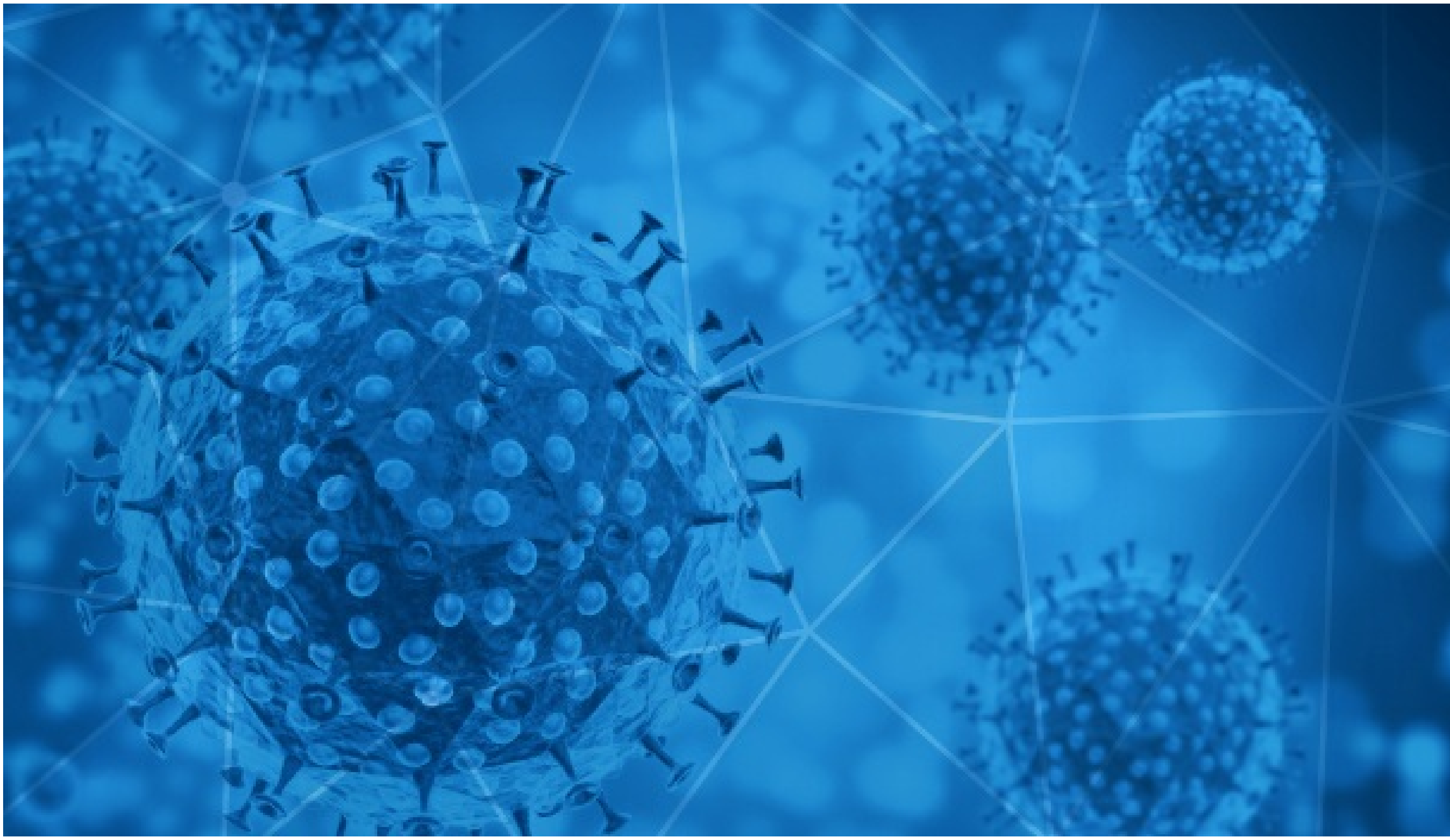
RiskIQ i3:

