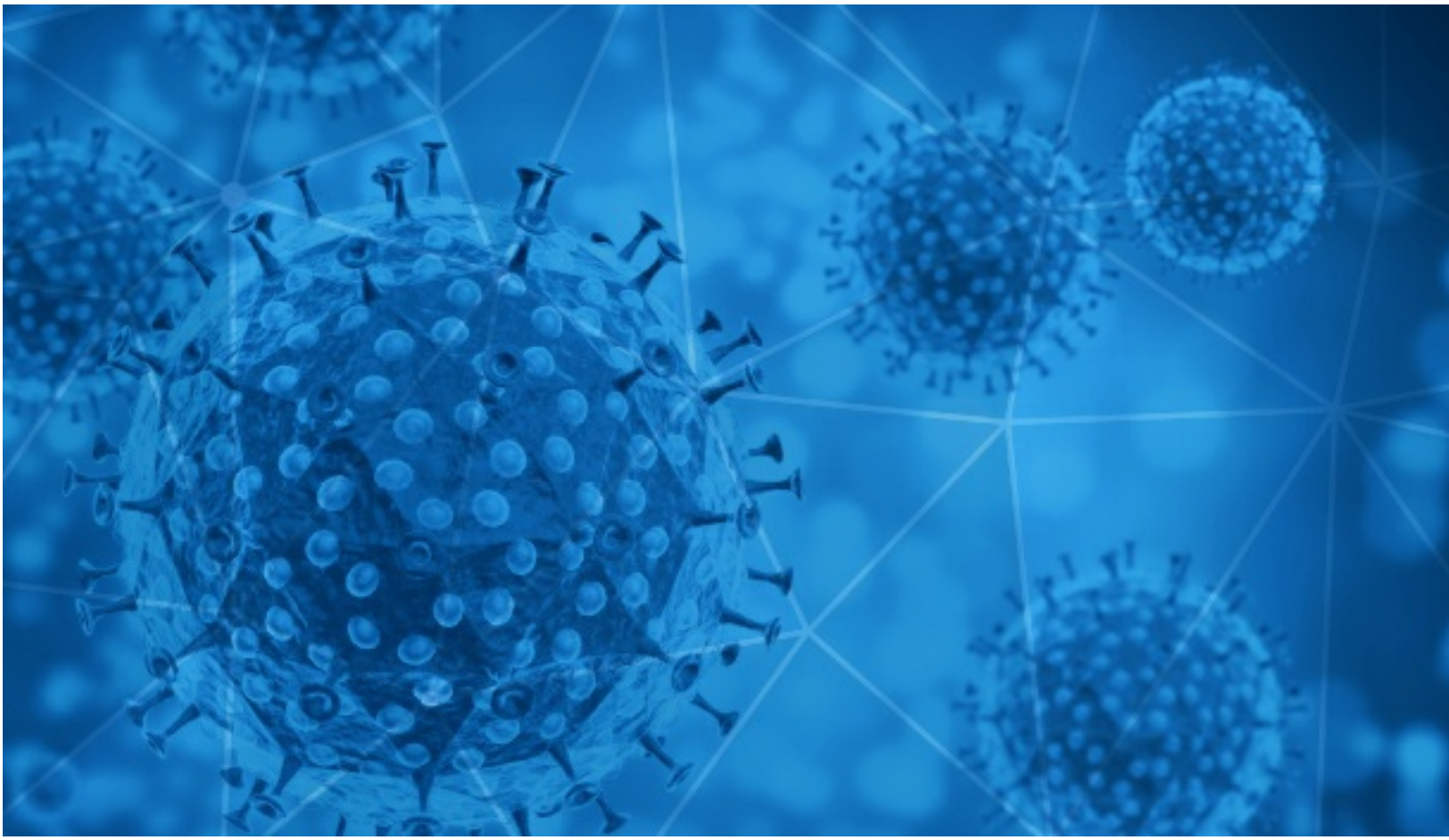
RiskIQ i3:

