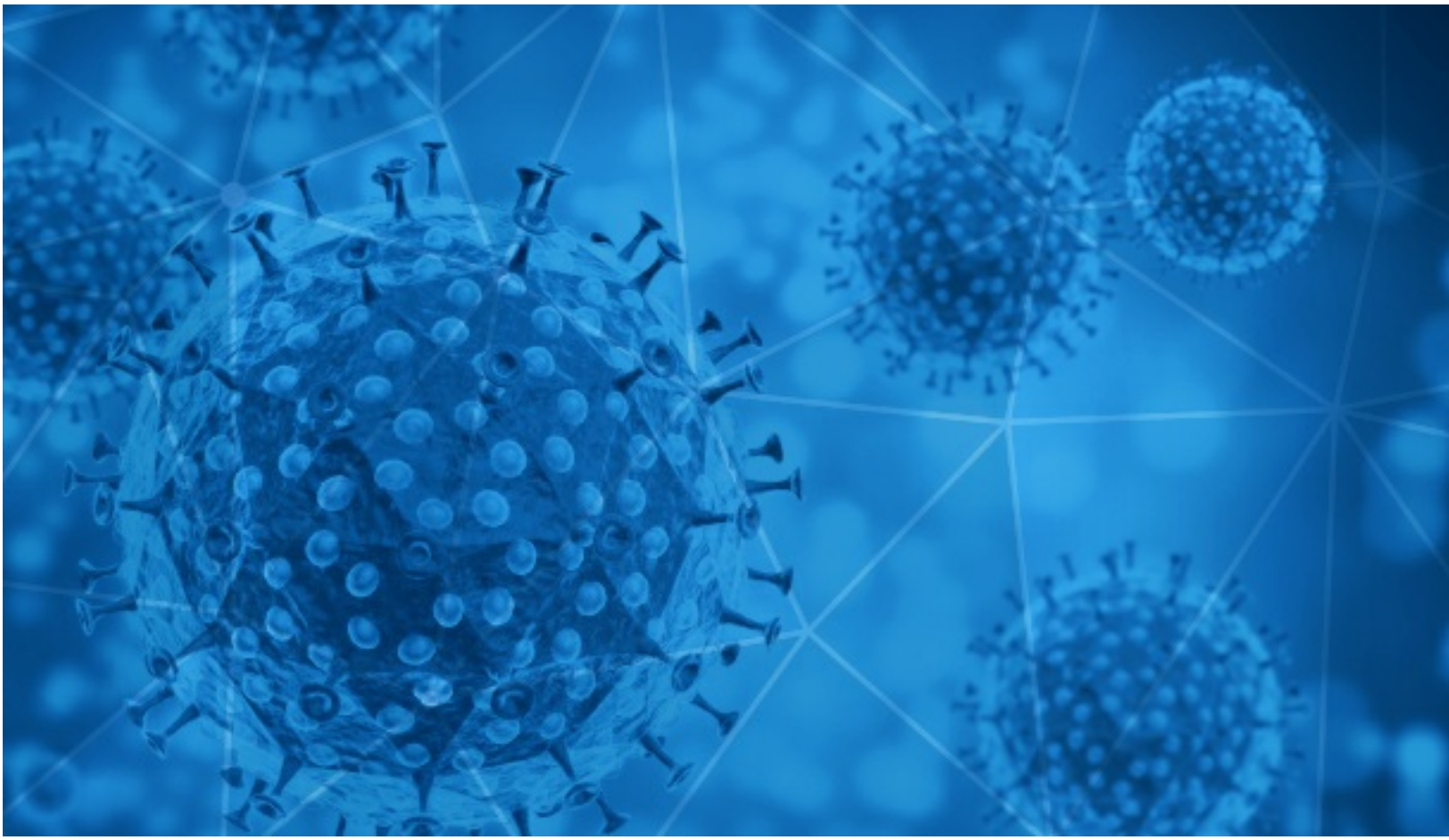
RiskIQ i3:

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

2021-01-26



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 2021-01-25 to 2021-01-26. During this period, RiskIQ analyzed 34,727 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,302 unique subject lines observed during the reporting period. The spam emails originated from 2,377 unique sending email domains and 4,273 unique SMTP IP Addresses. Analysts identified 2 emails which sent an executable file for Windows machines.