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

2020-10-01



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 2020-09-30 to 2020-10-01. During this period, RiskIQ analyzed 30,933 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,999 unique subject lines observed during the reporting period. The spam emails originated from 2,049 unique sending email domains and 4,834 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: The lesson from open schools	4306
Key moments from a bitter presidential debate, a COVID-19 outbreak in the NFL, and more from Apple News	3512
Hatsune Miku Expo 2020 USA & Canada Cancelled by the Coronavirus - Sankaku News	1129
ICO Covid Inversión	1097
COVID-19 PRODUCTS	963
My COVID-19 Donation	465
9 Inspiring Backyard Cottages | What Homeowners Want in the Time of COVID-19 | Modern Country Home on a Sweet Potato Farm	424
Espacios libres de Coronavirus el 100% del tiempo	423
Essential Covid19 PPE -	359
Aufgrund der Covid-19-Pandämie wurden Ihnen von FRANÇOIS 3,5 Millionen US-Dollar gespendet	357
Modern Country Home on a Sweet Potato Farm | Light and Airy Master Bath Makeover | What Homeowners Want in the Time of COVID-19	337
PRUEBA NASOFARINGEA - DETECCION DE COVID 19-	337
Test Rápido Covid-19 Segunda Generación - 10.000 Un Entrega Inmediata	331
How to manage the impact of COVID-19 on your Business	328
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	314
Light and Airy Master Bath Makeover | What Homeowners Want in the Time of COVID-19 | Modern Country Home on a Sweet Potato Farm	301
Naukri.com - COVID 19 Impact Survey	254
Protégete RESPONSABLEMENTE Contra el Covid -19 / Los Mejores Precios	232
Re: Covid-19 acrylic protect shield	222
COVID -19 RELIEF FUND	185
Honolulu COVID 19 Emergency Hospital	184
Covid-19 Rapid Test Kits	181
$3.5 Million Has Been Donated To You,By FRANÇOIS due to the covid-19 pandemic	179
Re: Re: Covid-19 acrylic shield	177
Test de deteccion rapida COVID19	177

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	4309
insideapple.apple.com	3697
gmail.com	2360
sankakucomplex.com	1129
houzz.com	1062
sabaziusvi.com	995
stargoldmedics.com	963
126.com	949
yeah.net	891
fashion.asos.com	842

Top-15 IPs Sending COVID Spam

208.100.24.254	1129
85.204.116.143	963
41.67.35.47	641
201.223.81.161	558
43.239.110.184	465
85.204.116.157	359
58.220.13.146	328
219.65.85.13	265
219.65.85.11	249
219.65.85.24	244

Top-15 Countries Sending COVID Spam

US	11889
IN	5350
CN	2982
ES	1535
RO	1347
DE	1043
AR	849
CL	802
FR	774
SD	641

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

PHHS 9 30 2020 End of Day Report for COVID 19	7
Covid 19 Wage Subsidy for affected Tourism/Manufacturing businesses	5
COVID-19 Focus OIC: novità contabili e fiscali, soluzioni, rinvii e orientamenti AdE Milano 20/10/20	3
NdP_MUUV lanza ViriScreen la primera mampara patentada con luz ultravioleta de uso médico que desinfecta de COVID el interior de los vehículos en menos de un minuto	3
[ODP-MASTER-PROVIDER-LIST] ODPANN 20-069 Update: Coronavirus Disease 2019 (COVID-19): 2020-2021 Waiver Cap Exception Guidance for the Person/Family Directed Support and Community Living Waivers	3
NP InfoJobs_6 de cada 10 empleados aprueban la gestión laboral de la COVID-19 de su empresa	3
IMA National Commemoration of 'International Day of Older Persons' Webinar on 'Care of Older Persons during Covid 19 Pandemic and beyond (Programme attached)	3
(Declaraciones de audio y vídeo) La Mesa Enfermera rechaza la realización de las pruebas de detección del coronavirus en las oficinas de farmacia	3
PRODUCTOS COVID PARA EMPRESAS	2
Nota de prensa - Asepeyo aborda nuevos proyectos de transformación digital, a partir de las lecciones aprendidas en la gestión de la COVID-19	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: 127,341
Domains with Potential Mail Servers: 2,874
Email-Capable Domains and Hosts: 48,134
Live Hosts and Domains Not Parked: 71,979

Mobile Apps

Apps in Official Stores: 439

by Store

Apple	223
Google	201
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,494

by Store Type:

Hybrid	823
Secondary	616
Affiliate	55

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1