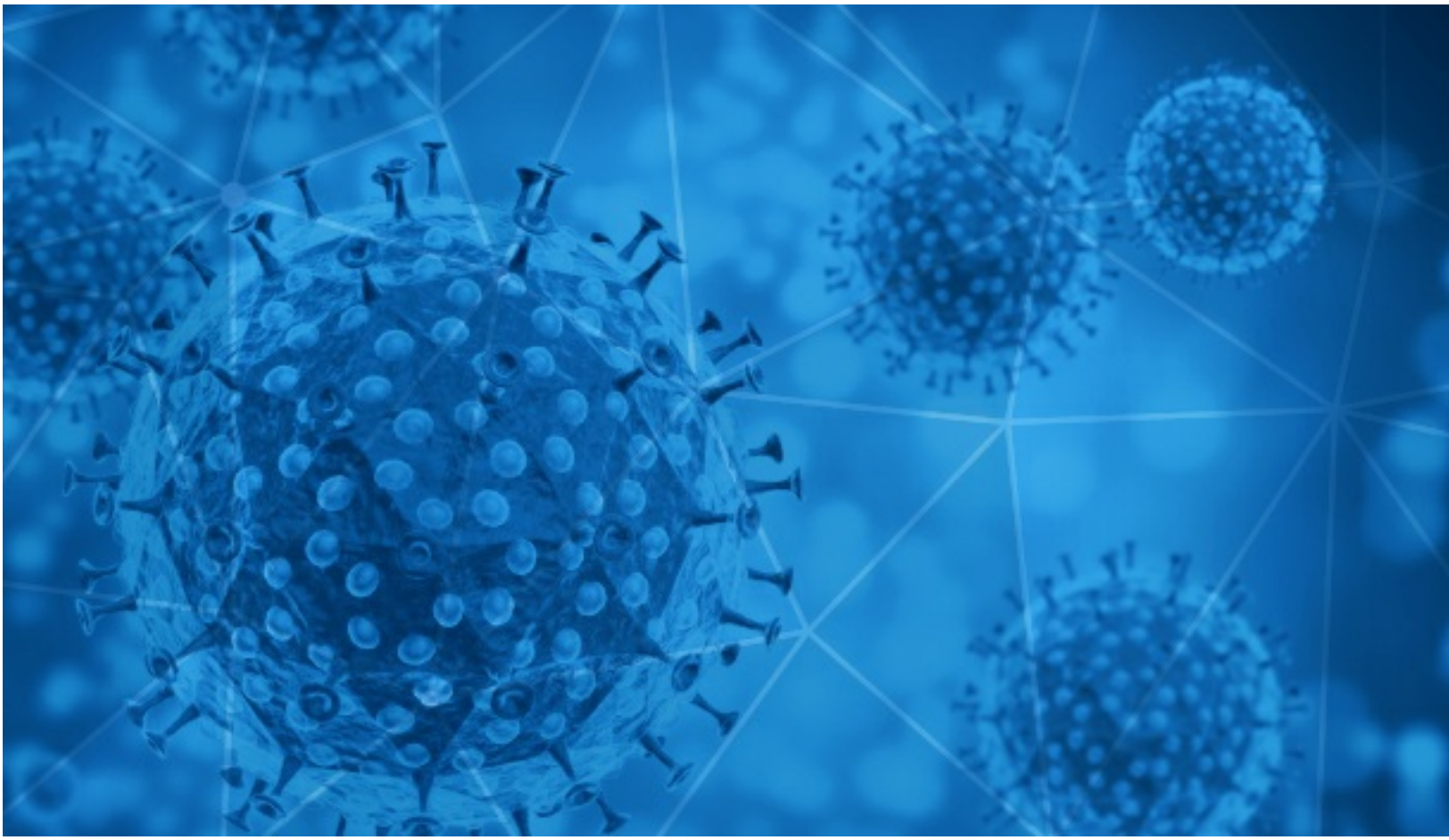
RiskIQ i3:

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

2020-09-18



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 2020-09-17 to 2020-09-18. During this period, RiskIQ analyzed 28,640 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,115 unique subject lines observed during the reporting period. The spam emails originated from 2,020 unique sending email domains and 4,328 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

