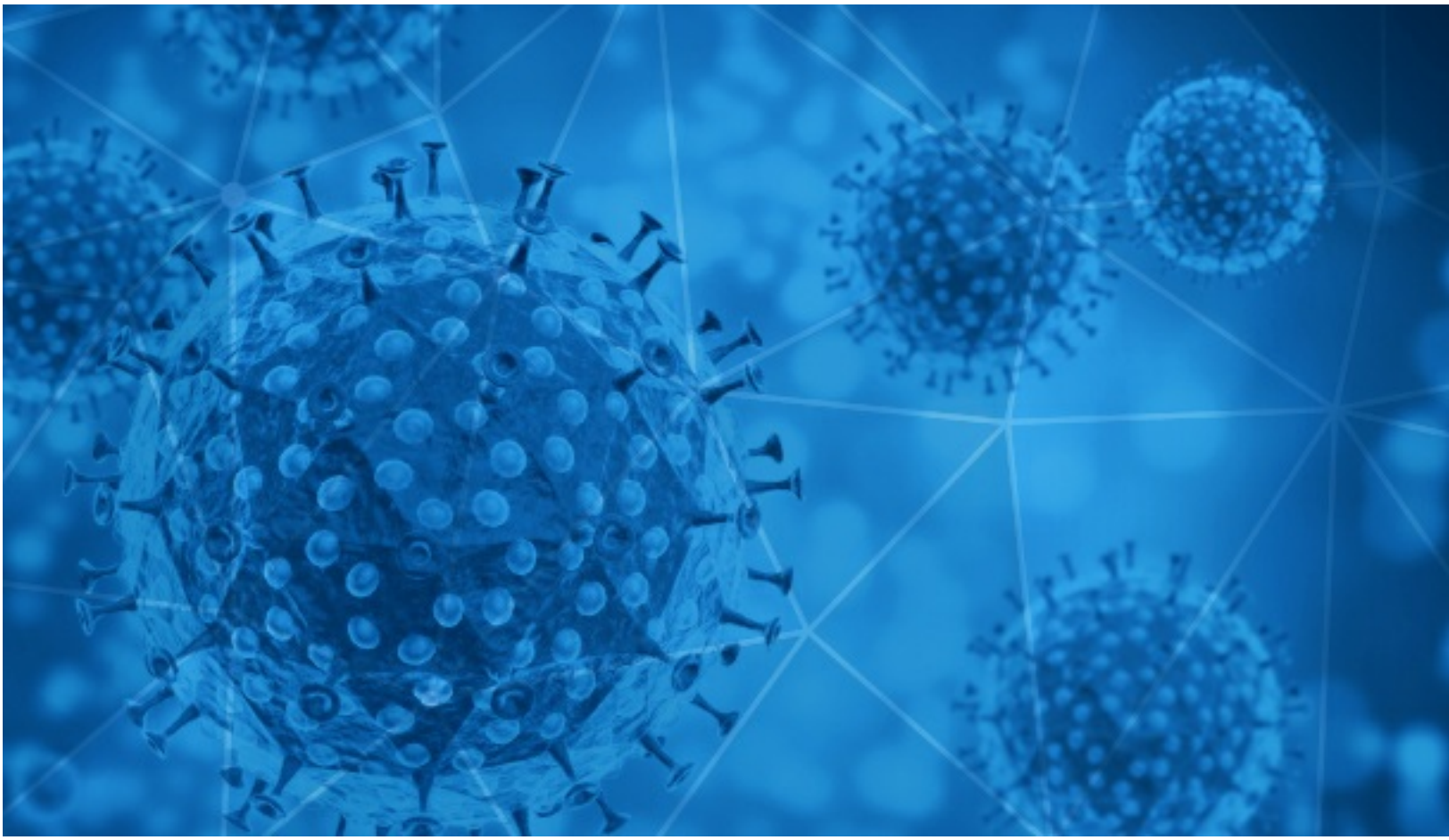
RiskIQ i3:

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

2021-01-25



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 2021-01-24 to 2021-01-25. During this period, RiskIQ analyzed 46,240 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 1,768 unique subject lines observed during the reporting period. The spam emails originated from 990 unique sending email domains and 2,371 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