Top-25 Subjects

Spirit of Aatmanirbhar Bharat is in sync with the mood of today’s youth, says PM; Compliments Corona Warriors...Read more in the newsletter!	5703
U.S. surpasses 25 million COVID-19 cases, the latest on the stimulus package, and more from Apple News	4917
The Corona Letter: Vaccine diplomacy leads to 'undiplomatic' pushback	3385
Public Relation Facebook Covid-19 Lottery Department	1811
COVID-19 Pantallas Protectoras	1207
YOU ARE COVID-19 REWARD BENEFICIARY.	673
Covid-19 Innovation Strategy by MD of UA Finance	475
_Step_Closer_To_FDA_ Approval_ 20 People_Take COVID19_ PILL!	462
UN Covid-19 Winning Notification	452
_Step_Closer_To_ FDA_ Approval_ 20_ people_ Take_ COVID19_PILL !	420
Join DC Health Link for a Virtual Townhall “Focus on the Facts: COVID-19 Vaccines and Communities of Color”	379
$100 Million Immediate Supports for COVID-19 Response!	377
Your Ultimate Protection against COVID-19. US FDA Registered	321
Covid-19 Payment For You And Your Family	284
Re: Digital signage solution for Covid-19	249
UN Covid-19 Winning Notification	233
COVID19 LOANS FROM UNITED NATIONS	229
SP CONTRA A COVID-19!	213
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove...etc.	208
COVID-19	194
Dropping K1 for CR-1 Visa, Covid Test Required to Enter US, Biden Exec Order and Other Hot Topics This Week	157
POLONIJNY PANEL PROFESORÓW #SZCZEPIMYSIE COVID-19 Szczepimy Sie tak nie a tu odpowiedz	143
Re: covid-19 touch monitor	137
covid 19 darowizny	133
COVID19-DARLEHEN VON VEREINTEN NATIONEN	133

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	5703
insideapple.apple.com	4956
timesofindia.com	3392
gmail.com	2677
e-nautia.com	1749
grupocorreomasivo.com	879
herculist.com	723
ceoinsights.net	475
126.com	386
subscriptions.dc.gov	379

Top-15 IPs Sending COVID Spam

59.152.229.114	1810
103.18.244.112	858
185.24.233.19	673
216.87.190.232	578
103.36.92.144	377
82.190.72.197	362
153.126.160.254	284
164.100.13.127	278
164.100.13.128	275
164.100.13.130	265

Top-15 Countries Sending COVID Spam

US	12500
IN	9234
FR	1828
HK	1811
CN	1117
IT	923
MY	874
JP	850
IE	743
DE	522

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

vaccination covid actualisation du protocole et information complementaire	1
AOM on COVID related expenses	1

Top-15 Subjects Containing doc/xlsx Files

WEB OnLine COVID 19 Superbonus 110%, Sisma e Ecobonus: novità Legge Bilancio e Circolare 30/E/20 AdE 11/3/21	23
BHP – obowiązki pracodawcy i pracownika w dobie Covid 19	13
Fujitsu advierte del aumento de ciberataques de desinformación, para generar caos y confusión sobre vacunas del Covid 19	5
Studio Accenture (Davos)_Digitale e sostenibilità per uscire dalla crisi post Covid	3
HERE ATTACHED WITH 24 TH JANUARY 2021 COVID	3
Fwd: Fw: FYI... Covid 19 Resources - Nonprofit Policy Platform Survey | New HSC Guidance Documents	2
NdP - L'IDIAPJGol seguirà a 600 persones amb covid-19 persistent durant un any	2
PR "PVO neapstiprina Covid-19 vakcīnas saistību ar smagi slimu senioru nāvi"	2
COVID, INAUGURATI OGGI I 9 NUOVI AMBULATORI ALL'OSPEDALE BETANIA	2
Fw: COVID-19 Vaccinations for RVU students rotating with Dr. Hor	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: 140,720
Domains with Potential Mail Servers: 2,564
Email-Capable Domains and Hosts: 51,176
Live Hosts and Domains Not Parked: 43,868

Mobile Apps

Apps in Official Stores: 506

by Store

Apple	249
Google	240
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,052

by Store Type:

Hybrid	1053
Secondary	932
Affiliate	67

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1