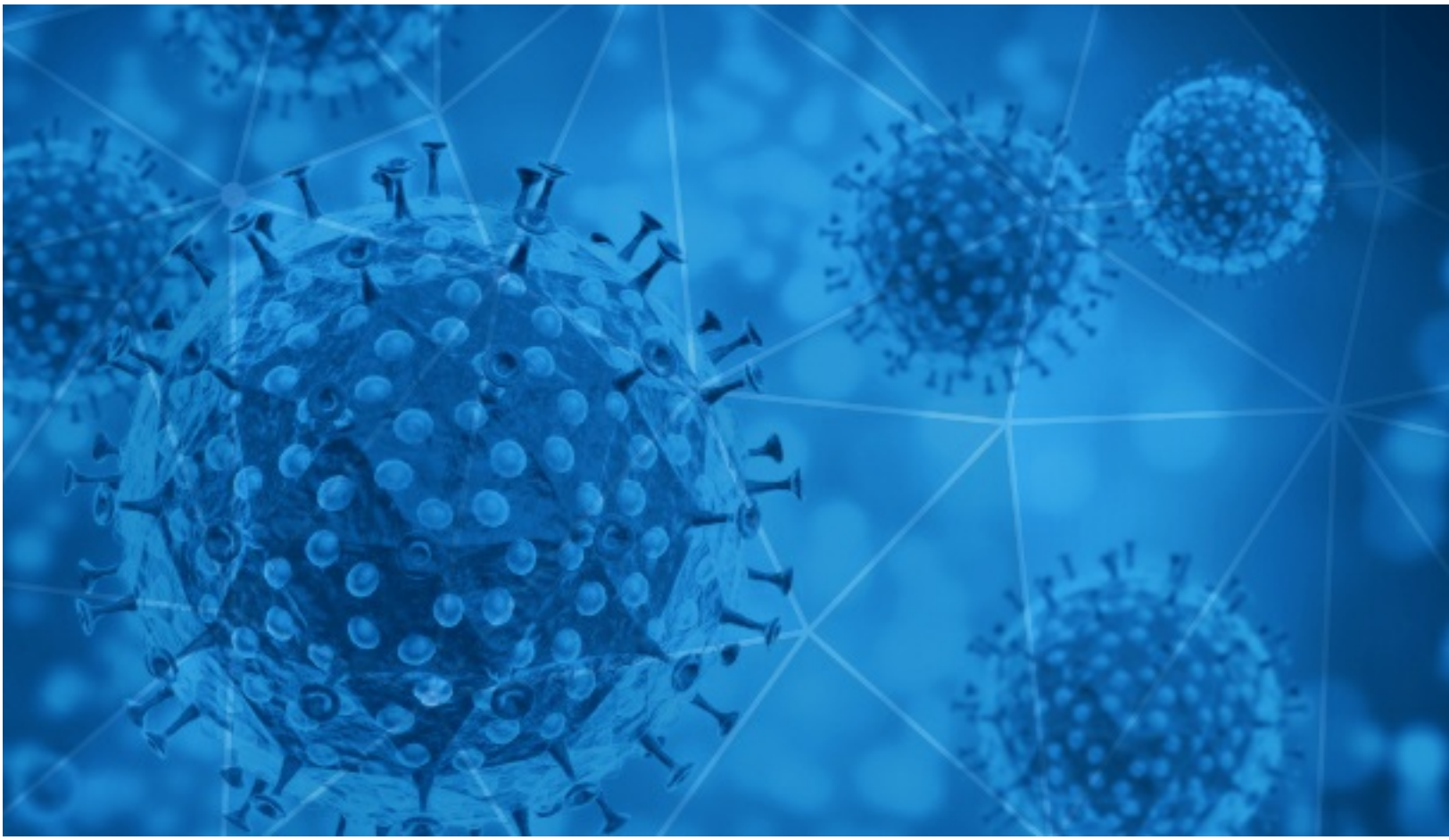
RiskIQ i3:

