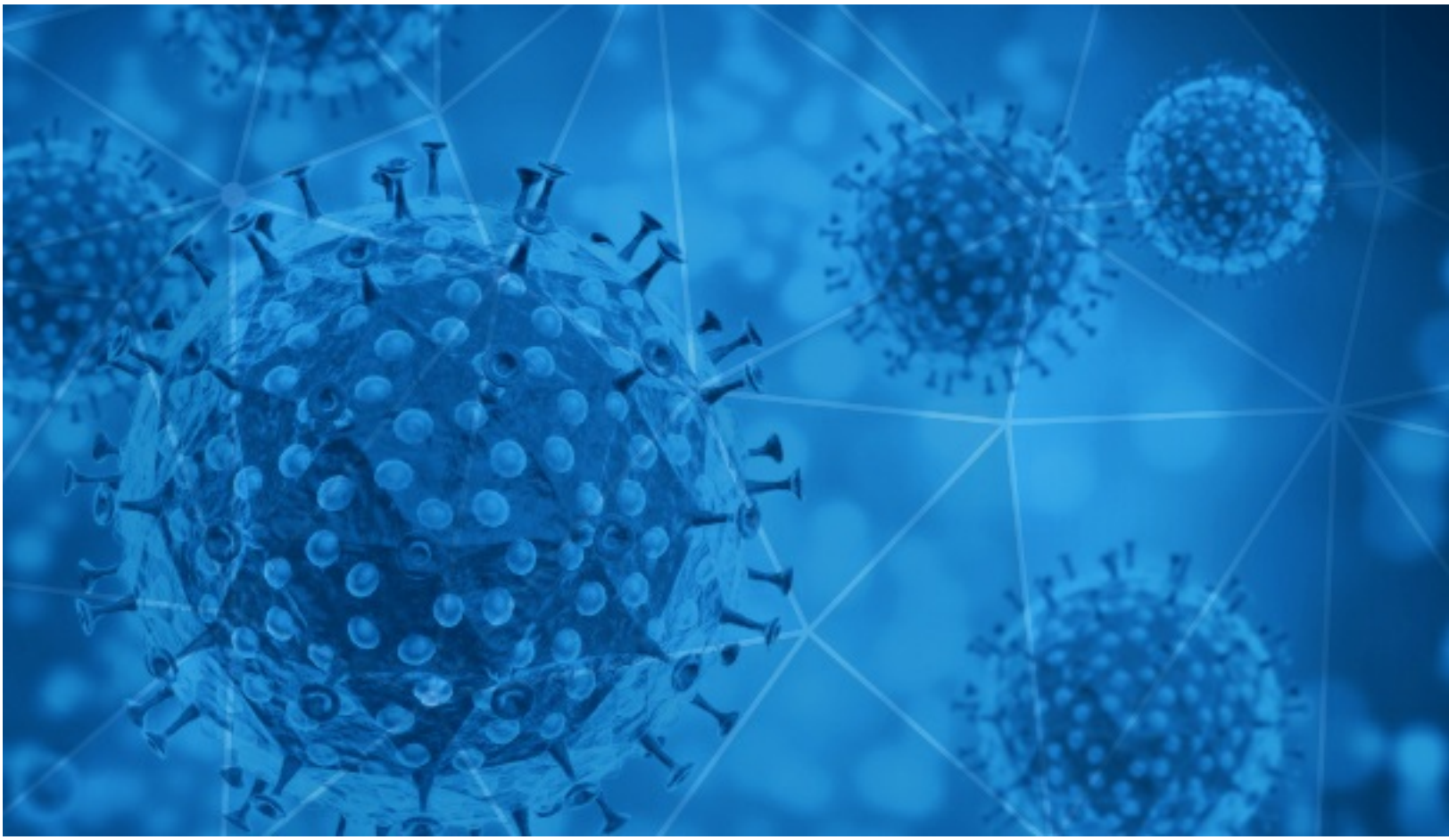
RISKIQ®

RiskIQ i3:

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

2021-01-18



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 2021-01-17 to 2021-01-18. During this period, RiskIQ analyzed 33,122 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,866 unique subject lines observed during the reporting period. The spam emails originated from 996 unique sending email domains and 2,015 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□	19042
The Corona Letter: Nearly 2 lakh shots, some hesitancy and a few glitches	4870
LJC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation	1364
HERZLICHEN GLÜCKWUNSCH, CASH COVID-19 PALLIATIVEN AUS MEINEN LOTTERIEGEWINNEN	509
Re: Personal, SME & Business Relief (COVID-19).	378
Arma tu Kit contra el Covid-19	302
‘We gaan de regels voor terugkerende reizigers waterdicht maken’ - Met deze handige tips red je zelf je coronakapsel - Derde passagier op vlucht naar Australian Open test positief, trainingen zijn uitgesteld - Uitbraak Britse variant in…	259
128 besmettingen 'Britse corona' in één woonzorgcentrum - Hoe vertrouweling van Gert Verhulst met 5 miljoen ging lopen - Aldi-klant gaat helemaal door het lint	210
Re: Personal, SME & Business Relief (COVID-19)	189
Covid-19 Global Relief Fund	123
Covid19 Relief Fund	116
✔ Testiranje na COVID-19 -50% | Razbijanje miogeloza i masaža leđa | Ginekološki pregled -42% Jankomir | Čišćenje kamenca -89% Vrapče | Lovran, Hotel Park 4 -40% | Medicinska pedikura -51% Dubrava | 10 godina mlađi izgled bez noža! -71%	97
Chinese protective products of COVID-19	93
Covid-19-Spenden	88
Covid-19: de nouveaux avantages extra-légaux pour 2021 | Tous les jobs en IT | L'Université d'Harvard met en ligne 140 cours gratuits	88
Covid-19 Payment $1,750,000.00!!!!!!!!!	86
COVID-19 Chinese protective products	85
--*--*--_FINALLY__THE__END__TO__COVID19_?_--*--*--	83
Re: Certyfikowane Przylbice COVID19	81
Hancock says UK nearing 'home straight' in Covid fight | Brexit is 'new dawn' | Next Merkel elected	70
LJC/Donation-ref:K011- You have been Chosen for our COVID-19 Donation.	68
Deze medicijnen zijn verborgen dikmakers * Zo ga je om met de bijwerkingen van het coronavaccin	67
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove…etc.	62
From United Nations Organization Regarding Your Covid Grant .	56
Re:□coronavirus civil mask / Chinese qualified manufacturer	54

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	19043
timesofindia.com	4876
gmail.com	1417
eremitmms.com	874
cmbmutualfunds.com	619
mailinator.cl	302
163.com	294
mail.standaard.be	259
nieuwsblad.be	221
outlook.com	178

Top-15 IPs Sending COVID Spam

103.131.245.194	871
103.225.53.125	713
81.46.222.75	558
5.83.23.13	496
103.225.52.221	461
103.225.52.51	448
103.225.53.126	442
103.225.55.186	437
103.225.53.227	437
103.225.53.28	422

Top-15 Countries Sending COVID Spam

JP	19065
IN	4875
US	2254
--	891
BE	845
PH	619
ES	610
FR	595
UA	526
CN	363

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	31
ECONOMIC AND SOCIAL COUNCIL (UN ECOSOC FIGHT FOR CORONA VIRUS PANDEMIC / 2020)	13
CCS 11118 Confirma Salud 14 nuevas defunciones y 70 contagios más de COVID-19 en la entidad	2
IMSS Boletín 027.- Hospital de Magdalena de las Salinas del IMSS reconvierte 114 camas para pacientes referidos con COVID-19 (FOTOS)	2
Fwd: CVASU COVID-19 test report on 17/01/2021	2
covid	2
IMSS Boletín 028.- Sumará IMSS 40 camas para atención a convalecientes de COVID-19 en Naucalpan (LINK DE VIDEO Y FOTOS)	2
hospitalizacion COVID	1
Ενημέρωση για COVID-19 από το Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών (17/1/2021)	1
TR: vaccination covid	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: 139,982
Domains with Potential Mail Servers: 2,563
Email-Capable Domains and Hosts: 53,196
Live Hosts and Domains Not Parked: 46,017

Mobile Apps

Apps in Official Stores: 506

by Store

Apple	248
Google	241
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,036

by Store Type:

Hybrid	1048
Secondary	925
Affiliate	63

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1