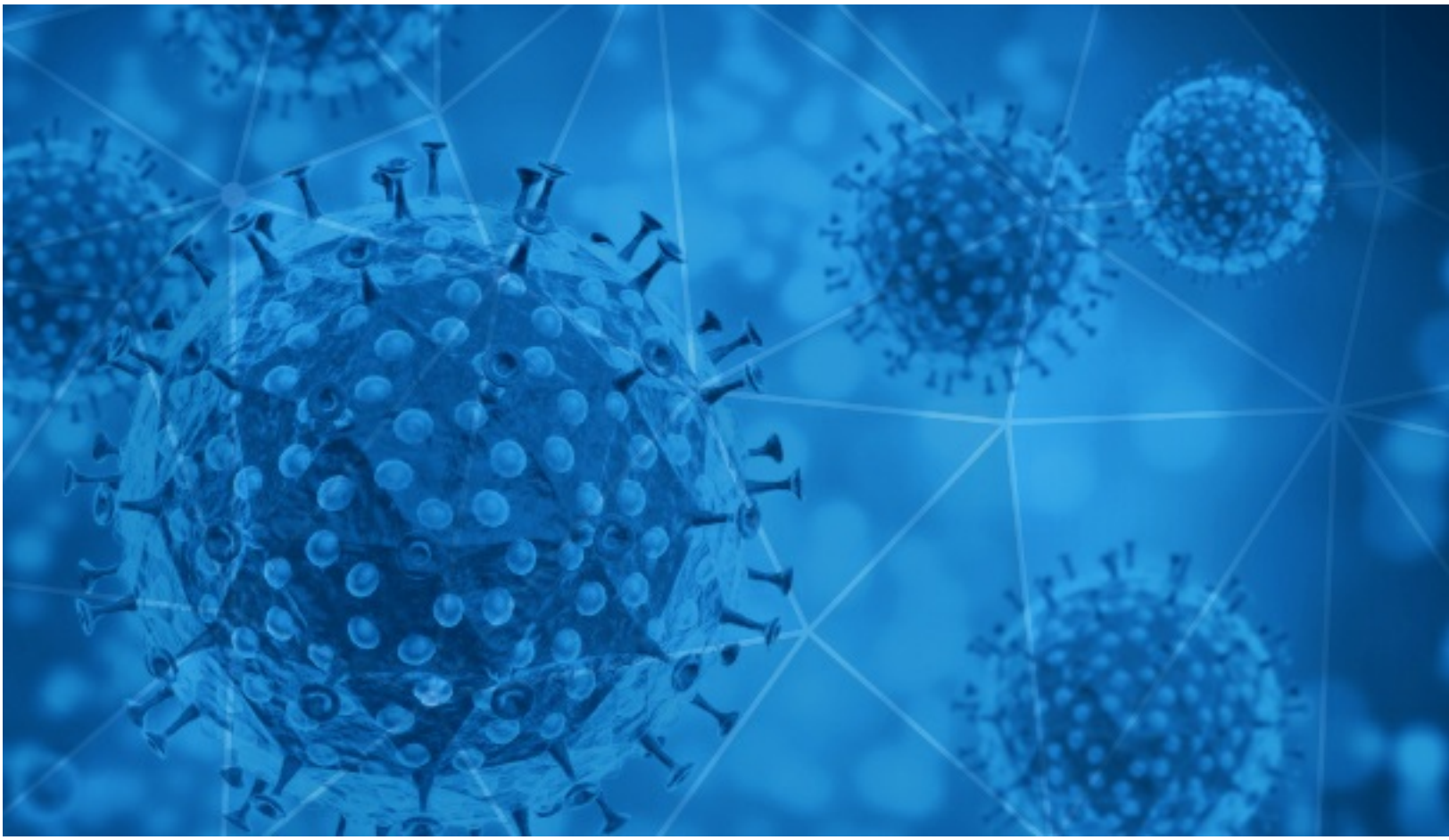
RiskIQ i3:

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

2020-09-17



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 2020-09-16 to 2020-09-17. During this period, RiskIQ analyzed 33,662 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,141 unique subject lines observed during the reporting period. The spam emails originated from 2,178 unique sending email domains and 4,243 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

