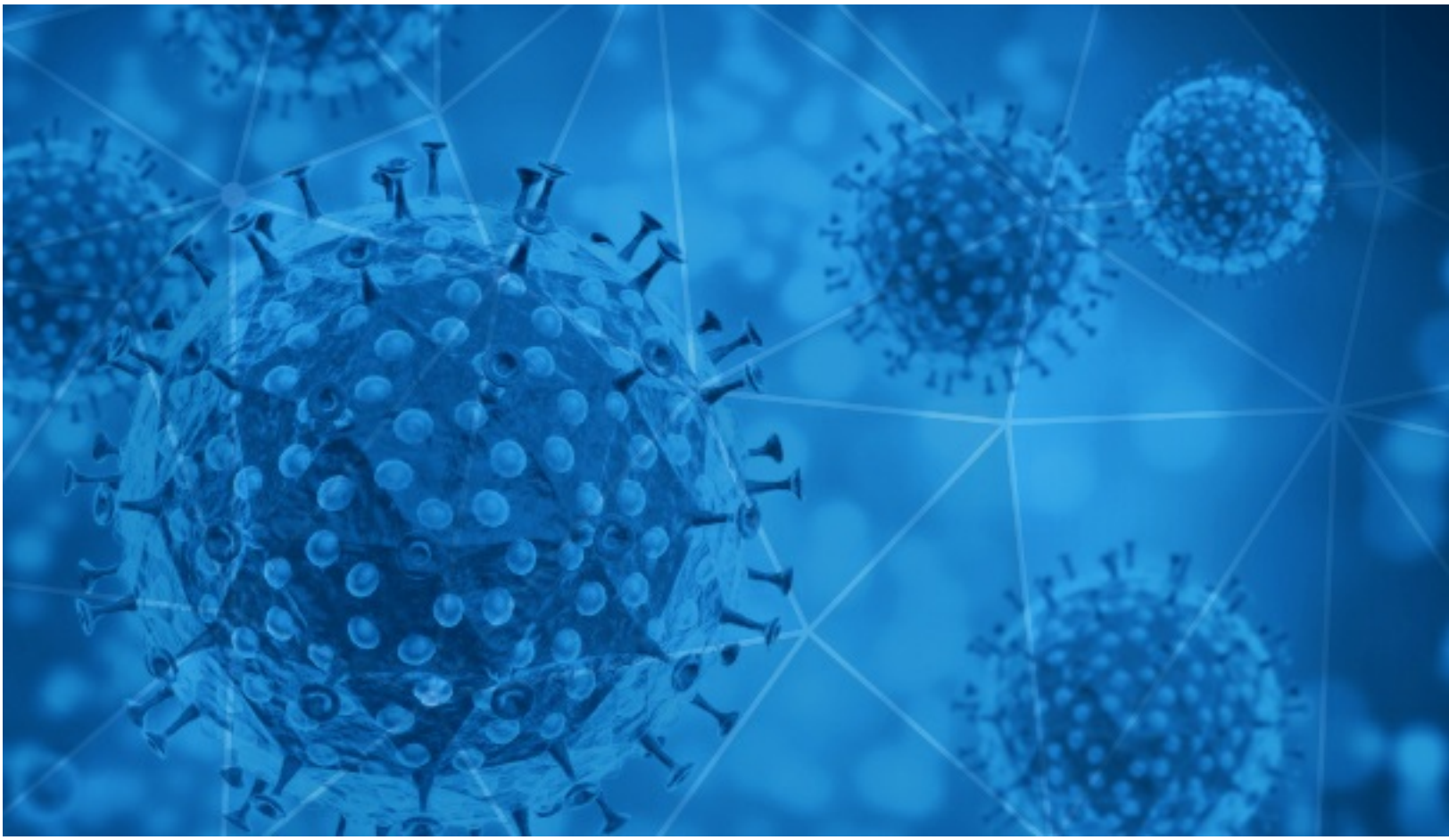
RiskIQ i3:

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

2020-06-05



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 2020-06-04 to 2020-06-05. During this period, RiskIQ analyzed 60,880 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 5,046 unique subject lines observed during the reporting period. The spam emails originated from 4,063 unique sending email domains and 6,934 unique SMTP IP Addresses. Analysts identified 34 emails which sent an executable file for Windows machines.

