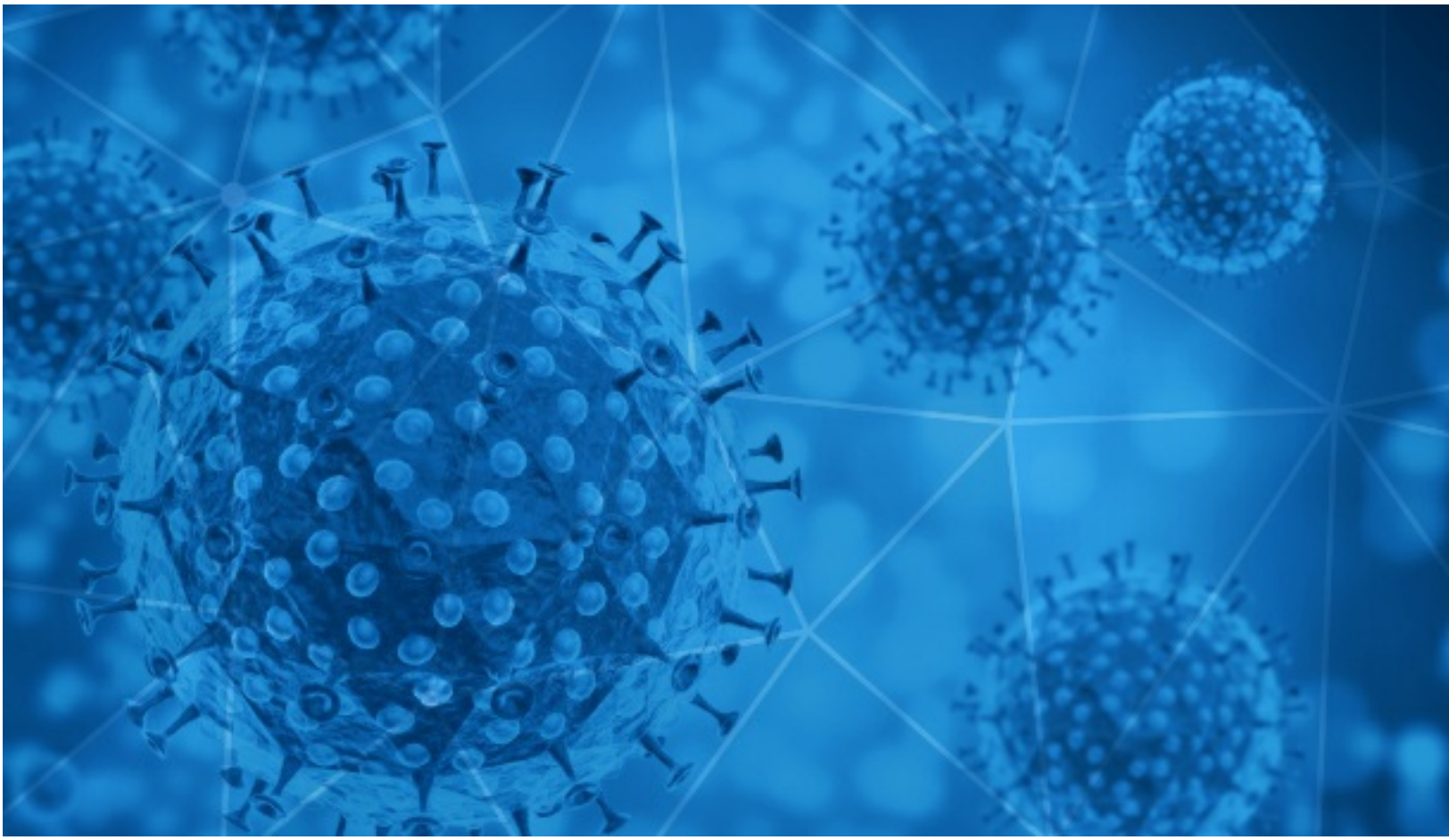
RiskIQ i3:

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

2020-10-22



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 2020-10-21 to 2020-10-22. During this period, RiskIQ analyzed 51,812 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,197 unique subject lines observed during the reporting period. The spam emails originated from 2,210 unique sending email domains and 4,898 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

