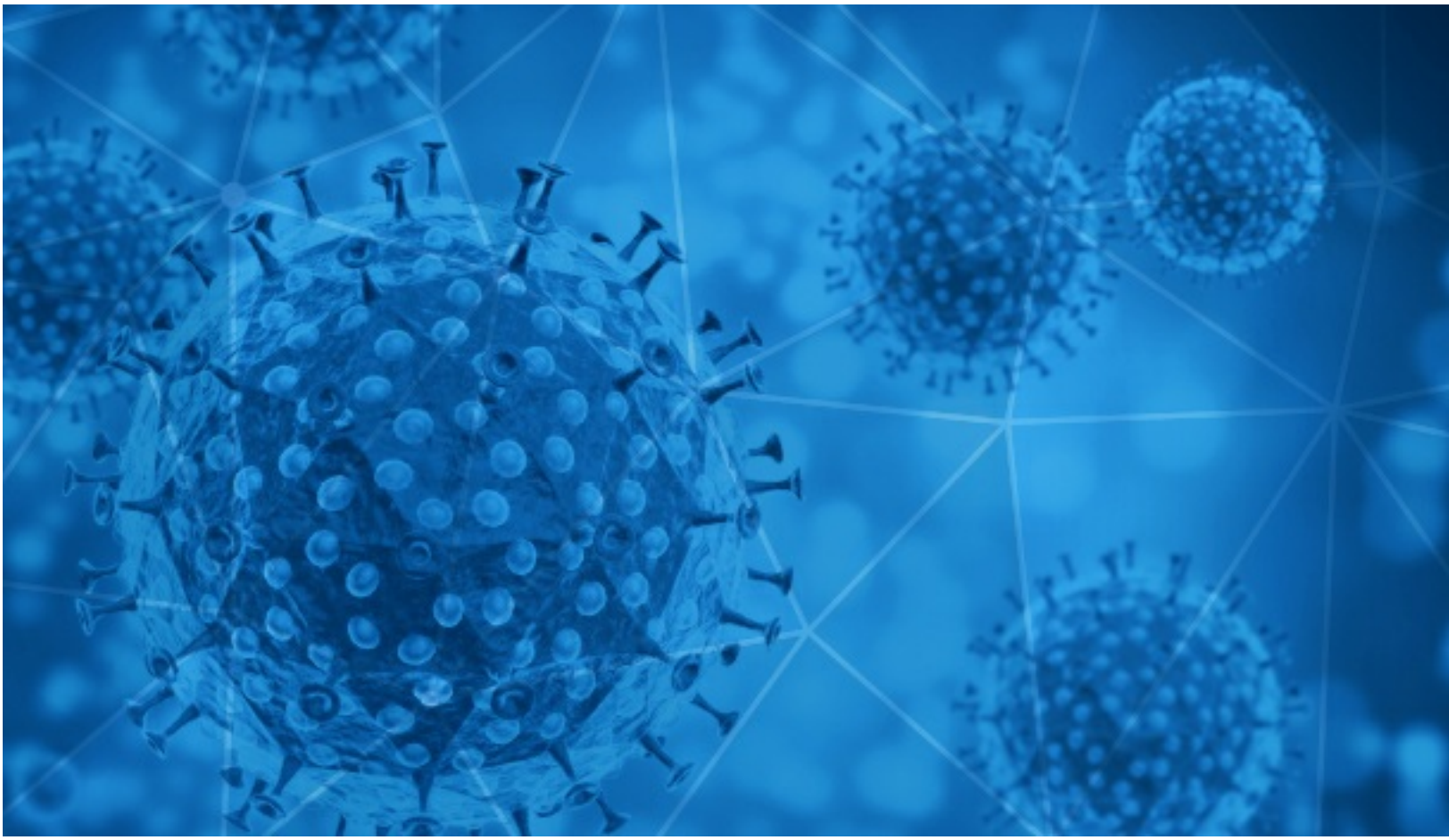
RiskIQ i3:

