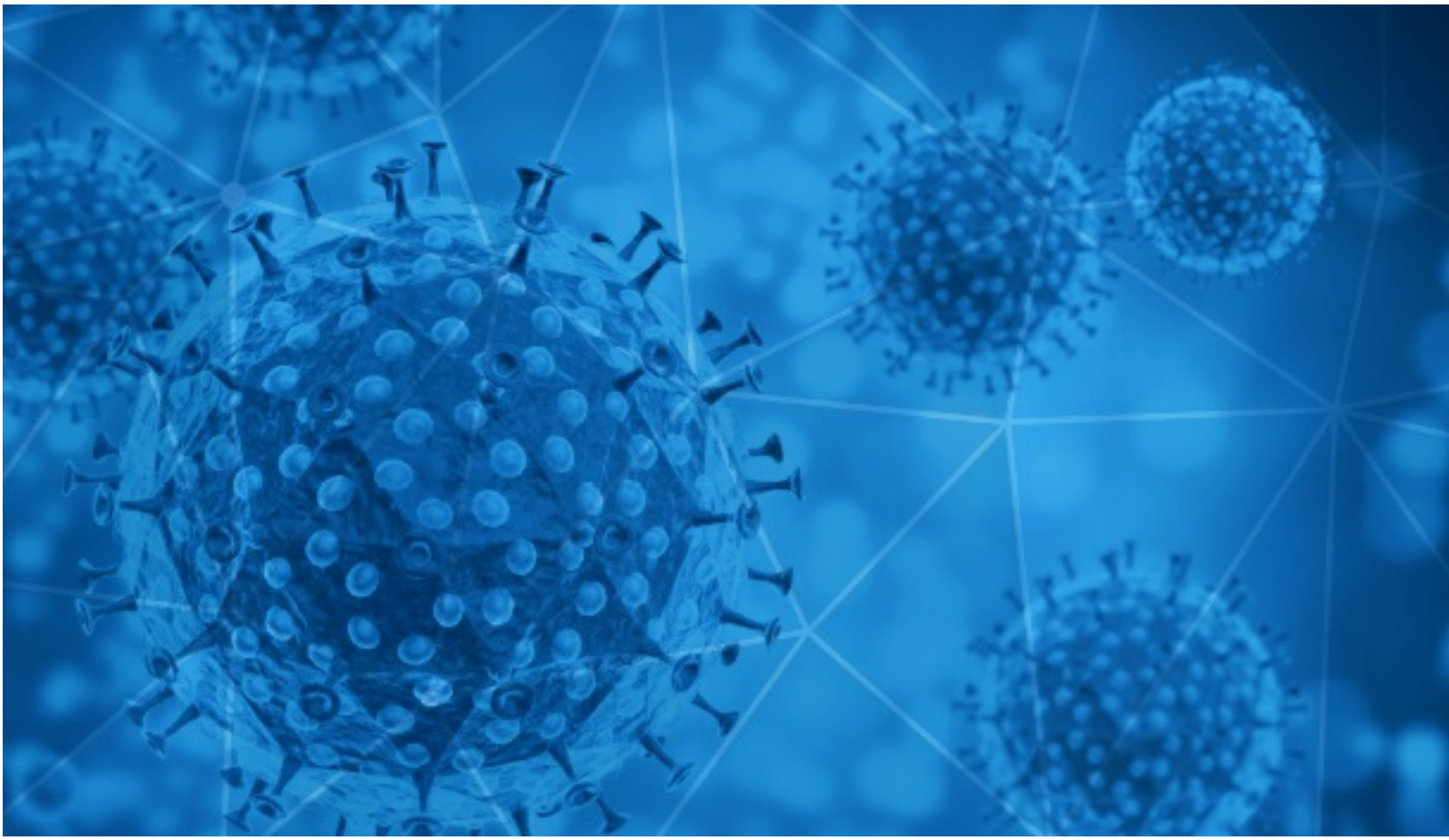
RiskIQ i3:

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

2020-09-02



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 2020-09-01 to 2020-09-02. During this period, RiskIQ analyzed 26,464 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,694 unique subject lines observed during the reporting period. The spam emails originated from 1,927 unique sending email domains and 3,816 unique SMTP IP Addresses. Analysts identified 2 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: Why India is not a WFH country	2121
Evite contagios, no al Covid19, Accese, Asistencia biométricos	1560
Essential Safety PPE For Covid19	718
Precios Imbatibles / Productos COVID 19	714
Reife Frauen zu Corona-Zeiten treffen	644
Cuidate del COVID19 con nuestros productos	642
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	524
Re; Covid 19 Loan Relief	488
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	481
Post COVID-19.	456
Your COVID-19 Registration	444
AuraAir: Único Filtro que Elimina el Covid-19 llegó a Chile	417
Desinfectamos su ambiente de coronavirus	378
COVID19 ESSENTIAL SAFETY PPE's	374
Contactless infrared body temperature thermometer defeat Coronavirus	351
Re: Defeat Coronavirus, non contact fever alarm device	343
Desinfeccion Preventiva Covid19	342
Desinfeccion covid19 mediante termoniebla	341
¡Oferta Imperdible! Test Rápidos Covid-19	323
Totem Covid-19 Test Rápido, Mascarillas, Guantes e Insumos	322
Re: Protectores faciales anti COVID 19 de excelente calidad y precio	304
Equipos de protección COVID 19	298
Join the Bowser Administration for a Community Leader Telephone Townhall on Coronavirus	290
Uniti combatteremo la crisi COVID-19	285
covid-19 and children - how does it affect them?	276

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	2499
timesofindia.com	2121
126.com	1973
countermail.com	1703
sopytecchile.com	1560
medicproduction.com	1122
keyable.net	694
data2web.de	644
dhs.wisconsin.gov	448
hotmail.com	393

Top-15 IPs Sending COVID Spam

46.101.218.158	1560
86.104.194.169	1092
190.247.226.144	761
113.116.205.53	661
46.20.37.30	644
103.109.37.55	549
211.241.209.104	488
181.46.136.168	481
201.231.58.10	447
119.122.91.122	362

Top-15 Countries Sending COVID Spam

US	5290
CN	3413
DE	3158
IN	2832
AR	2340
RO	1165
VN	837
CL	799
FR	797
KR	618

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

COVID-19 knocks spending by overseas visitors and students – Stats NZ Media and Information Release: International trade: June 2020 quarter	1
Dexellence Clinic - Chestionar COVID19 (Petre Sofia Andreea)	1

Top-15 Subjects Containing doc/xlsx Files

Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020	45
RV: CUMPLIMIENTO DE PROTOCOLOS DE BIOSEGURIDAD PARA MANEJO DE PANDEMIA CORONAVIRUS - COVID19	7
Fwd: Kính gửi CV244 v/v Hướng dẫn khai báo Y tế phòng, chống dịch bệnh Covid-19	3
Important Announcement | Federal Bank & Innoviti tie-up to extend affordability in times of COVID crisis through Debit Card EMI	3
CCS /9852 (Con corrección en el total de casos a nivel estatal) Rebasa la capital los 3 mil contagios de COVID-19; suman 11 mil 810 en el estado	2
NP- Minsa pone en marcha dos Centros de Atención y Aislamiento Temporal COVID-19 en Amazonas	2
CCS/9855 Concluye transmisiones programa SaludableMente de acompañamiento psicosocial ante el COVID-19	2
CCS /9852 Rebasa la capital los 3 mil contagios de COVID-19; suman 11 mil 819 en el estado	2
Notificación Casos Covid CIUDAD REAL	2
Южная Корея: крупномасштабное пожертвование плазмы крови способствует разработке лекарства от COVID-19. Пресс-релиз, фото, видео.	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: 121,708
Domains with Potential Mail Servers: 2,955
Email-Capable Domains and Hosts: 45,316
Live Hosts and Domains Not Parked: 66,811

Mobile Apps

Apps in Official Stores: 410

by Store

Apple	212
Google	183
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,262

by Store Type:

Hybrid	731
Secondary	479
Affiliate	52

Blacklisted Mobile Apps: 27

by Store Type:

Secondary	24
Official	2
Hybrid	1