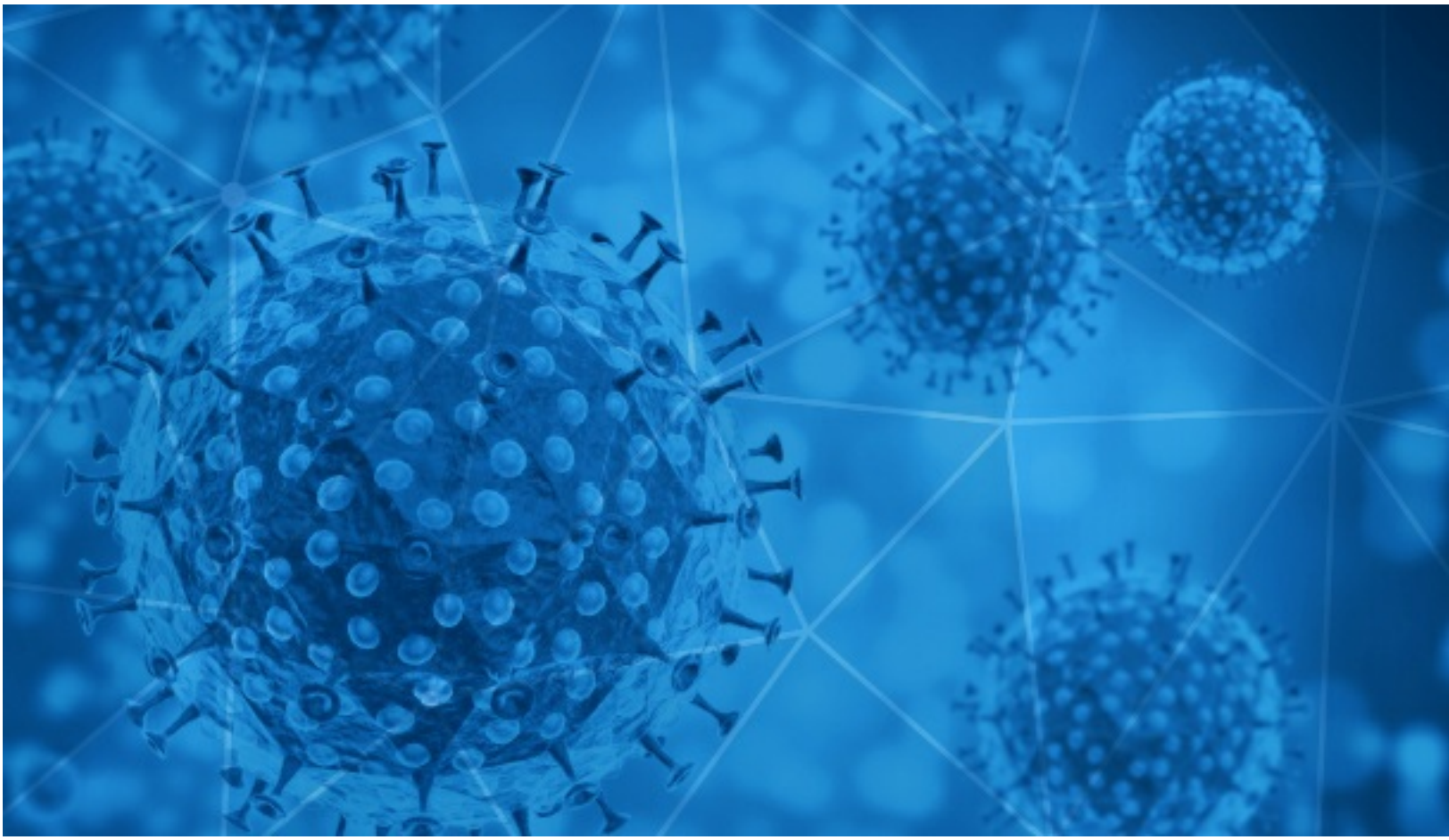
RiskIQ i3:

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

2020-10-23



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 2020-10-22 to 2020-10-23. During this period, RiskIQ analyzed 41,168 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,412 unique subject lines observed during the reporting period. The spam emails originated from 2,090 unique sending email domains and 4,110 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	11634
The Corona Letter: An Oxford scare and a mask reassurance	3578
Evite el coronavirus en su negocio	2178
Corona virus (Covid19) Bailout Fund	918
COVID-19 Asesoramiento contable para tu empresa	814
ATENCION COVID-19 Estudio Contable, Legal e Impositivo para tu negocio	804
Limpieza y desinfeccion COVID 19	748
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	645
UN. CORONA-VIRUS RELIEF FUND {1.202.156.29	549
COVID 19 community Dialogue Initiative 2020	534
The hottest post-coronavirus opportunityâ¦	483
Covid-19 Compensation Relief Funds of $850,000.00 USD :	452
Lampy sterylizujace UV-C jako dobry sposób walki z koronawirusem (covid-19)	372
Save your family! Covid19 initiative	341
0ferta test rápidos COVID 19	308
mi seguro insumos covid 19 protege a tu familia	287
Salve sua família! Iniciativa Covid19	253
Productos Prevención Covid en Oferta!	251
Help to fight COVID-19 fever alarm security door	248
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	231
Contactless infrared body temperature thermometer defeat Coronavirus	226
Let’s fight together to get through the COVID-19	220
(OECD)Support During COVID-19 Fund Approved	209
Re: Defeat Coronavirus, non contact fever alarm device	200
KEEP SCHOOLS OPEN SAFELY...COVID OR NOT!	194

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	11636
tutanota.com	4841
timesofindia.com	3585
gmail.com	2490
outlook.com	1079
bknegaraindonesia.com	922
yeah.net	687
keyable.net	674
126.com	476
promieniowanieuvc.pl	372

Top-15 IPs Sending COVID Spam

201.231.8.157	2459
168.227.76.6	922
201.231.6.185	771
181.46.136.168	645
113.116.204.26	636
201.231.83.246	618
201.231.10.127	554
1.202.156.4	549
45.143.223.147	534
190.119.171.165	452

Top-15 Countries Sending COVID Spam

JP	11748
US	5660
AR	5550
IN	4014
CN	3267
FR	1294
BR	992
IT	929
--	893
GB	867

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

Dwudniowy kurs Kadry i płace w dobie COVID 19 - szkolenie on-line	9
Coronavirus e smart working. La proposta di Fp Cgil: “Limitare il contagio attraverso il lavoro agile”	4
Coronavirus - SERVIZIO DI ACQUISTO MASCHERINE FFP2 - GUANTI IN LATTICE MONOUSO	4
Salute: Covid, da ENEA un dispositivo per test rapidi sul respiro (ENEAinform@ 22 ottobre 2020)	3
Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020	3
IL PRESIDENTE ACQUAROLI FIRMA NUOVA ORDINANZA ANTI-COVID: TRASPORTI, SCUOLA, CENTRI COMMERCIALI, MOVIDA	3
CURSO: PREVENCION MITOS Y REALIDADES SOBRE EL CORONAVIRUS. BIENESTAR Y RISILIENCIA EN LA FAMILIA Y EL TRABAJO EN EL CONTEXTO DE EPIDEMIA Y PANDEMIA	3
HOY, A LAS 11, Convocatoria de prensa: ¿Están dispuestas las enfermeras a vacunarse masivamente contra la gripe para hacer frente a la pandemia?, ¿cuál es su percepción de la vacuna del COVID-19?	3
COVID-19 WEBINAR DIRETTA STREAMING Gestione impresa tra adeguati assetti e MOG 231/01: obbligatorietà 2/12/20	3
ENIT ANNUNCIA IL MONITORAGGIO IN TEMPO REALE DALLE 28 SEDI ESTERE - ITALIA RESISTE NONOSTANTE IL COVID ED E' DI ESEMPIO IN EUROPA	3

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: 130,142
Domains with Potential Mail Servers: 2,723
Email-Capable Domains and Hosts: 49,192
Live Hosts and Domains Not Parked: 46,773

Mobile Apps

Apps in Official Stores: 462

by Store

Apple	235
Google	212
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,628

by Store Type:

Hybrid	865
Secondary	706
Affiliate	57

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1