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

2020-11-16



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 2020-11-15 to 2020-11-16. During this period, RiskIQ analyzed 24,171 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,702 unique subject lines observed during the reporting period. The spam emails originated from 982 unique sending email domains and 2,867 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Will vaccine hoarding prolong the pandemic?	3691
COVID cases rise in all 50 states 4 the first time +White men swung 2 Biden. Trump gains with blacks	1468
COVID-19 Compensation Claim	1050
Diddy Takes A Hilarious DIVE {VIDEO} R&B Singer Jeremih In ICU Battling COVID+ Trump FINALLY admits-	956
Atencion covid Estudio Contable Legal e Impositivo para tu negocio	533
COVID 19 LOCK DOWN COMPENSATION FUND	418
Re: Digital signage solution for Covid-19	399
Weyts werkt aan aparte teststrategie in scholen - Jong, gezond, antistoffen, en toch opnieuw besmet - Topduivin New Kim uit Berlaar verkocht voor recordbedrag - Drie agenten gewond na coronacontrole in Elsene - Nobelprijswinnaar voor vrede op oorlogspad	380
Arrêtons Covid 19 ensemble	375
Boost your internet speeds while you're quarantined from the CoronaVirus	370
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	367
Coronavirus 'Stay home - earning big money home'	356
Do you have Covid Antibodies ?	334
Re: Personal, SME & Business Relief (COVID-19)	333
Reserve Your Seat . Thriving not just surviving post-COVID	267
Re: Covid-19 acrylic protect shield	251
Covid 19 Command Center	240
[Earn Credits] How to bank *BIG WINNING* Traffic in Covid-19?	228
Covid 19 loan offer	214
COVID-19 Cash Support Grants	211
Let’s fight together to get through the COVID-19	206
Biden Coronavirus Task Force Member Profited Off Lockdown Policies He Pushed: Report	176
protective supplies for corona	171
Re: Hand wash with 75% alcohol, keep away from Covid-19	170
I suspect I had Covid-19 in May. I had the symptoms. I wasn't tested. Testing was dif...?	165

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	3693
sampark.gov.in	2506
caribbeanfever.com	2424
126.com	1184
aliyun.com	1085
yeah.net	1067
gmail.com	646
aol.com	635
outlook.com	626
163.com	542

Top-15 IPs Sending COVID Spam

194.68.48.50	1050
192.3.3.143	422
211.23.8.250	418
51.195.139.18	375
103.105.196.32	370
91.151.89.167	368
201.231.10.98	279
189.254.149.228	240
120.229.72.95	222
219.65.85.13	213

Top-15 Countries Sending COVID Spam

IN	6755
US	6493
CN	3290
SE	1056
FR	828
AR	556
BE	542
RU	530
TR	498
TW	445

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	13
Fwd: Mundspülungen gegen Corona	2
Proposal. COVID-19	2
Covid Case	2
Reporte diario de los fallecidos por COVID-19 al 11/11/2020	2
REPORTE DIARIO COVID 19	2
RE: REPORTE COVID-19 RAICA 15.11.2020 (CORTTE: 07.00 HORAS)	2
CCS/10619 Suman más de 2 mil 700 los decesos por COVID-19 en Chihuahua	1
Fwd: COVID-19 LA ZONA ROSSA IN CAMPANIA LE PROPOSTE DICONFESERCENTI DONNA CHE FANNO IMPRESAPRATICO':Le misure di restrizione non devono essere intese come punizioni o situazionidi vantaggio, bensì devono essere interpretate come la presenza dello Stato incondizioni di difficoltà	1
[Mailinglist-anm] Potenziamento uffici del processo settore lavoro primo grado a seguito Covid 19	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: 132,682
Domains with Potential Mail Servers: 2,645
Email-Capable Domains and Hosts: 50,516
Live Hosts and Domains Not Parked: 45,950

Mobile Apps

Apps in Official Stores: 475

by Store

Apple	239
Google	221
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,744

by Store Type:

Hybrid	913
Secondary	772
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1