Wildfires raise COVID-19 risks, Louisville announces Breonna Taylor settlement, and more from Apple News	3870
The Corona Letter: The need for antibody standards	3485
Essential Medical PPE to be Safe From COVID19	1739
Covid-19 Rapid Test Kits	1048
Essential Medical Protective Equipment to Fight Covid19	978
Reife Frauen zu Corona-Zeiten treffen	841
Help to fight COVID-19 fever alarm security door	835
Coronavirus (Covid19) Relief Bailout	799
Insumos protección covid	759
LA SANIFICAZIONE DEGLI AMBIENTI è IL CAPOSALDO CONTRO EMERGENZA COVID19	673
More bad news for Sunshine Patriot Debra Strickland, and her Nye County Commissioners' "Second Amendment Sanctuary" lie. Federal Judge Rules PA Governor's COVID Shutdown Unconstitutional.	582
US/EU AFFORDABLE CERTIFIED COVID19 PPE	459
[Earn Credits] >>> [VIRAL] How to get $4990 a day during the "corona recession"	418
Prevencion de covid19	381
Test Rápido Covid-19 Segunda Generación - 10.000 Un Entrega Inmediata	372
Videos para la prevencion de Covid	369
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	357
<□□> Wildfires raise COVID-19 risks, Louisville announces Breonna Taylor settlement, and more from Apple News	324
Covid-19: Website Design / Website Development Services | SEO (Results Guaranteed) [REDACTED_DOMAIN]	320
Re: Covid-19: Website Design | SEO (Results Guaranteed) [REDACTED_DOMAIN]	272
Covid-19: Website Design Quote | SEO (Results Guaranteed) - [REDACTED_DOMAIN]	249
Bryo Contra Covid19	227
The IRS loophole that will protect your IRA/401(k) from the coronavirus	216
COVID-19 : Redesign Website | SEO (Results Guaranteed) [REDACTED_DOMAIN]	213
Let’s fight together to get through the COVID-19	186

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

insideapple.apple.com	4305
timesofindia.com	3490
medicproduction.com	2198
gmail.com	2047
sinosa.co.za	1048
126.com	997
stargoldmedics.com	978
keyable.net	933
data2web.de	841
cexchange-io-uk.org	799

Top-15 IPs Sending COVID Spam

86.104.194.171	1739
85.204.116.71	978
113.116.205.127	880
46.20.37.30	841
103.20.213.86	799
181.160.214.0	759
201.231.115.70	614
142.202.205.210	589
209.123.15.146	581
65.175.100.77	460

Top-15 Countries Sending COVID Spam

US	10955
IN	6098
CN	3267
RO	3211
DE	2402
GB	1023
AR	970
CA	877
CL	864
KR	639

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

Financial Accounting Impact of COVID-19- An In-depth Look at IFRS	16
COVID-19 Società pubbliche, P.A. e PPP: opportunità partenariato pubblico, industriale e per l'innovazione Roma 14/10/20	4
Re: Fw: Nurse Upskilling Program on Covid19 management: Free of cost and online training.....Please nominate participants	3
Profesjonalny sekretariat w dobie pracy zdalnej / BHP w dobie Covid19	3
COVID-19 Impatto crisi pandemica e L. 40/2020: quali comportamenti e soluzioni gestionali? Milano 28-29/10/20	3
CCS / 10006: Suman 13,680 casos confirmados de COVID-19; fallecimientos 1,298	2
Reporte semanal seguimiento casos COVID 19 ClÃnica de Marly	2
Precizări de presă privind infectarea cu COVID-19 a unei persoane din cadrul Centralei Ministerului Afacerilor Externe	2
NdP.- Cómo reducir la factura de la electricidad de una empresa en tiempos de Covid-19	2
Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020	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: 124,169
Domains with Potential Mail Servers: 2,967
Email-Capable Domains and Hosts: 45,948
Live Hosts and Domains Not Parked: 69,540

Mobile Apps

Apps in Official Stores: 416

by Store

Apple	211
Google	190
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,337

by Store Type:

Hybrid	777
Secondary	505
Affiliate	55

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	25
Hybrid	2
Official	2