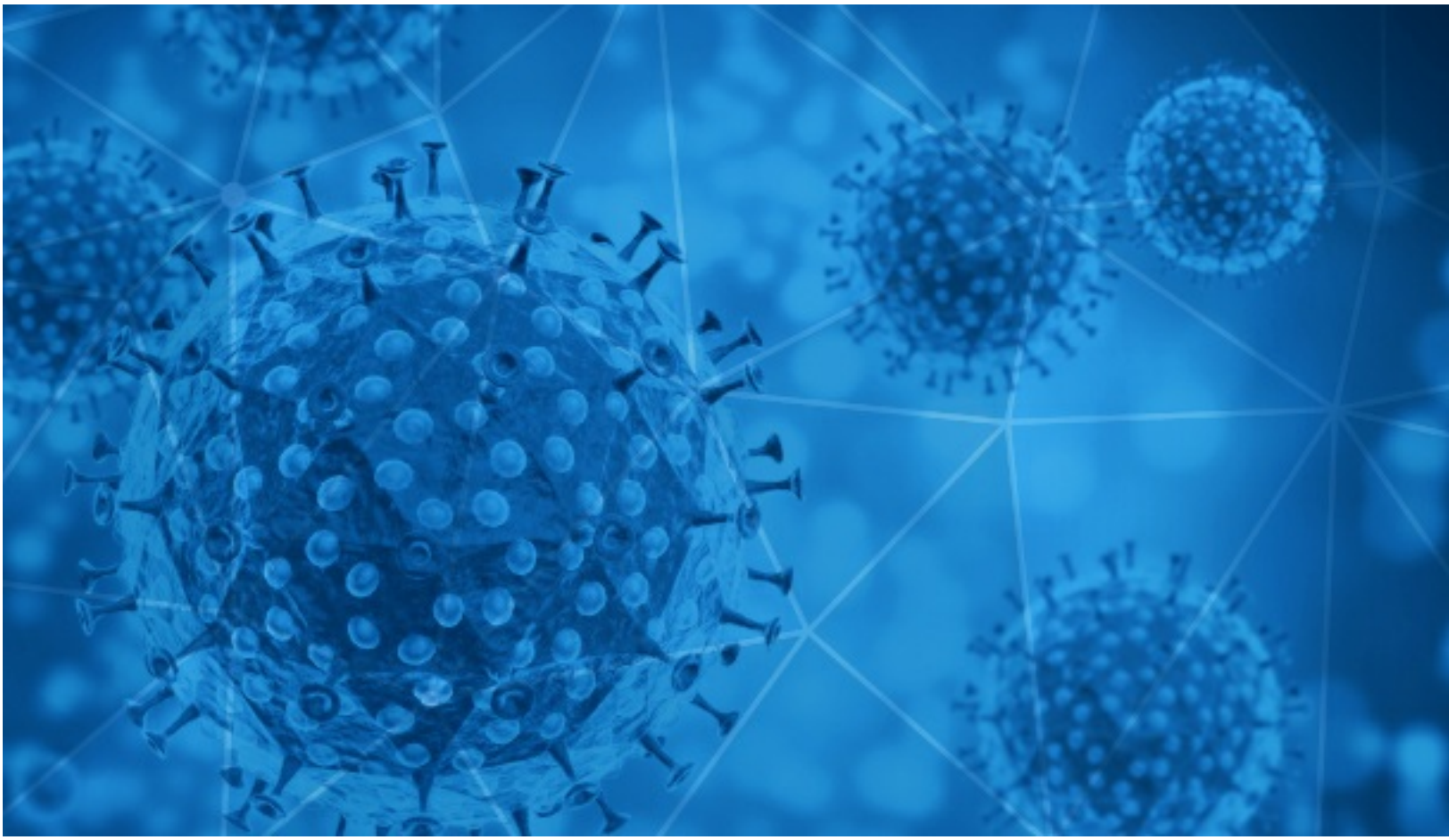
RiskIQ i3:

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

2020-09-09



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 2020-09-08 to 2020-09-09. During this period, RiskIQ analyzed 21,940 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,121 unique subject lines observed during the reporting period. The spam emails originated from 1,487 unique sending email domains and 3,081 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: How India slipped	2633
¡Protege a tus trabajadores, Productos COVID-19!	1176
COVID-19 LATEST NEWS	841
Essential Medical Protective Equipment - Covid	715
Aprovecha productos de protección Covid en Oferta!!!	524
Tokyo Olympics Set to Commence July 23rd Regardless of the Coronavirus - Sankaku News	486
Protejase del Covid…	468
Post COVID-19 Plans..	451
Your Relief For Coronavirus (Covid19).	436
Productos Covid-19	382
Cuidate del COVID19 con nuestros productos	354
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	346
Precios Imbatibles / Productos COVID 19	340
covid-19 and children - how does it affect them?	313
Contactless infrared body temperature thermometer defeat Coronavirus	280
Covid-19: Quality IT Projects | SEO (Results Guaranteed) [REDACTED_DOMAIN]	272
Re: Defeat Coronavirus, non contact fever alarm device	261
Reife Frauen zu Corona-Zeiten treffen	237
Instalación Medidas de Prevención Covid-19 - OFERTA LIMITADA	235
Evite contagios, no al Covid19, Accese, Asistencia biométricos	220
Join the Bowser Administration for a Community Leader Telephone Townhall on Coronavirus	217
Precios Rebajados Covid-19	211
E' arrivata la guida per gli hotel al tempo del covid 19: migliora la tua ospitalità. Scaricala ora, è gratis.	165
Desinfecciones profesionales Covid - 19	158
Re: Covid-19 acrylic protect shield	156

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gmail.com	2740
timesofindia.com	2633
126.com	1275
brandmed.cl	1176
outlook.com	824
stargoldmedics.com	715
trendingtopic.cl	573
keyable.net	541
sankakucomplex.com	486
countermail.com	354

Top-15 IPs Sending COVID Spam

223.38.30.100	841
51.83.130.184	715
5.56.22.142	618
5.56.22.141	575
113.116.207.88	487
208.100.24.254	486
193.142.59.134	451
177.136.47.226	446
181.46.136.168	346
116.197.158.125	313

Top-15 Countries Sending COVID Spam

US	4369
IN	3157
DE	2492
CN	2351
FR	1952
KR	950
--	848
AR	749
CL	669
BR	661

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	11
Perftoran - laboratorij za razvoj cepiva za COVID-19 v Fotopubovem projektnem prostoru	7
PHHS 9 8 2020 End of Day COVID 19 Summary	6
Emergenza COVID-19 GREEN ECONOMY: fattibilità intervento, ecobonus 110% e cessione del credito Roma 22/10/20	5
Fwd: Achats subventionnés de Noix de Cajou - Soutien à la filière Anacarde COVID-19 – Protocoles d'accord post 20 août 2020	3
Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020	2
CONSEJERÍA DE EDUCACIÓN Y JUVENTUD. CURSO COORDINADORES COVID	2
NdP - ¿Cómo superar el síndrome postvacacional en plena segunda ola del COVID?	2
NON COVID: Priority: SAPR command compliances and processes	1
COVID 19 Line List	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: 123,465
Domains with Potential Mail Servers: 2,966
Email-Capable Domains and Hosts: 45,813
Live Hosts and Domains Not Parked: 68,605

Mobile Apps

Apps in Official Stores: 411

by Store

Apple	212
Google	184
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,297

by Store Type:

Hybrid	754
Secondary	490
Affiliate	53

Blacklisted Mobile Apps: 29

by Store Type:

Secondary	25
Hybrid	2
Official	2