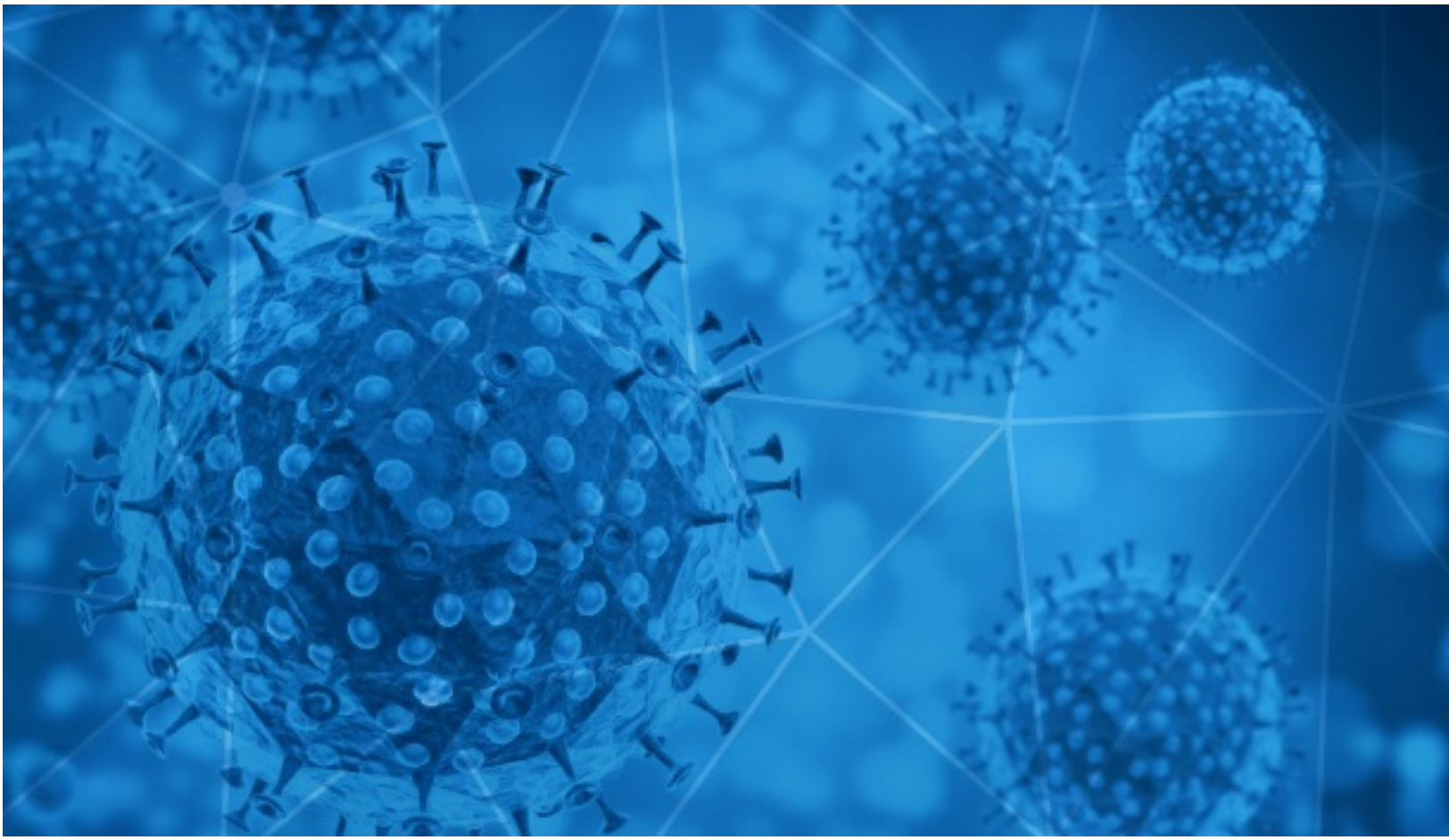
RiskIQ i3:

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

2020-09-03



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 2020-09-02 to 2020-09-03. During this period, RiskIQ analyzed 36,718 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,699 unique subject lines observed during the reporting period. The spam emails originated from 1,623 unique sending email domains and 3,735 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

COVID-19 Essential Medical Protectives	3635
COVID19 ESSENTIAL SAFETY PPE's	2537
COVID19 ESSENTIAL SAFETY PPE	2333
The Corona Letter: Of primate concern	1641
Essential Medical Protectives - COVID19	1633
Desinfectamos su ambiente de coronavirus	1280
Safety Essential PPE - Covid19	1265
Desinfeccion Preventiva Covid19	1262
Desinfeccion covid19 mediante termoniebla	1238
Invitation for "Covid-19 Awareness Social Contact" Programme 2020	679
TermoScanner Anti-Covid. Sconti fino al 50 % e pronta consegna. Non abbassiamo la guardia!!!	609
Precios Imbatibles / Productos COVID 19	596
ATALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID -19	540
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	538
Evite contagios, no al Covid19, Accese, Asistencia biométricos	534
COVID-19 Pandemic - Most valuable financial lessons learnt	523
Cuidate del COVID19 con nuestros productos	487
Reife Frauen zu Corona-Zeiten treffen	404
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	400
Totem Covid-19 Test Rápido, Mascarillas, Guantes e Insumos	337
Re: Defeat Coronavirus, non contact fever alarm device	314
Your Covid Antibody IgG + IgM test report can be generated at Rs.750 only | Book your timing Slot.	303
Precios Rebajados COVID-19	286
Contactless infrared body temperature thermometer defeat Coronavirus	269
Bryo Contra Covid19	267

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

medicproduction.com	6135
stargoldmedics.com	5268
countermail.com	4267
126.com	2197
timesofindia.com	1641
gmail.com	1548
bcrec.ac.in	679
livejob.info	622
keyable.net	583
sopytecchile.com	534

Top-15 IPs Sending COVID Spam

139.99.133.125	5231
86.104.194.171	3635
190.247.240.6	3527
86.104.194.169	2537
151.22.250.164	622
113.116.205.19	536
46.101.218.158	534
201.231.19.33	513
46.20.37.30	403
181.46.136.168	400

Top-15 Countries Sending COVID Spam

RO	6196
US	5986
AU	5268
AR	4743
CN	3396
IN	2337
DE	1651
IT	1048
CL	805
FR	588

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

TR: Circ. n° 189-2020 - Mise à jour du protocole national pour assurer la santé et la sécurité des salariés en entreprise face à l'épidémie de covid-19	1

Top-15 Subjects Containing doc/xlsx Files

Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020	13
BHP w dobie Covid19 /ZFŚS/ Profesjonalny sekretariat w dobie pracy zdalnej	9
Unimore e BPER Banca insieme per un progetto di ricerca sul COVID-19	9
Emergenza COVID-19 Partecipate Pubbliche, P.A. e PPP: partenariato pubblico, industriale e per l'innovazione Roma 14/10/2020	6
TEUTEUGA O LE POLOAIGA COVID19 02 SETEMA 2020	6
Bezpieczne Dziecko 2020/2021 - NNW (w tym COVID-19) + OC bez konieczności zawierania polisy!	4
TR: * SPAM *** tr: COVID 19: MESURES DE PREVENTION EN ENTREPRISE & PROTOCOLE A TENIR PAR LES EMPLOYEURS. (VOIR FICHIERS & LIENS CI-DESSOUS)**	2
FW: Update on COVID-19 Practices	2
INFORMATION COVID MDCVA	2
STARTS IN 15 MINUTES - ECSA-HC WEBINAR: Disease surveillance in the COVID-19 Pandemic	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: 121,870
Domains with Potential Mail Servers: 2,948
Email-Capable Domains and Hosts: 45,366
Live Hosts and Domains Not Parked: 66,666

Mobile Apps

Apps in Official Stores: 410

by Store

Apple	212
Google	183
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,268

by Store Type:

Hybrid	734
Secondary	482
Affiliate	52

Blacklisted Mobile Apps: 27

by Store Type:

Secondary	24
Official	2
Hybrid	1