Top-25 Subjects

BANNED GOODS DUE TO COVID 19 PANDEMIC	16683
Covid19- Fund Compensation Notice./Paying Center	3057
The Corona Letter: When medical research is prime time news	2786
Paneles anti Covid-19 para atención de Público.	2039
Products for COVID-19	1616
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	1301
Insumos Protectores Covid-19 Despachos a Todo Chile	1230
Deadline for UNICEF Covid-19 Innovation Challenge 2020 + 3 new USA Scholarships	1085
Free LinkedIn Premium for Caregivers and Veterans, Select Benefits Exams Resuming, COVID-19 VA Patient Dashboard	727
REPORT WITH REGARDS TO COVID-19 FOR ALL INDIAN PORTS	709
Cursos En Linea - Sobre Proteccion al Empleo Modificaciones a la Ley Covid19	694
Front Sight's Response to Nevada's Current COVID-19 Restrictions…	637
Korea Trend News-COVID19-2	568
Persuasive Selling during Covid 19	526
Top tech trends that COVID-19 pandemic will accelerate	380
Seminario: Nuevas Medidas Tributarias en Tiempos de COVID-19	353
Mamparas de proteccion contra el coronavirus	342
Mamparas de proteccion COVID19	342
Como Implementar un Ecommerce en Tiempos de covid-19 retos y oportunidades	341
Maquina para Desinfecciones COVID por Termonebulización en $120	323
ATALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ TRÙNG COVID -19	309
Covid-19 Compensation Relief Funds :	303
FBI: Aid To Navigate CORONAVIRUS Challenges!	294
Test Rapido Covid-19	293
Protege tu espacio del covid-19	292

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

gov.org	16683
gmail.com	5976
timesofindia.com	2786
publica20.club	2039
126.com	2024
medicproduction.com	1620
frontsight.com	1613
163.com	1529
insumosprotectorescovid19.com	1230
myschool.com.ng	1085

Top-15 IPs Sending COVID Spam

133.167.123.176	16653
91.212.153.94	3057
160.20.147.106	2039
209.123.15.146	1611
167.99.191.76	1230
184.107.73.137	1085
209.58.149.66	908
119.122.90.13	762
88.218.16.73	709
95.211.208.25	707

Top-15 Countries Sending COVID Spam

JP	16888
US	11787
--	5792
CN	5415
IN	3800
CA	2885
DE	2010
ES	1252
FR	1141
NL	1061

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 TESTING KIT	26
FW: Tender Kampong Bahru - Invitation to quote pharmaceutical and medical equipment for the treatment of COVID-19	5
Fwd: Tender Kampong Bahru - Invitation to quote pharmaceutical and medical equipment for the treatment of COVID-19	1

Top-15 Subjects Containing doc/xlsx Files

BHP – obowiązki pracodawcy i pracownika w dobie Covid 19	7
Бесконтактная антивирусная ручка для двери! Решение против COVID-19 !	5
Tarcza Antykryzysowa 4.0-zmiany w prawie pracy w dobie covid19	5
NOS- Items to Fight Covid 19	3
Covid-19 Compensation Fund	2
Covid-19 Compensation Fund	2
Имотният пазар във Варна и региона след COVID-19 – във фокуса на първата онлайн дискусия на Imoti.net	2
Más de 600 enfermeras han fallecido por el COVID-19 en todo el mundo	2
Junio 06 - RETENCIONES EN LA FUENTE DEL IMPUESTO A LA RENTA / Liquidación de compras y prestación de servicios / Aplicación de ley Humanitaria / Gestión financiera en COVID / Retenciones en la fuente del IVA / Formación de Asistente de RRHH	2
bangladesh40- june 2020 - sustainable economic yarns post 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: 103,450
Domains with Potential Mail Servers: 2,751
Email-Capable Domains and Hosts: 39,636
Live Hosts and Domains Not Parked: 41,070

Mobile Apps

Apps in Official Stores: 284

by Store

Apple	165
Google	111
WindowsPhone	7
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 631

by Store Type:

Hybrid	380
Secondary	223
Affiliate	28

Blacklisted Mobile Apps: 19

by Store Type:

Secondary	18
Official	1