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

2021-02-11



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 2021-02-10 to 2021-02-11. During this period, RiskIQ analyzed 41,405 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,589 unique subject lines observed during the reporting period. The spam emails originated from 1,961 unique sending email domains and 3,683 unique SMTP IP Addresses. Analysts identified 758 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	17770
The Corona Letter: India preps up to expand vaccination drive	2426
ICO Covid Inversión	1132
Looking for the perfect COVID PROOF BUSINESS TODAY!?	1099
UN Covid-19 Winning Notification	1014
Gorilla Glue Woman Gets Ponytail Cut Off+Paris Hilton abused for 11 months +2K Jamaicans catch COVID	830
Introducing Instant Covid-19 Home Test App	748
Better than COVID Vaccine…	680
Realiza tu test COVID anticuerpos o antígenos a 9,95€ (Exento de IVA). Generador de OZONO a 39,95€*	557
NOVITA’ SUL MERCATO “ANCHE IN ITALIA TEST SALIVARE COVID-19 ANTIGEN SPITTEST PCL”	556
Re: Personal, SME & Business Relief (COVID-19) *	546
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!!!	458
COVID TASTE RESULT	450
VENETO: prorogato al 31/12/2021 l'intervento straordinario per finanziamenti agevolati per esigenze di liquidita' delle imprese colpite dall'emergenza da covid-19	441
Are Covid Restrictions or Economic Barriers Impacting your Bottom Line? Obtain Business Funding | Request Details	265
CUIDADO DE ADULTOS MAYORES /// PROTOCOLO ANTE EL COVID19	217
Re: BATCH REF: FEB/COVID/2021/836278215 redacted@threatwave.com	156
UN Covid-19 Winning Notification	132
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW	124
Attn Beneficiary congratulation for our Covid 19 relief package.	123
Re: covid-19 touch monitor	117
Your Ultimate Protection against COVID-19. US FDA Registered	111
Новые реакции вашему сообщению в чате «Украина запретила регистрировать российские вакцины от COVID-19»	110
Open VLD-voorzitter Lachaert: ‘Sihame moet dringend duidelijkheid verschaffen’ - Straks slaan we weer meer vaccins in de vriezer op - Coronablog | Duitse regering wil lockdown verlengen tot midden maart - Zij moesten maanden wachten op uitkering -…	107
RSA Liguria. Covid19 è stata una strage. Epidemia colposa.	102

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

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

giant-pw.com	17773
gmail.com	3865
timesofindia.com	2436
sabaziusiv.com	1026
caribbeanfever.com	830
who.int	748
mellitoxx.cyou	680
cmbmutualfunds.com	624
amonmed.es	557
sicurezzanews.it	556

Top-15 IPs Sending COVID Spam

157.245.42.150	1587
47.112.227.11	901
84.38.133.27	748
72.19.13.60	680
185.221.173.42	467
103.225.52.24	458
103.225.52.229	452
103.225.53.123	447
210.5.156.90	446
46.254.37.34	441

Top-15 Countries Sending COVID Spam

JP	17959
US	8220
IN	2680
CN	1810
DE	1505
ES	1466
IT	1207
NL	1150
--	836
FR	809

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Introducing Instant Covid-19 Home Test App	748
AGO DEC 2020 EXERCICE 2019 REPRISE DU SUIVI DU BUDGET 2018 distanciel "coronavirus" barrages.	1

Top-15 Subjects Containing doc/xlsx Files

WEBINAR COVID 19 bilancio IAS/IFRS: equilibrio finanziario, aspetti contabili rilevanti e novità fiscali - 4 CFP Odcec - 25/2/21	17
UN Covid 19 Relief fund.	7
ULTIMI POSTI - COVID 19 WEB ON LINE ANTICORRUZIONE E TRASPARENZA: proroga al 31/03/2021 del PTPCT – 24/02/2021	6
I: COVID 19_monitoraggio capacità assistenza_File madre_01.02 - 05.02_Teams.xlsx	3
COVID-19 Statement for 2/10/21	3
Marie Dalmaso covid negative	2
ADQUISICION DE ALIMENTOS BASICOS POR EMERGENCIA COVID-19 PARA EL HNERM	2
Cotação 055/2021 Avental - COVID	2
Relación empleados cuestionario y consentimiento Covid	2
Новий прайс. Знижені ціни. Захисні товари проти covid-19	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: 143,189
Domains with Potential Mail Servers: 2,589
Email-Capable Domains and Hosts: 52,062
Live Hosts and Domains Not Parked: 44,544

Mobile Apps

Apps in Official Stores: 511

by Store

Apple	252
Google	242
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,082

by Store Type:

Hybrid	1065
Secondary	950
Affiliate	67

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1