{COVID-19} □□□□□□□□□□□□□□□□□□	16393
Spirit of Aatmanirbhar Bharat is in sync with the mood of today’s youth, says PM; Compliments Corona Warriors...Read more in the newsletter!	8698
The Corona Letter: Vaccine hesitancy makes a U-turn	4122
Public Relation Facebook Covid-19 Lottery Department	2314
Covid19 Global Relief Fund	1874
Relief Fund Covid19 Pandemic	1697
Covid-19 Payment For You And Your Family	1436
Harvardâs first line of defense against coronavirus	876
$100 Million Immediate Supports for COVID-19 Response!	614
UN Covid-19 Winning Notification	587
_Step_Closer_To_FDA_ Approval_ 20 People_Take COVID19_ PILL!	520
Your Ultimate Protection against COVID-19. US FDA Registered	411
Covid-19 Financial Relief Donation..	382
Re: Digital signage solution for Covid-19	269
UN Covid-19 Winning Notification	220
COVID-19 PANDEMIC COMPENSATION FUND 123987	218
Scholen in Antwerpen en Bekkevoort gesloten na uitbraak - Michel haalt uit naar farma - Waarom het virus ons onverdraagzaam maakt - Gevlucht voor droogte: 'In Zweden kun je nog rekenen op het klimaat' - Geen WK veldrijden door corona?	202
Re: covid-19 touch monitor	131
CovidShield - Make your Business Safer for Everyone	130
SP CONTRA A COVID-19!	130
Covid-19 Financial Relief Donation!!	129
Protest tegen avondklok ontspoort - Experts zien zorgwekkende coronatrend - Sneeuw in heel België	111
CovidShield - Reopen your Business the Right Way	105
Covid-19 : de nouveaux avantages extra-légaux pour 2021 | Tous les jobs techniques | Intéressé(e) par le codage ? BeCode et Microsoft lancent 5 nouvelles écoles !	91
How to Solve COVID-Related Problems (Retrenchments, Redundancies, Closures & Other Terminations)	91

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	16395
sampark.gov.in	8698
timesofindia.com	4122
fundstepnltdinfo.com	3571
gmail.com	2846
megalotintl.com	1655
ex.ua	639
acraccademia.it	572
e-nautia.com	522
herculist.com	511

Top-15 IPs Sending COVID Spam

51.79.158.32	3571
59.152.229.114	2312
153.126.160.254	1436
103.18.244.112	902
103.225.55.48	707
103.225.52.52	655
103.36.92.144	639
212.108.234.36	462
103.225.54.199	419
103.225.52.9	374

Top-15 Countries Sending COVID Spam

JP	17856
IN	12650
FR	3874
US	3252
HK	2417
MY	918
RO	743
SG	696
CN	695
BE	499

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

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

Dépistage COVID (volontaire)	1

Top-15 Subjects Containing doc/xlsx Files

ECONOMIC AND SOCIAL COUNCIL (UN ECOSOC FIGHT FOR CORONA VIRUS PANDEMIC / 2020)	25
ANC Weekly COVID-19 Reports	10
Fw: Covid, maxi assembramento nei pressi dell'Orientale. Ragazzo si arrampica su un lampione e stacca telecamera videosorveglianza tra gli applausi. Borrelli (Europa Verde): "Siano identificati i responsabili e multati per vandalismo e mancato distanziamento"	4
Fwd: isolamento precauzionale caso sospetto covid nido Brontolos	1
CCS/11179 Rebasa Chihuahua las 4 mil 600 defunciones por COVID-19	1
Fwd: VERY URGENT NOTICE - REPORTING OF POSITIVE COVID CASES	1
Fw: Details of employees who were confirmed to be infected with COVID-19 on (23rd Jan 2021)	1
Covid-19. Relatório do dia 24 de Jan. de 2021	1
B JEFFERSON MANOR EMPLOYEE Covids	1
Conferencia mañana CIDH derechos humanos ante COVID y texto situación triquis	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: 140,635
Domains with Potential Mail Servers: 2,574
Email-Capable Domains and Hosts: 51,188
Live Hosts and Domains Not Parked: 44,066

Mobile Apps

Apps in Official Stores: 506

by Store

Apple	249
Google	240
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,051

by Store Type:

Hybrid	1053
Secondary	931
Affiliate	67

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1