PM chairs meeting on COVID-19 vaccine delivery & distribution; Hands over property cards to people in rural India...More in the newsletter!	7351
Ensure election-like arrangement for Covid-19 vaccine delivery, says PM; Releases autobiography of Dr. Balasaheb Vikhe Patil...More in the newsletter!	7084
Mitch McConnell dims hopes of coronavirus relief, NASA reaches an asteroid, and more from Apple News	5427
ATENCION COVID-19 Estudio Contable, Legal e Impositivo para tu negocio	2638
COVID-19 Asesoramiento contable para tu empresa	2595
Limpieza y desinfeccion COVID 19	1332
Evite el coronavirus en su negocio	1305
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO COVID19	1105
WORLD HEALTH ORGANIZATION $500,000 GRANT CONFIRMATION FOR CORONA VIRUS	1100
COVID 19 community Dialogue Initiative 2020	1091
Test de deteccion rapida COVID19	912
Test rapido para la deteccion del Coronavirus	891
TermoScanner Anti-Covid in pronta consegna. Prezzi dimezzati e modelli a partire da soli Euro 499,00. Non Abbassiamo la guardia!!!	782
Tokyo's Coronavirus Recuperation Set Abundant in Food - Sankaku News	594
Re: [izumrud] Листовка о COVID-19	549
Covid-19 Compensation Relief Funds of $850,000.00 USD :	533
COVID-19 Update: We're open & shipping daily! details	407
Productos para protección COVID-19	399
Register Now | Future of Work post Covid-19	331
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	288
What has changed for PE/VC investments post Covid-19. Register now to join the experts.	283
Contactless infrared body temperature thermometer defeat Coronavirus	258
Re: Defeat Coronavirus, non contact fever alarm device	249
Help to fight COVID-19 fever alarm security door	243
Flu/Covid-19 Weekly questionnaire - Reminder week 43	200

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

sampark.gov.in	14435
tutanota.com	10014
insideapple.apple.com	5562
gmail.com	3417
outlook.com	1382
yeah.net	869
livejob.it	782
keyable.net	750
sankakucomplex.com	594
126.com	577

Top-15 IPs Sending COVID Spam

201.231.6.185	4519
201.231.8.171	1422
181.46.136.168	1105
45.143.223.147	1091
190.247.241.142	1056
201.231.5.31	987
190.247.240.10	931
185.221.173.42	781
201.231.5.124	747
113.116.204.176	684

Top-15 Countries Sending COVID Spam

IN	14882
US	12007
AR	11261
CN	3791
--	1273
IT	1270
FR	985
NL	708
DE	674
PE	537

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

Online Workshop on "Kaizen Response to COVID Challenge – Improve Productivity Rapidly!" - 28 – 29 October 2020: 3.00 – 6.00 p.m.	12
NP_La Generación Pandemial: llega el corona baby boom	7
COVID-19 WEBINAR DIRETTA STREAMING Processi di DIGITALIZZAZIONE: presidi normativi e industria 4.0 1/12/20 (intera giornata)	6
PHHS 10 21 2020 End of Day COVID 19 Summary	5
Taxation, Payroll Reconciliation and Impact of Covid 19 on your Payroll Function Course 2020	4
CONVOCATORIA | El origen del virus copa más de la mitad de los bulos sobre la Covid-19	3
Convocatoria: MAÑANA, ¿Están dispuestas las enfermeras a vacunarse masivamente contra la gripe para hacer frente a la pandemia?, ¿cuál es su percepción de la vacuna del COVID?	3
Fwd: Corona-Pandemie 2020. Vollzug des Infektionsschutzgesetzes (IfSG) und der Bay. Infektionsschutzmaßnahmenverordnung (Bay.IfSMV)	2
Fwd: Διαδικτυακή εκδήλωση στο πλαίσιο της ελληνικής προεδρίας του Συμβουλίου της Ευρώπης «Προωθώντας την ισότητα των φύλων: ο ρόλος και το πλαίσιο λειτουργίας των θεσμικών μηχανισμών για την ισότητα εν μέσω COVID-19.	2
NUEVA FORMACION COVID PARA EMPRESAS	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: 130,052
Domains with Potential Mail Servers: 2,730
Email-Capable Domains and Hosts: 49,160
Live Hosts and Domains Not Parked: 46,718

Mobile Apps

Apps in Official Stores: 464

by Store

Apple	237
Google	212
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,618

by Store Type:

Hybrid	863
Secondary	698
Affiliate	57

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1