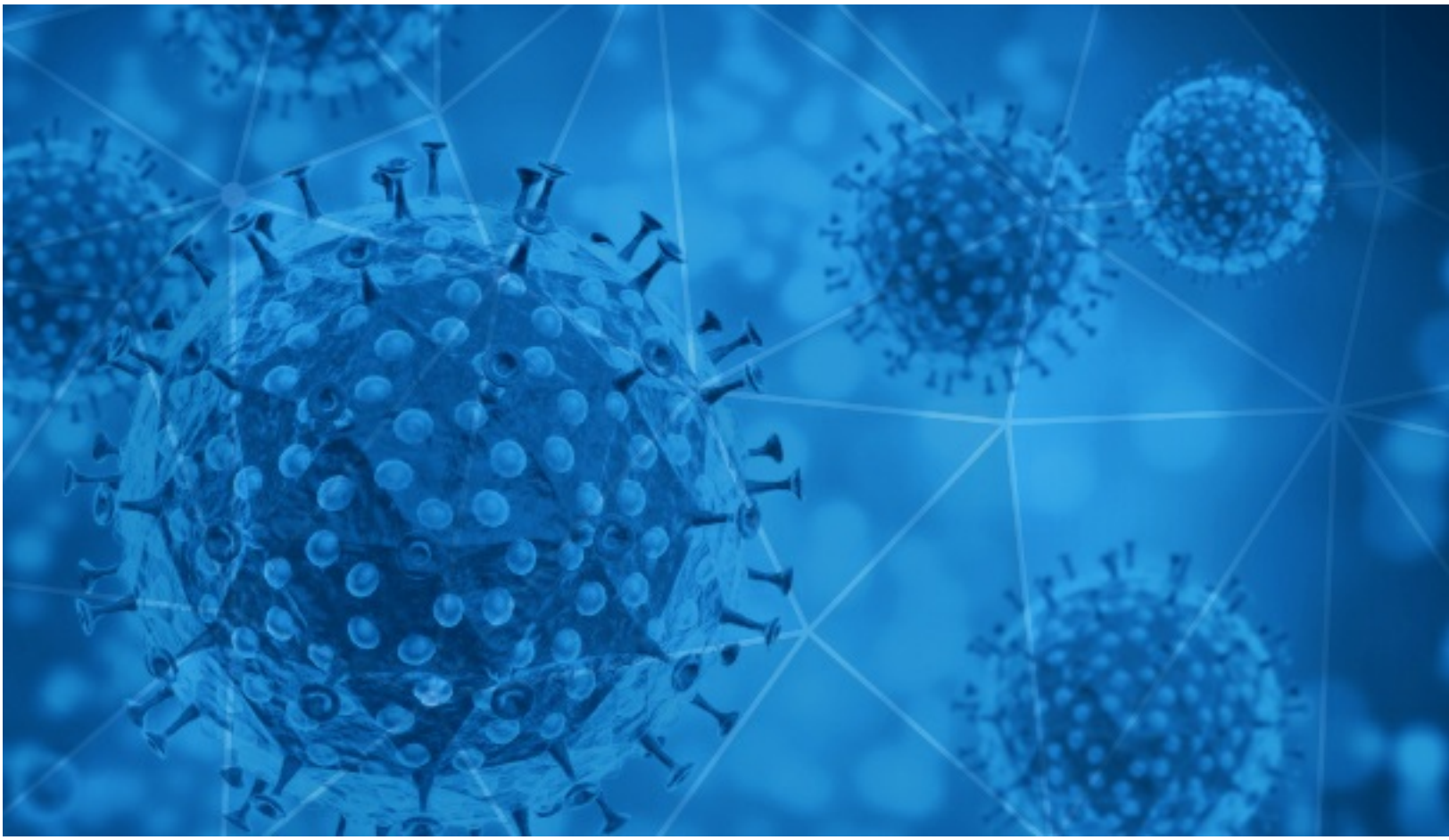
RiskIQ i3:

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

2020-09-30



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 2020-09-29 to 2020-09-30. During this period, RiskIQ analyzed 24,468 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,111 unique subject lines observed during the reporting period. The spam emails originated from 1,745 unique sending email domains and 3,888 unique SMTP IP Addresses. Analysts identified 0 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: When numbers don't suit politics	3630
More than 1 million coronavirus deaths, how the candidates are preparing for tonight's debate, and more from Apple News	2104
Pruebas Rápidas COVID-19 - Marca CELLEX // EE.UU.	783
Test de deteccion rapida COVID19	517
My COVID-19 Donation	511
Aprovecha productos de protección Covid en Oferta!!!	491
Limpieza y desinfeccion COVID 19	295
Re: CAYCH DIY foam hand soap, Kids love toy and gift. (Covid-19 Epidemic Prevention Products)	291
Register Now | Skills to learn for career growth amid COVID-19	274
post covid opportunities	274
Incontri online in Italia (no corona)	270
Protégete RESPONSABLEMENTE Contra el Covid -19 / Los Mejores Precios	259
COVID-19 KILLED ANTHONY	225
COVID 19: NUEVA PRUEBA NASOFARINGEA - MAYOR EFECTIVIDAD-	214
800.000,00 USD Covid -19 Financial Relief Funds!	201
COVID -19 RELIEF FUND	199
La Nueva Forma De Trabajar En Tiempos De Coronavirus Rentabilizando Tu Voz	194
Liquidacion Final Covid19	190
Re: Covid-19 acrylic protect shield	180
Re: Corona virus Protection Pills.Order confirmation	178
Corona virus Protection Pills and sex pills.	175
Mamparas de proteccion COVID19	175
YOU ARE LUCKY TO BE SELECTED FOR COVID-19 IMPACT	174
Magnette: ‘Akkoord vanavond of vannacht’ - ‘Maar 2 flessen jenever per dag was al moeilijk’ - Meer dan helft bevolking ziet nut van ‘coronabadges’ - Pick-up trekt aandacht op betoging Vlaams Belang: ‘Niets te maken met nazisme’	172
Newsletter quotidiana ADVexpress - Le strategie per la ripartenza di MSC Crociere; Ricerca Astra/Club degli Eventi sull'impatto del Covid; Discovery Media lancia Pop Up; Monica Magnoni entra nel Gruppo Roncaglia	172

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	3630
insideapple.apple.com	2104
gmail.com	1699
countermail.com	1135
yeah.net	804
focazen.com	783
126.com	776
163.com	531
houzz.com	409
claimintl.com	313

Top-15 IPs Sending COVID Spam

43.239.110.184	511
201.231.83.223	352
201.231.58.102	282
93.158.205.70	274
5.199.131.7	270
91.207.249.35	225
219.65.84.186	219
219.65.85.17	219
159.203.58.154	217
219.65.85.24	207

Top-15 Countries Sending COVID Spam

US	8311
IN	4656
CN	2477
DE	1407
AR	1198
FR	725
--	597
BE	597
NL	534
CA	441

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

Prawo pracy po zmianach - najnowsze przepisy a COVID 19	7
PHHS 9 29 2020 End of Day Summary COVID 19	5
Convocatoria Enfermeras estomaterapeutas denuncian la situación de los pacientes ostomizados en la primera ola de COVID-19 y temen lo que está venir	4
covid 19 health payment	4
Tomorrow : CII Virtual Session on "How to Reboot Manufacturing Post Covid-19 Impact? Using the AI/ Digital Technology" : 30 September 2020	3
50 εκ. ευρώ από την Περιφέρεια Κρήτης για μικρές και πολύ μικρές επιχειρήσεις της Κρήτης που επλήγησαν από την πανδημία Covid-19	2
Invitation | COVID-19 INNOVATION IDEATHON GRAND FINALE | Webinar | 30th September-2020 | 11:00-12:00 Hrs	2
ERYC Covid 19 Update	2
FW: Порядок действий при положительном результате тестирования на Covid-19; Информирование предприятия при заболевании работника или его родственников с симптомами ОРЗ, ОРВИ с подозрением на Covid-19	1
Autodichiarazione Covid-19.docx	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: 127,198
Domains with Potential Mail Servers: 2,893
Email-Capable Domains and Hosts: 48,095
Live Hosts and Domains Not Parked: 71,675

Mobile Apps

Apps in Official Stores: 436

by Store

Apple	220
Google	201
WindowsPhone	14
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 1,487

by Store Type:

Hybrid	819
Secondary	613
Affiliate	55

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1