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

2021-02-05



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 2021-02-04 to 2021-02-05. During this period, RiskIQ analyzed 48,060 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 3,678 unique subject lines observed during the reporting period. The spam emails originated from 2,213 unique sending email domains and 4,193 unique SMTP IP Addresses. Analysts identified 38 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	17297
The Corona Letter: Can vaccine shots be interchanged?	3573
COVID TASTE RESULT	3009
YOU ARE COVID-19 REWARD BENEFICIARY	2350
TermoScanner e strumenti DPI Anti-Covid in pronta consegna con sconti oltre il 70% e prezzi a partire da Euro 39,00 + spedizione gratuita. Non Abbassiamo la guardia!!!	2316
COVID LOANS FROM UNITED NATIONS	1563
Public Relation Facebook Covid-19 Lottery Department	1510
COVID-19 Pantallas Protectoras	684
_Step_Closer_To_FDA_ Approval_ 20 People_Take COVID19_ PILL!	437
Controla el COVID de Forma Efectiva y Segura en tu Empresa	354
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove...etc.	319
COVID-19 Impact on Banking and Financial Services	312
, See how Covid 19 Affected Your Pension Fund	280
Do you have Covid Antibodies ?	232
Multi State Taxation and COVID	230
[QC] ATALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID -19	208
[CND Español - 4330]. Pandemia, restricciones y venta de pruebas falsas de Covid-19	208
CE FDA 510K GLOVES covid-19 Vaccine ,back to me	180
Good Morning, SA | Zuma must be arrested, says Glynnis Breytenbach, scientists fear Covid-19 variants without global vaccination	180
COVID-19	173
COVID Healthcare - Verified Contacts Leads	172
[QC] ATALIAN VIỆT NAM - CUNG CẤP DỊCH VỤ KHỬ KHUẨN PHÒNG CHỐNG COVID -19	166
Destination Thailand News - News Alert - Tourist attractions open to visitors under COVID-19 prevention guidelines	143
Urgent Job Opening || Sterling OMS Consultant || Baton Rouge, LA (Remote till COVID) || Contract **	142
COVID -19 NUTZENFONDS	116

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

epc-store.com	17300
gmail.com	5300
timesofindia.com	3573
livejob.it	2408
rediffmail.com	1518
outlook.com	1350
yahoo.com	1187
mailinator.cl	684
163.com	678
mail.com	518

Top-15 IPs Sending COVID Spam

115.238.247.228	2912
185.221.173.42	2408
87.248.52.51	1635
114.104.155.95	1276
210.5.156.90	1171
110.186.72.61	722
59.152.229.114	663
103.225.54.195	607
103.225.55.22	462
216.87.190.232	436

Top-15 Countries Sending COVID Spam

JP	17504
US	7233
CN	7181
IT	4286
IN	3873
FR	1548
GB	1057
DE	802
HK	677
VN	594

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

URGENT TENDER#675320 (covid19 kits)	37

Top-15 Subjects Containing doc/xlsx Files

***IMPORTANT* Bulk Quote Request-Covid19**	83
WEB OnLine COVID 19 Appalti e subappalti: direzione e controllo, gestione cantieri e tutela dei lavoratori 25/3/21	21
WEBINAR COVID 19 bilancio IAS/IFRS: equilibrio finanziario, aspetti contabili rilevanti e novità fiscali - 4 CFP Odcec - 25/2/21	14
CUMPLIMIENTO DE PROTOCOLOS DE BIOSEGURIDAD PARA MANEJO DE PANDEMIA CORONAVIRUS - COVID19	11
Teuteuga ole Poloaiga COVID19 - 04 Fepuari 2021	8
Epilessia e Covid: il punto della Società Italiana di Neurologia in occasione della Giornata Mondiale	6
ECONOMIC AND SOCIAL COUNCIL (UN ECOSOC FIGHT FOR CORONA VIRUS PANDEMIC / 2020)	5
Masti + Dezinfectanti COVID-19 - In atentia Departamentului de Achizitii	3
Nel fine settimana i test anti-Covid anche a PescaraFiere in via Tirino	3
EXISTENCIAS MEDIPLUS *VACUNA COVID*	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: 141,322
Domains with Potential Mail Servers: 2,572
Email-Capable Domains and Hosts: 51,272
Live Hosts and Domains Not Parked: 43,931

Mobile Apps

Apps in Official Stores: 511

by Store

Apple	252
Google	242
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,072

by Store Type:

Hybrid	1061
Secondary	944
Affiliate	67

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1