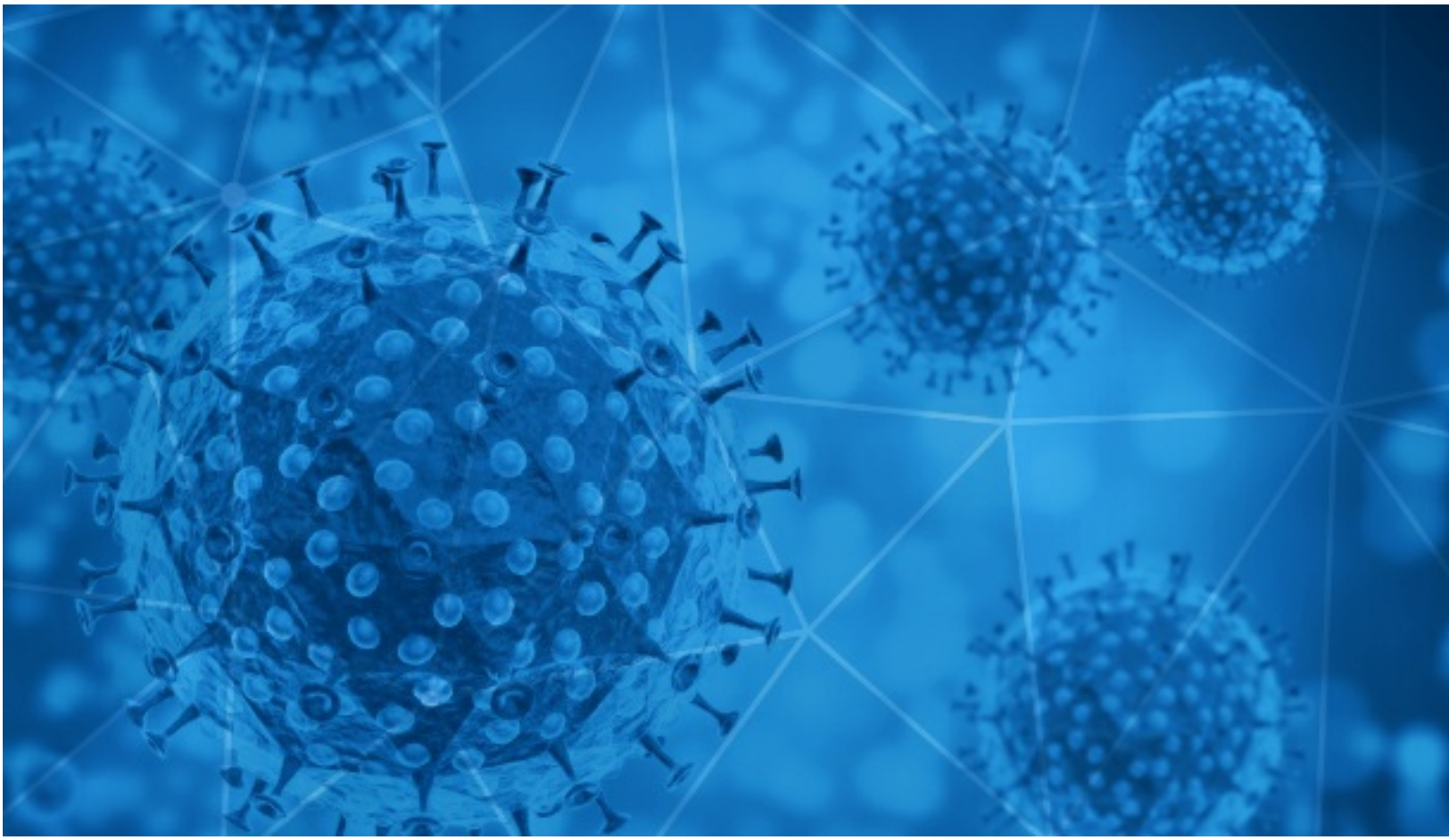
RISKIQ®

RiskIQ i3:

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

2020-05-26



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 2020-05-25 to 2020-05-26. During this period, RiskIQ analyzed 61,784 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 5,972 unique subject lines observed during the reporting period. The spam emails originated from 4,505 unique sending email domains and 7,018 unique SMTP IP Addresses. Analysts identified 11 emails which sent an executable file for Windows machines.

