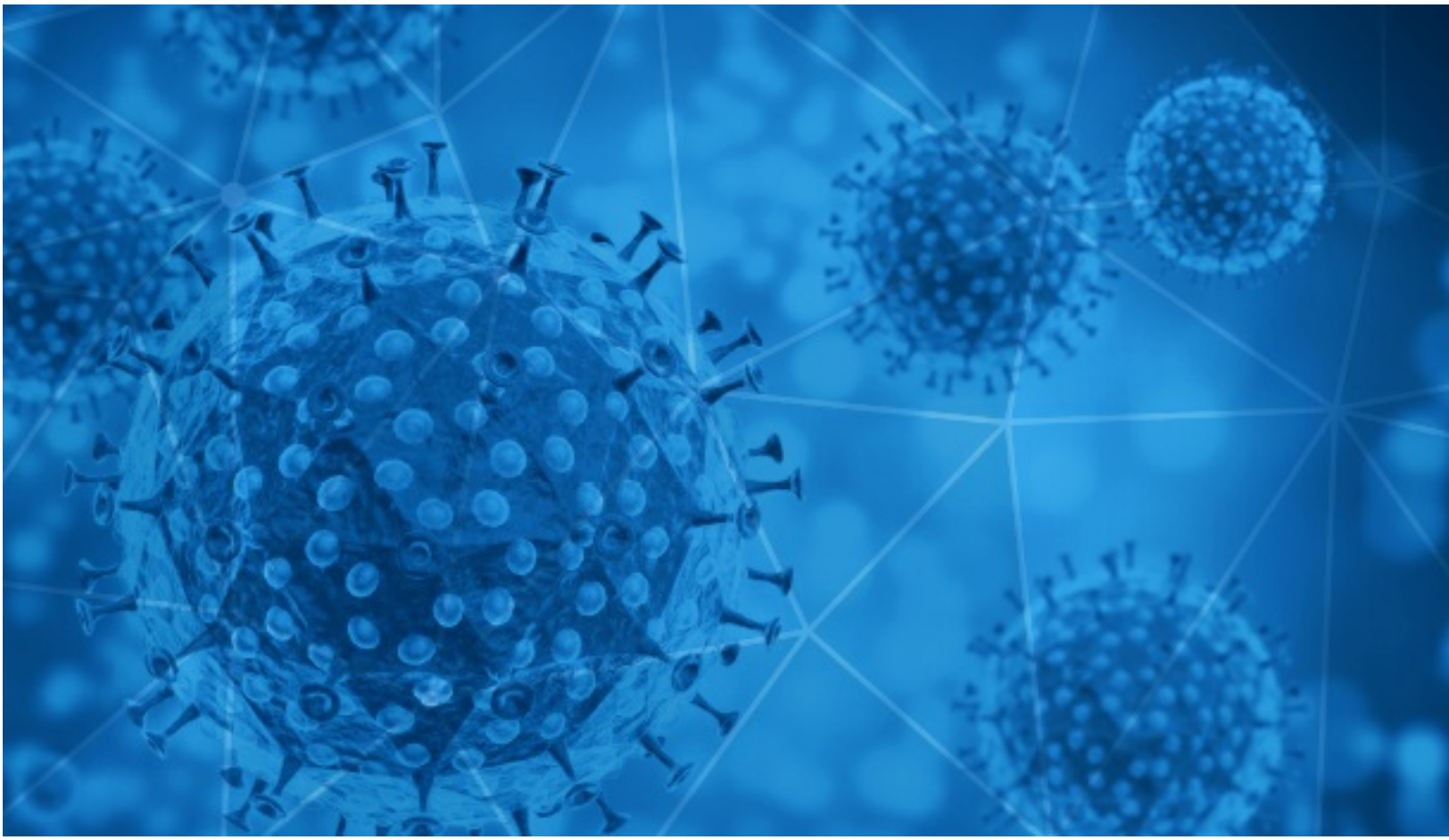
RiskIQ i3:

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

2020-10-12



RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

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

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 2020-10-11 to 2020-10-12. During this period, RiskIQ analyzed 43,047 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,020 unique subject lines observed during the reporting period. The spam emails originated from 883 unique sending email domains and 2,731 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	18626
The Corona Letter: The virus' real picture	4792
COVID 19 Donation	1931
(□□) #□□□□□□ □ □□ □□ [2020□ □□□ CORONA □□ □□] □□□ □□□□ □□□~ [□□□□ □□□□ □□ □ □□□□ □ / □□□□□ □□□ □□□ □□□□]	1602
Covid-19 Loan Program -From Ms Margert Schwites.	1371
Let's fight COVID with 5x Immunity Booster	1296
Test rapido para la deteccion del Coronavirus	435
Protection from Coronavirus and other diseases	432
Test de deteccion rapida COVID19	426
Re: Your Order Corona virus Protection Pills and sex pills.	391
Help to fight COVID-19 fever alarm security door	340
Contactless infrared body temperature thermometer defeat Coronavirus	340
Re: Defeat Coronavirus, non contact fever alarm device	321
Limpieza y desinfeccion COVID 19	268
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	260
Na 'angstaanjagende coronacijfers: ‘Verstrengingen zijn nodig’ - Politie legt studentenfeest in Brussels hotel stil - ‘Je wenst niemand erge ziekte toe, maar voor Trump maak ik een uitzondering’ - Steven Van Gucht: ‘Ik zou persoonlijk niet gaan…	216
Re: Covid-19 Protective acrylic sneeze guards	213
Hi, Reminder call for your Covid antibody test at Rs 750 only | Confirm soon.	208
RE: IMPORTANT INFORMATION ,CORONA VIRUS DEATH …	207
Re: Covid-19 acrylic protect shield	197
"Tweede lockdown is niet veraf" - "Coronacijfers stijgen sneller dan verwacht" - GROTE TEST. Zijn biogroenten lekkerder dan gewone?	195
Re: Re: Covid-19 acrylic shield	192
COVID -19 RELIEF FUND	180
Re:□coronavirus civil mask / Chinese qualified manufacturer	176
Mamparas de proteccion COVID19	176

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

epc-store.com	18630
timesofindia.com	4793
gmail.com	3932
qoo10.com	1602
tutanota.com	1468
keyable.net	1001
126.com	903
yeah.net	833
163.com	629
seajin.chtah.com	540

Top-15 IPs Sending COVID Spam

43.239.110.184	1929
191.96.165.251	1463
181.239.232.106	1149
113.116.206.106	926
103.225.55.168	665
103.225.53.71	602
103.225.53.84	535
103.225.54.228	511
103.225.53.151	500
103.225.54.154	457

Top-15 Countries Sending COVID Spam

JP	18703
IN	6974
US	3768
CN	3648
FR	1704
IT	1672
KR	1629
AR	1483
BE	783
--	436

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Top-15 Subjects Containing doc/xlsx Files

ANC Weekly COVID-19 Reports	36
CCS/10278: Suman 17,599 casos confirmados y 1,504 fallecimientos por COVID-19	2
URBANO VEGA - AREA COVID/PEDIATRIA	2
Daily Report Covidb19 PJO PT.GPE	1
Fw: COVID-19 Positive case	1
COVID-19 Site Impact Monitoring (Tableau)	1
REPORTE DIARIO E MEDICAMENTOS COVID-19 C.S. ZAMACOLA DIA 10-10-2020	1
COVID-19 EMAILER	1
IMSS Boletín 688.-Realizan en UMAE No. 34 de Nuevo León exitosa cirugía de corazón abierto a joven paciente con COVID-19 (LINK DE VIDEO Y FOTOS)	1
Emailer- Intensive & Focussed COVID- 19 Campaign	1

RiskIQ
22 Battery St., 10th Flr
San Francisco, CA 94111
United States

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: 128,930
Domains with Potential Mail Servers: 2,802
Email-Capable Domains and Hosts: 48,675
Live Hosts and Domains Not Parked: 72,851

Mobile Apps

Apps in Official Stores: 454

by Store

Apple	230
Google	209
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,564

by Store Type:

Hybrid	849
Secondary	658
Affiliate	57

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1