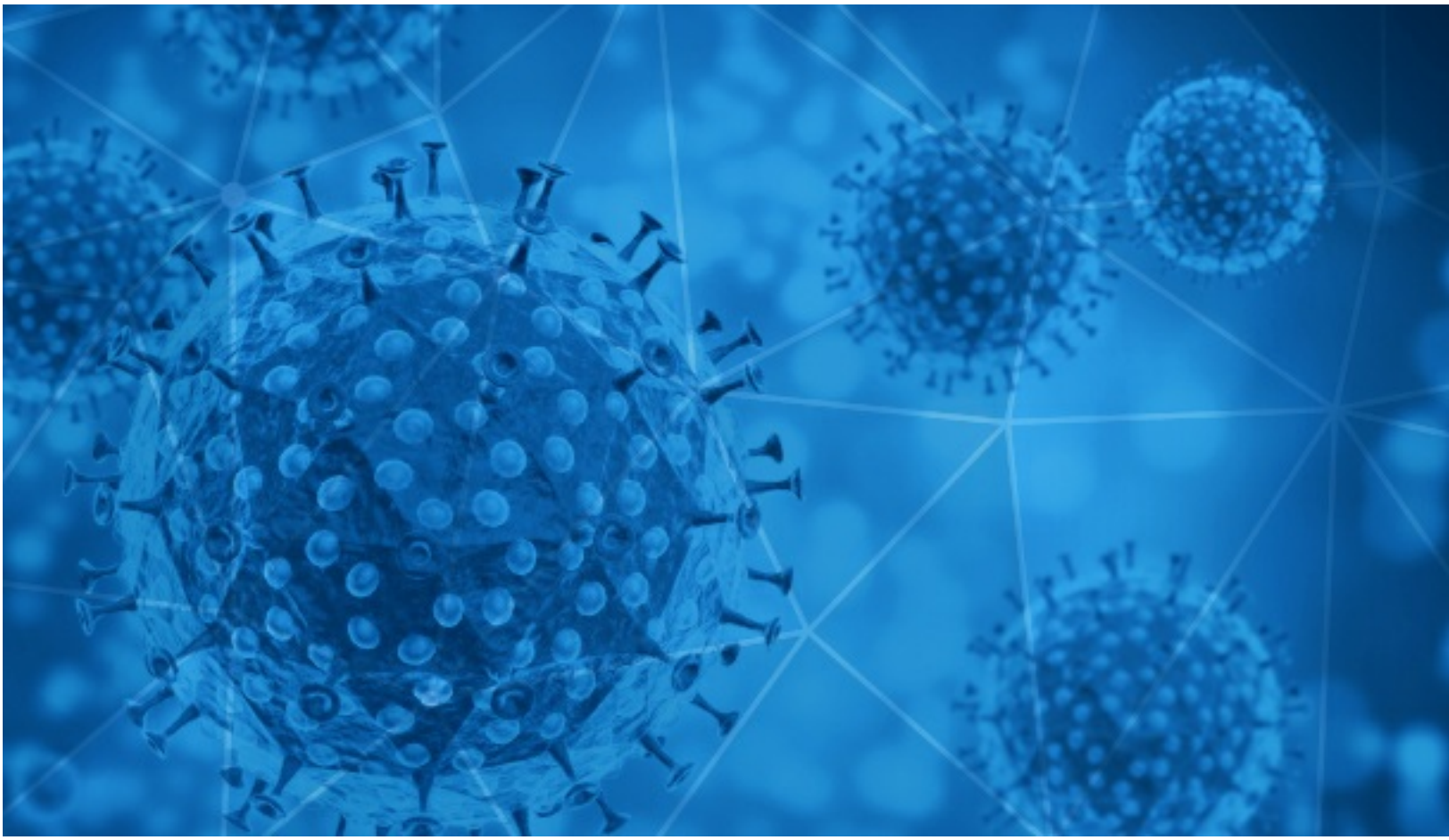
RiskIQ i3:

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

2020-10-21



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 2020-10-20 to 2020-10-21. During this period, RiskIQ analyzed 27,330 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 2,943 unique subject lines observed during the reporting period. The spam emails originated from 1,960 unique sending email domains and 4,150 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: The cold chain hurdle	3460
Ensure election-like arrangement for Covid-19 vaccine delivery, says PM; Releases autobiography of Dr. Balasaheb Vikhe Patil...More in the newsletter!	2442
COVID 19 community Dialogue Initiative 2020	1661
Limpieza y desinfeccion COVID 19	1462
Test de deteccion rapida COVID19	877
Test rapido para la deteccion del Coronavirus	855
RE: The Home Depot COVID-19 Clearance!	583
WORLD HEALTH ORGANIZATION $500,000 GRANT CONFIRMATION FOR CORONA VIRUS	577
Re: [izumrud] Листовка о COVID-19	437
WORLD HEALTH ORGANIZATION $500,000 GRANT CONFIRMATION FOR CORONAVIRUS	422
Evite el coronavirus en su negocio	380
Mascarillas y Otros Covid	355
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	352
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	321
Re: Defeat Coronavirus, non contact fever alarm device	297
0ferta test rápidos COVID 19	296
Help to fight COVID-19 fever alarm security door	262
Fwd:Credito Covid-19 Aprobado.	239
Contactless infrared body temperature thermometer defeat Coronavirus	239
Fwd:Cri¿½dito Covid-19 Aprobado.	235
Productos Prevención Covid en Oferta!	219
Auto INS Rates Drop Due To COVID	200
Your COVID-19 Test Results	176
Re: COVID-19 Stimulus Package90.106	154
Let’s fight together to get through the COVID-19	152

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

tutanota.com	3574
timesofindia.com	3460
gmail.com	2698
sampark.gov.in	2436
outlook.com	1810
yeah.net	822
keyable.net	798
126.com	505
publimailer.com	474
yahoogroups.com	440

Top-15 IPs Sending COVID Spam

45.143.223.147	1661
201.231.5.239	794
201.231.10.124	780
113.116.207.167	750
201.231.19.102	662
201.231.27.146	536
65.52.22.71	475
165.22.32.231	355
181.46.136.168	352
201.231.58.53	320

Top-15 Countries Sending COVID Spam

IN	6380
US	6321
AR	4003
CN	3098
--	1844
FR	906
DE	672
GB	582
CL	538
CA	367

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

WHO EBOOK ON CORONA VIRUS	1

Top-15 Subjects Containing doc/xlsx Files

Online Workshop on "Kaizen Response to COVID Challenge – Improve Productivity Rapidly!" - 28 – 29 October 2020: 3.00 – 6.00 p.m.	19
Ocena ryzyka zawodowego (aktualizacja pod względem COVID -19)	14
PHHS 10 20 2020 End of Day COVID 19 Summary	7
LISTA BONO COVID.xlsx	3
Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020	3
ULTIMO SOLLECITO COVID-19 WEBINAR DIRETTA STREAMING Impatto crisi pandemica e L. 40/20 28-29/10/20	3
Release "Kampung Siaga Covid-19 Pertamina Ajak Warga Tafure Senam Bersama Guna Cegah Corona"	2
COVID-19 WEBINAR DIRETTA STREAMING Licenziamento del DIRIGENTE 18/11/20 (intera giornata)	2
Báo cáo tình hình ủng hộ, tài trợ của các doanh nghiệp cho các hoạt động phòng, chống dịch Covid 19 trong năm 2020	2
CCS 10379 Podrían triplicarse contagios de COVID-19 en esta semana, quédate en casa: Salud	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: 129,950
Domains with Potential Mail Servers: 2,738
Email-Capable Domains and Hosts: 49,087
Live Hosts and Domains Not Parked: 46,525

Mobile Apps

Apps in Official Stores: 464

by Store

Apple	237
Google	212
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,612

by Store Type:

Hybrid	860
Secondary	695
Affiliate	57

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1