When a COVID-19 vaccine could be widely available, the wedding linked to 7 coronavirus deaths, and more from Apple News	3934
The Corona Letter: Cloned antibodies raise hopes of a cure	3691
US/EU AFFORDABLE CERTIFIED COVID19 PPE	1584
Covid-19 Rapid Test Kits	1179
Help to fight COVID-19 fever alarm security door	1010
Reife Frauen zu Corona-Zeiten treffen	607
Nuestra respuesta al COVID-19, evitando contagios!	571
Covid-19: Website Design Quote | SEO (Results Guaranteed) - [REDACTED_DOMAIN]	529
Re: Covid-19: Website Design | SEO (Results Guaranteed) [REDACTED_DOMAIN]	464
Prevencion de covid19	438
Videos para la prevencion de Covid	419
Re: COVID-19 : Redesign Website | SEO (Results Guaranteed) [REDACTED_DOMAIN]	382
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	330
Test de deteccion rapida COVID19	281
Test sierologici per COVID-19: finalmente disponibili anche per le IMPRESE.	269
Dear award recipient, COVID -19 Compensation funds.	252
Let’s fight together to get through the COVID-19	204
Today's offer! 60% off on COVID antibody IgG + IgM test. Book your Appointment	200
Laat COVID-19 uw zorg niet beinvloeden!	198
Your Covid Antibody IgG + IgM test report can be generated at Rs.750 only | Book your timing Slot.	179
COVID-19 Relief Fund, Please Send all Replies to sv277@aol.com4	175
Re: Covid-19 acrylic protect shield	171
Re: keep away from Covid-19	130
$800,000.00 Usd Covid-19 Relief Funds	124
Re:Against Covid-19, Direct factory Skymed,V Gloves, Superior ,SUPERLEUR GB, Kichyglove brand NITRILE GLOVES	122

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	3934
timesofindia.com	3691
gmail.com	1843
medicproduction.com	1584
sinosa.co.za	1179
countermail.com	1138
keyable.net	1010
yeah.net	830
126.com	745
data2web.de	607

Top-15 IPs Sending COVID Spam

85.204.116.74	1584
113.116.205.216	974
46.20.37.30	606
201.231.5.220	529
142.202.205.210	449
157.119.122.97	360
190.247.241.202	340
157.119.122.39	302
157.119.122.136	291
190.247.241.106	269

Top-15 Countries Sending COVID Spam

US	8943
IN	6106
CN	3314
RO	1595
AR	1179
DE	1173
GB	960
CA	830
PL	678
FR	572

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

17-09-20 - Informations DRH MI - Gestion des cas COVID et des cas contacts	1

Top-15 Subjects Containing doc/xlsx Files

Profesjonalny sekretariat w dobie pracy zdalnej / BHP w dobie Covid19	12
Prawo pracy po zmianach - najnowsze przepisy a COVID 19	9
Dokumentacja pracownicza w dobie COVID 19 - szkolenie on-line	8
COVID-19 Green economy e fonti rinnovabili: fattibilità, ecobonus, e cessione credito Roma 22/10/20	6
Emergenza COVID-19 Focus OIC: novità contabili e fiscali, adempimenti, soluzioni e rinvii Milano 20/10/20	5
Precizări de presă privind actualizarea listei „zonelor de risc“ stabilită de autoritățile germane în contextul pandemiei de COVID-19	4
covid 19 compensation	4
Test COVID-19: todo lo que la población quiere saber sobre el diagnóstico en la nueva campaña del Consejo General de Enfermería	4
Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020	4
Deltio Typou - Apallagi apo Dimotika Teli Covid 19	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: 125,846
Domains with Potential Mail Servers: 2,964
Email-Capable Domains and Hosts: 47,546
Live Hosts and Domains Not Parked: 69,433

Mobile Apps

Apps in Official Stores: 418

by Store

Apple	211
Google	192
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,347

by Store Type:

Hybrid	783
Secondary	509
Affiliate	55

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	25
Hybrid	2
Official	2