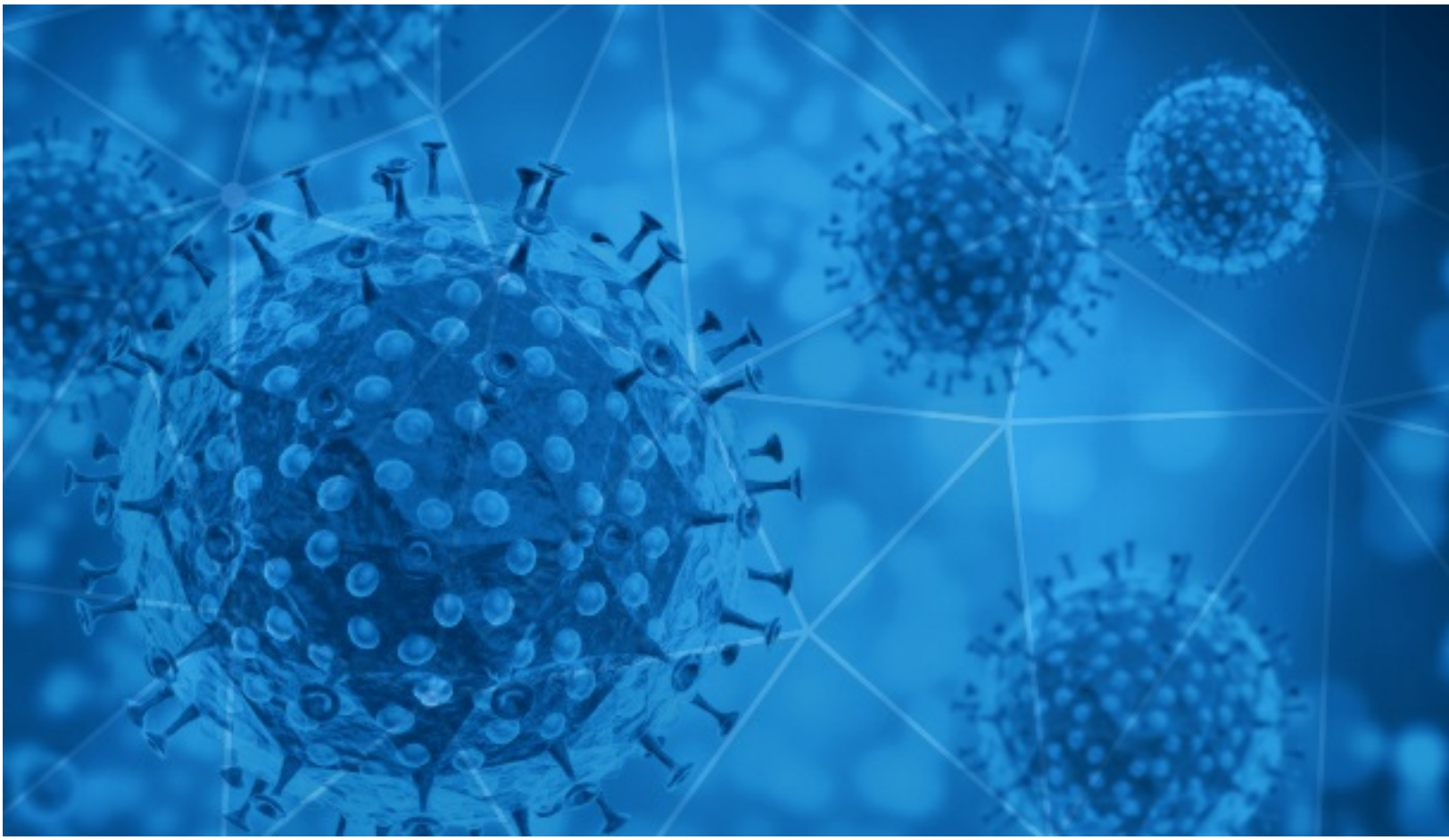
RiskIQ i3:

