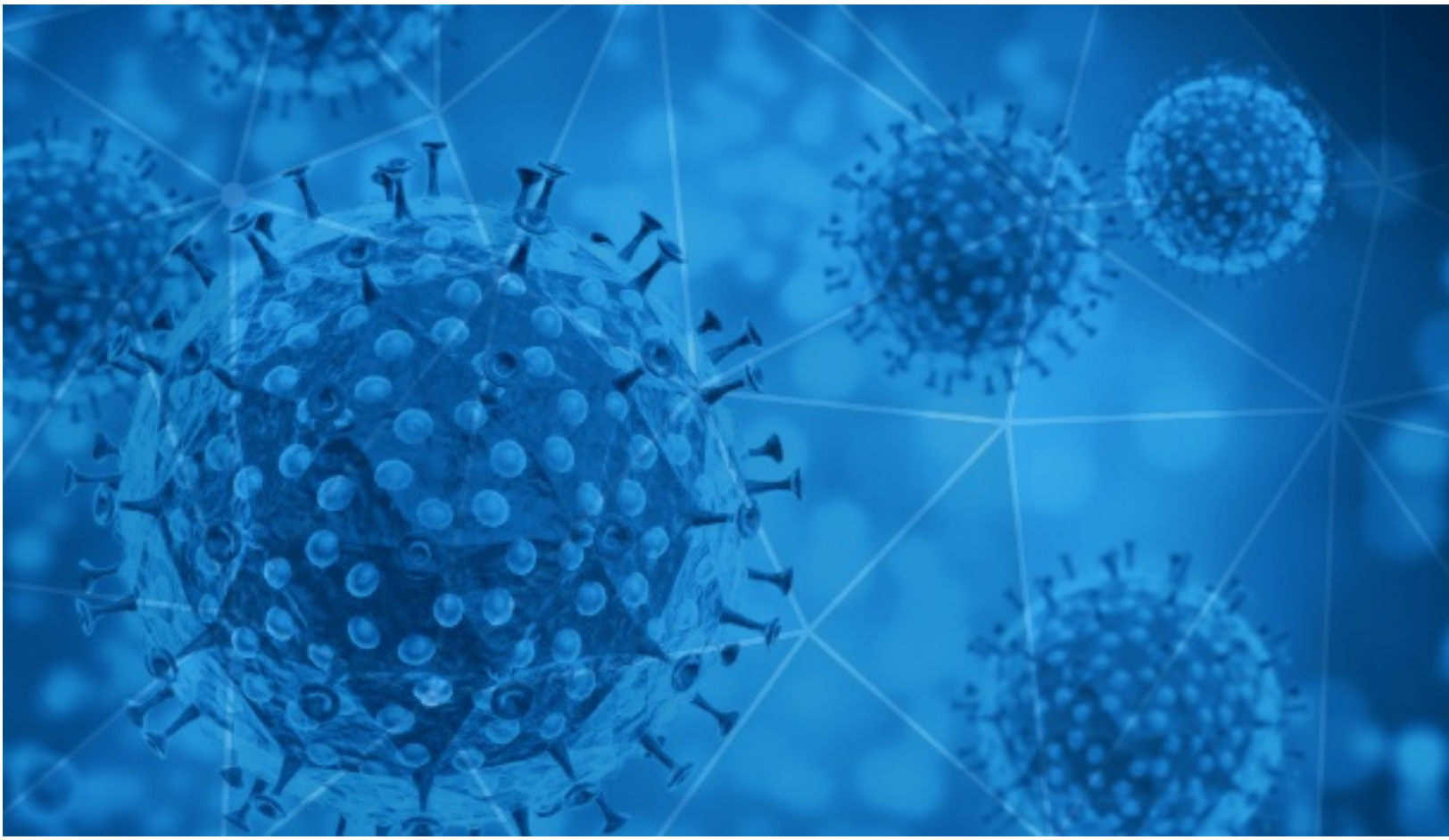
RiskIQ i3:

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

2020-11-10



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 2020-11-09 to 2020-11-10. During this period, RiskIQ analyzed 41,645 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 6,239 unique subject lines observed during the reporting period. The spam emails originated from 2,362 unique sending email domains and 4,914 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	13221
The Corona Letter: A cytokine storm in a teacup?	3757
Cambios en ICO Covid	1169
Taller: Jornadas de Trabajo, su Implementación Práctica y Normas Especiales Covid 19	569
SPENDE FÜR WEIHNACHTEN UND UNTERSTÜTZUNG FÜR COVID 19	533
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	521
COVID-19, puoi venire in Filiale solo su appuntamento	479
Post Covid 19 Project/Business Loan Offer	465
Coronavirus 'Stay home - earning big money home'	385
Atencion covid Estudio Contable Legal e Impositivo para tu negocio	371
UNITED NATIONS COMPENSATION&COVID19 ASSISTED	360
Google Alert - "You need this right nowfor fight Covid and Fun"	338
Covid-19 Impacts Babies with Birth Defects!	321
Congratulation!!! You have been awarded United Nations Covid-19 funds	297
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	295
Recruitment at Coronation Group, Timekeepers, Premiere Urgence, Willers Solutions, Greenlight Planet	290
Contactless infrared body temperature thermometer defeat Coronavirus	230
Help to fight COVID-19 fever alarm security door	229
Re: Defeat Coronavirus, non contact fever alarm device	227
Let’s fight together to get through the COVID-19	220
Re: Re: Covid-19 acrylic shield(Support OEM)	176
Re: Covid-19 Protective acrylic sneeze guards(1/5 lower than your purchase price)	162
Good morning, SA | Fears of second Covid-19 wave a MAC goes to ground, Trump forges ahead with legal plan to overturn election	149
Re: Hand wash with 75% alcohol, keep away from Covid-19	137
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)..	137

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	13225
timesofindia.com	3757
service.alibaba.com	1697
gmail.com	1488
yeah.net	881
ediscomspa.com	852
126.com	806
sabaziusii.com	771
outlook.com	710
keyable.net	686

Top-15 IPs Sending COVID Spam

113.89.40.36	686
103.124.94.147	569
200.17.137.44	533
181.46.136.168	521
89.32.41.211	507
103.225.52.205	446
103.225.55.225	388
103.225.52.67	377
103.225.53.139	368
113.116.194.95	365

Top-15 Countries Sending COVID Spam

JP	13298
US	6498
CN	5482
IN	4538
ES	1825
AR	1015
IT	960
FR	956
--	910
DE	660

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

COVID 19 WEB DIRETTA STREAMING LICEITA' Licenziamento DIRIGENTE: quali scelte e strategie aziendali? Analisi e soluzioni 18/11/2	22
PROROGA COVID19 DPCM 5/11/20 WEB DIRETTA STREAMING Gestione lavoro, CIGO-CIGD-FIS, protocolli sicurezza, responsabilità 24/11/20	16
Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	11
OFFERTA ANTICOVID,ATTREZZATURE E MACCHINE PER PULIZIA	2
Биотек - Барање за р��зервација на COVID 19	2
"El Coronavirus resultó más efectivo que cualquier plan para avanzar en la Inclusión Financiera" [Nota de Prensa Ar/Análisis Económico]	2
CCS/10564: Suman 29,735 casos confirmados por COVID-19 y 2,393 fallecimientos	2
COVID update, 11/09/2020	2
BDH Surveillance for Covid- 19 08 November 2020_1_1_4.xlsx	1
Fwd: CV 367 Vv hướng dẫn cài đặt và sử dụng hệ thống hỗ trợ phòng, chống dịch bệnh 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: 132,113
Domains with Potential Mail Servers: 2,656
Email-Capable Domains and Hosts: 50,299
Live Hosts and Domains Not Parked: 46,070

Mobile Apps

Apps in Official Stores: 469

by Store

Apple	237
Google	217
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,718

by Store Type:

Hybrid	901
Secondary	758
Affiliate	59

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1