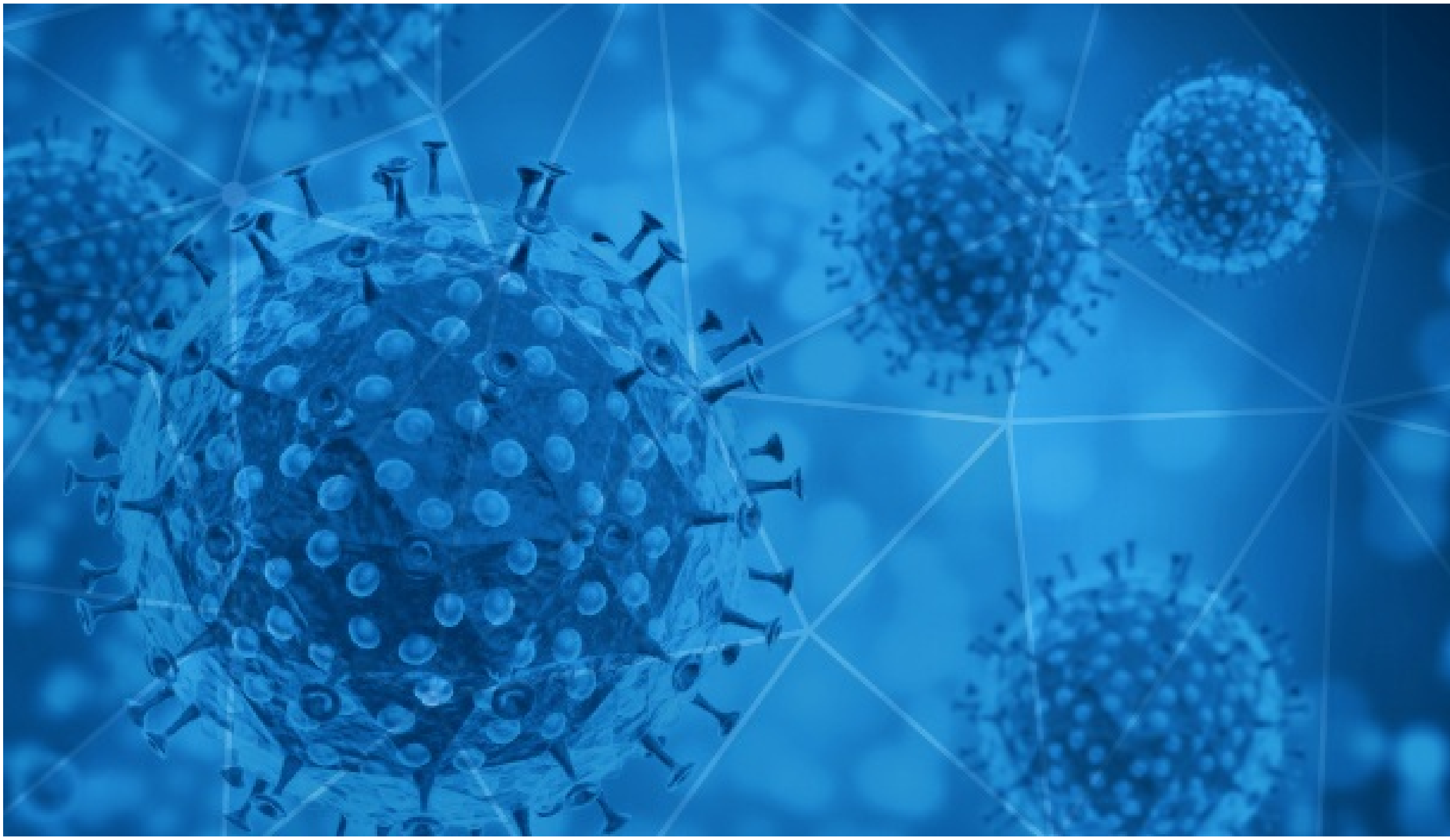
RiskIQ i3:

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

2020-09-16



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 2020-09-15 to 2020-09-16. During this period, RiskIQ analyzed 19,640 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,288 unique subject lines observed during the reporting period. The spam emails originated from 1,486 unique sending email domains and 3,005 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: A reality check from a vaccine maker	1427
Reife Frauen zu Corona-Zeiten treffen	1355
Essential Medical PPE to Prevent COVID19	1197
Essential Medical Protective Equipment to Fight Covid19	1110
Coronavirus (Covid19) Relief Bailout	556
Frente al Coronavirus nos Cuidamos Todos !	522
Videos para la prevencion de Covid	510
Prevencion de covid19	476
Evita Contagios de CORONAVIRUS con SHYCOCAN	456
Covid-19 Rapid Test Kits	317
Join the Bowser Administration for a Community Leader Telephone Townhall on Coronavirus	305
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	254
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	233
Contactless infrared body temperature thermometer defeat Coronavirus	215
Re: Defeat Coronavirus, non contact fever alarm device	213
Cuidate del COVID19 con nuestros productos	195
COVID-19 : Redesign Website | SEO (Results Guaranteed) [REDACTED_DOMAIN]	182
Federal Judge Rules PA Governor's COVID Shutdown UnConstitutional. Sunshine Patriot Debra Strickland, and her Nye County Commissioners' "Second Amendment Sanctuary" nothing but lip service...	182
Covid-19 Mask, Auto Mask machine	181
My COVID-19 charity donation	176
COVID19 Support Funds	165
Re: For Your Covid-19	163
Let’s fight together to get through the COVID-19	146
¡COVID-19, Protege el ingreso de tus trabajados!	138
Alternatives to Traditional Air Carriers Amidst Covid Crisis	136

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	1427
gmail.com	1358
data2web.de	1355
medicproduction.com	1303
countermail.com	1181
stargoldmedics.com	1110
126.com	1106
keyable.net	551
grupocorreomasivo.com	522
cexchange-io-uk.org	474

Top-15 IPs Sending COVID Spam

46.20.37.30	1355
86.104.194.169	1197
85.204.116.71	1110
190.247.254.15	647
113.116.205.15	522
103.20.213.86	474
190.247.240.86	281
210.104.208.203	247
181.46.136.168	233
209.123.15.146	182

Top-15 Countries Sending COVID Spam

US	4063
CN	2534
RO	2414
IN	2403
DE	2134
AR	1584
FR	778
KR	470
GB	394
ES	300

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

CUMPLIMIENTO DE PROTOCOLOS DE BIOSEGURIDAD PARA MANEJO DE PANDEMIA CORONAVIRUS - COVID19	13
PHHS 9 15 2020 End of Day COVID 19	6
Financial Accounting Impact of COVID-19- An In-depth Look at IFRS	6
Nuevo pulsador sin contacto para la época Covid	3
covid 19 Payments.	2
Loughborough College- Communicating about Covid cases at the college	2
FW: Je partage « COVID 15 Septembre (HCN) » avec vous	2
China manufacturer factory directly | excellent quality favourable price fast delivery | disposalbe non-woven medical\surgical\civilian face mask anti covid-19	2
RT-PCR COVID-19,Rapid Antigen and Total Antibody Screening Solution with Emergency Services across Pan-India	1
RE: REPORTE COVID PEDREGAL	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: 124,108
Domains with Potential Mail Servers: 2,960
Email-Capable Domains and Hosts: 45,910
Live Hosts and Domains Not Parked: 69,621

Mobile Apps

Apps in Official Stores: 415

by Store

Apple	211
Google	189
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,330

by Store Type:

Hybrid	772
Secondary	503
Affiliate	55

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	25
Hybrid	2
Official	2