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

2021-01-12



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 2021-01-11 to 2021-01-12. During this period, RiskIQ analyzed 28,786 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 5,536 unique subject lines observed during the reporting period. The spam emails originated from 4,925 unique sending email domains and 4,177 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Which vaccine will you get?	3989
Covid-19 Test	1194
Covid Test	1101
COVID19 Testing At Home Painlessly Using The Pulse Oximeter	880
Skip Painful COVID19 Testing, Instead Test From Home Using Pulse Oximeter	878
Painlessly Test For COVID19 At Home On Your Fingertips Using All New Pulse Oximeter	829
Skip Painful COVID19 Testing, PulseOximeter Allows You To Test From Home Effortlessly	677
Testing For COVID19 Has Been Made Simpler With All New Pulse Oximeter	660
Stoping COVID19 With The Pulse Oximeter- The Most Important Test You May Ever Take	659
Need windows? Nervous about COVID-19? We Offer Free Virtual Consultations!	655
Extra editie: blijf bouwen en verbouwen in corona-wintertijd	649
HERZLICHEN GLÜCKWUNSCH, CASH COVID-19 PALLIATIVEN AUS MEINEN LOTTERIEGEWINNEN	467
Let’s fight together to get through the COVID-19	422
COVID 19 SPENDE	371
COVID-19 vaccine research survey	297
COVID-19 RELIEF AID.	297
Wearing KN95 Certified Masks Can Help Contain COVID19 VIRUS- Shop Today 50%!O(MISSING)ff	246
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove...etc.	206
COVID-19 Vaccine Acceptance survey -- 19 استبيان قبول لقاح كوفيد	202
COVID-19 coming back to China and Impact on the logistics market	178
Destination Thailand News - News Alert - Thailand Orders 63 million doses of Covid-19 Vaccines and Offers 2yr Amnesty to Migrant Workers	161
Vrachtwagen rijdt in op auto die vertraagt voor file: twee doden - Ook Trumps vluchtroute is afgesneden - Uitgelegd: zo krijg je in Vlaanderen je coronavaccin in één van de 120 centra - Republikeins congreslid excuseert zich na citeren Hitler tijdens...	158
Take Advantage Of 50%!O(MISSING)ff KN95 Certified Mask To Help Curve COVID19 Virus	152
COVID-19: Employer support – live webinars	149
Wear KN95 Certified Mask To Help Curve COVID19 Virus	142

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	3992
copayhealpmckesson.com	2588
stargoldmedics.com	2378
betwithustips.com	1996
gmail.com	1288
expobase.be	788
163.com	456
hongchengco.com	349
covt-com.tk	320
akhirawahdnshaamolananjibobih.com	316

Top-15 IPs Sending COVID Spam

213.142.149.74	2581
172.245.93.73	2378
194.116.228.131	1991
81.95.112.26	788
45.148.8.74	593
45.148.8.75	585
45.148.8.76	574
45.148.8.77	541
5.83.23.13	467
45.149.77.81	371

Top-15 Countries Sending COVID Spam

US	7749
--	4771
IN	4255
TR	3157
CN	1908
BE	1024
GB	707
UA	594
FR	380
DE	375

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

COVID-19-Newsletter Janvier 2021	1

Top-15 Subjects Containing doc/xlsx Files

COVID, LOCKDOWN, Election, Protest, Riots NOW IS THE TIME FOR YOUR 1ST FINANCIAL REVIEW	38
Greeting and How to fight Corona in home.	3
1130 test eseguiti nel primo giorno dello screening anti-Covid	3
PEDIDO MATERIAL COVID	2
Nota de Prensa: Abanderamiento, el novedoso modelo de negocio que reduce el cierre de bares y salva empleos ante el COVID-19	2
In-school Covid-19 Vaccination for Teachers and School Staff | 19-التطعيم ضد كوفيد للمعلمين والعاملين في المدارس	2
Right to Represent and Rate Confirmation :: CVSJP00050360:: Pharmacist - Covid-19 Vaccination Support :: 285 West Pine,Ponchatoula,LA-70454	2
Fwd: COVID report from CVASU	2
WG: 20210104_EKSZ_ Kampfmittelbegleitung einer Baumaßnahme zur "Coronaverfügung II" der Region Hannover - Tauber	2
Corona-Beschränkungen in Hessen: Auslegungshinweise	2

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: 139,144
Domains with Potential Mail Servers: 2,568
Email-Capable Domains and Hosts: 53,005
Live Hosts and Domains Not Parked: 51,548

Mobile Apps

Apps in Official Stores: 502

by Store

Apple	245
Google	241
WindowsPhone	15
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,010

by Store Type:

Hybrid	1036
Secondary	911
Affiliate	63

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1