Top-25 Subjects

Covid-19: non fermiamoci adesso	5066
Re: UN COVID-19 Stimulus	4527
Sales: Face Mask, Gloves & COVID-19 Safety Kits	3605
The Corona Letter: A bittersweet homecoming for migrants	2898
Re: Vanity upon Vanity, COVID -19.cc	1988
Competencias a desarrollar tras el Covid19	1705
Protejase del Covid-19, Productos Certificados	1530
Re: CAYCH first DIY foam hand wash, make kids more happier and healthier. (Covid-19 Epidemic Prevention Products)	1426
Catalogo articulos prevencion Covid-19	1267
Ripartire dopo il COVID con la Germania	1208
Covid19- Compensation Notice.	961
Covid-19 Cash Support für Sie	889
AHORRA Dinero, Emprende y Protege tus espacios contra el Covid-19 con Productos Novedosos	831
Products for COVID-19	753
URUGENT!!! Covid - 19 Zimmerman Swiss RFQ.	733
Ofertas de Locura para la Contingencia COVID-19 Insuperable!	703
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO ANTE EL COVID19	666
Control de Asistencia: Evite el contagio COVID-19 con Tarjetas de Proximidad, Rostro o Palma	638
BANNED GOODS DUE TO COVID 19 PANDEMIC	580
Trajes Protectores Reutilizables COVID-19	560
AW: Covid-19-Hilfsfonds (Antwort für Details)	552
Все игроки РПЛ с COVID-19	541
LAZIO: contributi a fondo perduto, per far fronte ai danni causati dall'emergenza COVID-19, a favore di operatori del settore turistico. Scadenza 5 giugno 2020.	512
covid- 19 desimfección sanitización	456
VENETO: contributi alle attività commerciali di valore storico e artistico, iscritte nell'elenco regionale dei luoghi storici del commercio, per far fronte alle conseguenze dell epidemia di Covid-19. Scadenza 22 giugno 2020.	426

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	7264
ediscomspa.com	5064
onet.eu	4527
rediffmail.com	3605
126.com	3207
timesofindia.com	2899
163.com	2509
trendingtopic.cl	2359
focazen.com	2055
innovalearnexperience.com	1705

Top-15 IPs Sending COVID Spam

103.141.137.241	4527
51.91.221.33	2024
45.95.169.100	1643
119.122.89.46	1343
193.70.146.201	1331
51.77.33.44	985
91.143.80.127	961
46.254.37.34	938
51.77.33.43	909
209.58.149.66	753

Top-15 Countries Sending COVID Spam

US	13505
IT	7897
--	7171
CN	7156
FR	6097
IN	3358
DE	2464
UA	1426
AR	1338
GB	1173

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

RE: RFQ: Pedido pendiente antes de Covid-19 / procedimiento de trabajo para garantizar una entrega segura	9
LISTADO PRODUCTOS EXENTOS IVA - COVID 19 - REAL DECRETO	1
Dexellence Clinic - Chestionar COVID19 (Stoica Violeta)	1

Top-15 Subjects Containing doc/xlsx Files

Covid-19 Related Products Price List	11
[International School of South Africa] Covidtydskapsule	11
Coronavirus, in Campania celebrato il primo battesimo d'Italia.	11
SEDECO invita "Apoyo para personas residentes de la Ciudad de México que perdieron su empleo formal derivada del SARS-COV2 (COVID-19)"	10
Covid 19 Sanitizing tunnels -Affordable protection for your staff and clients	7
CII - List of Participants - Webinar on 'Managing Supply Chains to Maximise Sales Post Covid-19': Wednesday, 27 May 2020: 3:00 p.m. to 5:00 p.m.	6
Comunicato stampa - CORONAVIRUS BANCO FARMACEUTICO TORINO DONATE 3.450 MASCHERINE FFP2 AD ANPAS	4
PROTEGE A TU EMPRESA FRENTE AL COVID	4
Comunicato stampa - Contraccezione e Covid-19: Bayer fa il punto della situazione con tre esperte ginecologhe.	4
La Secretaría de Desarrollo Económico de la Ciudad de México, les invita participar en el programa: "Apoyo para personas residentes de la Ciudad de México que perdieron su empleo formal antes y durante la emergencia derivada del SARS-COV2 (COVID-19)	4

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: 98,238
Domains with Potential Mail Servers: 2,952
Email-Capable Domains and Hosts: 36,838
Live Hosts and Domains Not Parked: 39,499

Mobile Apps

Apps in Official Stores: 272

by Store

Apple	160
Google	105
WindowsPhone	6
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 552

by Store Type:

Hybrid	319
Secondary	207
Affiliate	26

Blacklisted Mobile Apps: 17

by Store Type:

Secondary	16
Official	1