RISKIQ®

RiskIQ i3:

COVID-19 Daily Update

04/03/2020

Table of Contents

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. Customer agrees that RiskIQ shall not have any liability resulting from Customer's use of this information.

Notable Events: Previous 24 Hours

Life in China is now ruled by a green symbol on a smartphone screen. Green is the "health code" that says a user is symptom-free and it's required to board a subway, check into a hotel or just enter Wuhan, according to AP reporting.

The U.S. and European nations are evaluating the use of phone-based surveillance technology to help combat the spread of COVID-19. The U.S. federal government, in coordination with the CDC, is creating a portal to track phone geolocation data to help predict where outbreaks could occur next. Researchers at the Massachusetts Institute of Technology developed an app that tracks COVID-19 patients and those they interact with. Some European nations are tracking individuals who have been exposed to the virus and must be quarantined.

The Kansas Department of Health and Environment is using a GPS program to track residents' locations through their cell phones in a bid to slow coronavirus cases, Dr. Lee Norman, the head of department, revealed in a press conference Wednesday, 04/01/2020. Kansas is the first state to publicly acknowledge its use of such a program.

Rob Jackson, chair of the Global Carbon Project, reported carbon emissions could fall by as much as 5% year-on-year as a result of the COVID-19 pandemic. Such a decrease would be the biggest drop in carbon emissions since World War Two. Scientists warn carbon emissions will go back up once confinement practices end since there have been no structural changes to facilitate long-term emissions reduction.

American cities and states are working to provide shelter and health services to the homeless population, which is considered to be vulnerable to COVID-19. The $2 trillion relief bill passed and signed in March provides $12 billion to state and local governments to help get homeless people off the streets. There is not currently any national data tracking confirmed COVID-19 cases amongst the homeless, though Los Angeles County reported two such cases. Researchers from three universities released a study last week estimating 4.3% of the nation's homeless population could be killed by the virus and more than 21,000 will need to be hospitalized.

Captain Brett Crozier, commander of the aircraft carrier USS Theodore Roosevelt, was relieved of his command on Thursday, 04/02/2020, after drafting a strongly worded letter asking for assistance to control the outbreak of COVID-19 aboard the ship. Acting Navy Secretary Thomas Modly said Crozier was relieved of his command for failing to use the chain of command to report the issue and for sending his letter over "non-secure unclassified email." Crozier will reportedly keep his rank and remain in the Navy.

Morgan Stanley forecasted the U.S. economy will shrink 5.5% in 2020—the steepest drop since 1946—and will experience 38% contraction in the second quarter. Morgan Stanley also reports unemployment will peak at 15.7% in the second quarter. U.S. Congressional Budget Office projections show greater than 7% decline in gross domestic product in the second quarter.

Digital Exploitation

Marriott International disclosed on Tuesday 03/31/2020 a new data breach that impacted 5.2 million guests, according to CNET reporting. The hotel group said information exposed may include names, addresses, emails, phone numbers and birthdays as well as loyalty account details and information like room preferences.

ThreatPost reporting provided details about a spoofing campaign that promises users important information about new coronavirus cases in their local area. The phishing emails don't include specific names or greetings in the body of the messages, suggesting they are being sent out to a broad target audience.

A separate ThreatPost report indicates older phishing kits that were previously deployed and then retired are resurfacing and targeting people working from home. Attackers are using recycled phishing kits from as far back as July 2019 in coronavirus-based phishing attacks.

Security researchers are now seeing malware that either wipes everything off the computers of victims, or corrupts the master boot record of Windows machines so the computer hard drive is unusable. There's no financial gain from doing this. According to IT World Canada, victims will know they've been hit if a message pops up saying coronavirus has been installed.

Microsoft has started to send targeted notifications to dozens of hospitals about vulnerable public-facing VPN devices and gateways located on their network. As part of their tracking of various groups behind human-operated ransomware attacks, Microsoft has seen one of the operations known as REvil (Sodinokibi) targeting vulnerabilities in VPN devices and gateway appliances to breach a network, according to BleepingComputer.

New Blacklist Data

hxxps://sundayblogging[.]com/wp-content/themes/table/Covid-19-Stay-at-home/AMEXFRESH/AMEXFRESH/AMEXFRESH/home/

hxxps://goa-covid-19[.]in/

hxxps://fcovid-19[.]com/

hxxps://dentalleadgroup[.]com/COVID-19/banks/directing/atbonline/

hxxps://financialsupportcovid-19[.]com/

hxxps://grand-avtolombard[.]ru/wp-includes/js/swfupload/swf-ent/American-Express-Covid-19/home/

hxxps://iecfab[.]xyz/covid-19/

hxxps://newyork-20covid-19[.]com/

hxxps://orecon[.]co[.]jp/xmlrc-re/american-express-covid-19-stay-at-home/home/

hxxps://safefromcovid-19[.]com/

hxxps://supplycovid-19[.]com/

hxxps://pox-oreoo-8[.]com/cgi-binn/Covid-19-American-Express[.]com/home/

hxxps://permovqu[.]com/covid-19/banks/directing/atbonline/

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 04/02/2020-04/03/2020. During this period, RiskIQ analyzed 222,897 spam emails containing either "*corona*" or "*covid*" in the subject line. There were 16,097 unique subject lines observed during the reporting period. The spam emails originated from 9,190 unique sending email domains and 17,839 unique SMTP IP Addresses. Analysts identified 313 emails which sent an executable file for Windows machines.
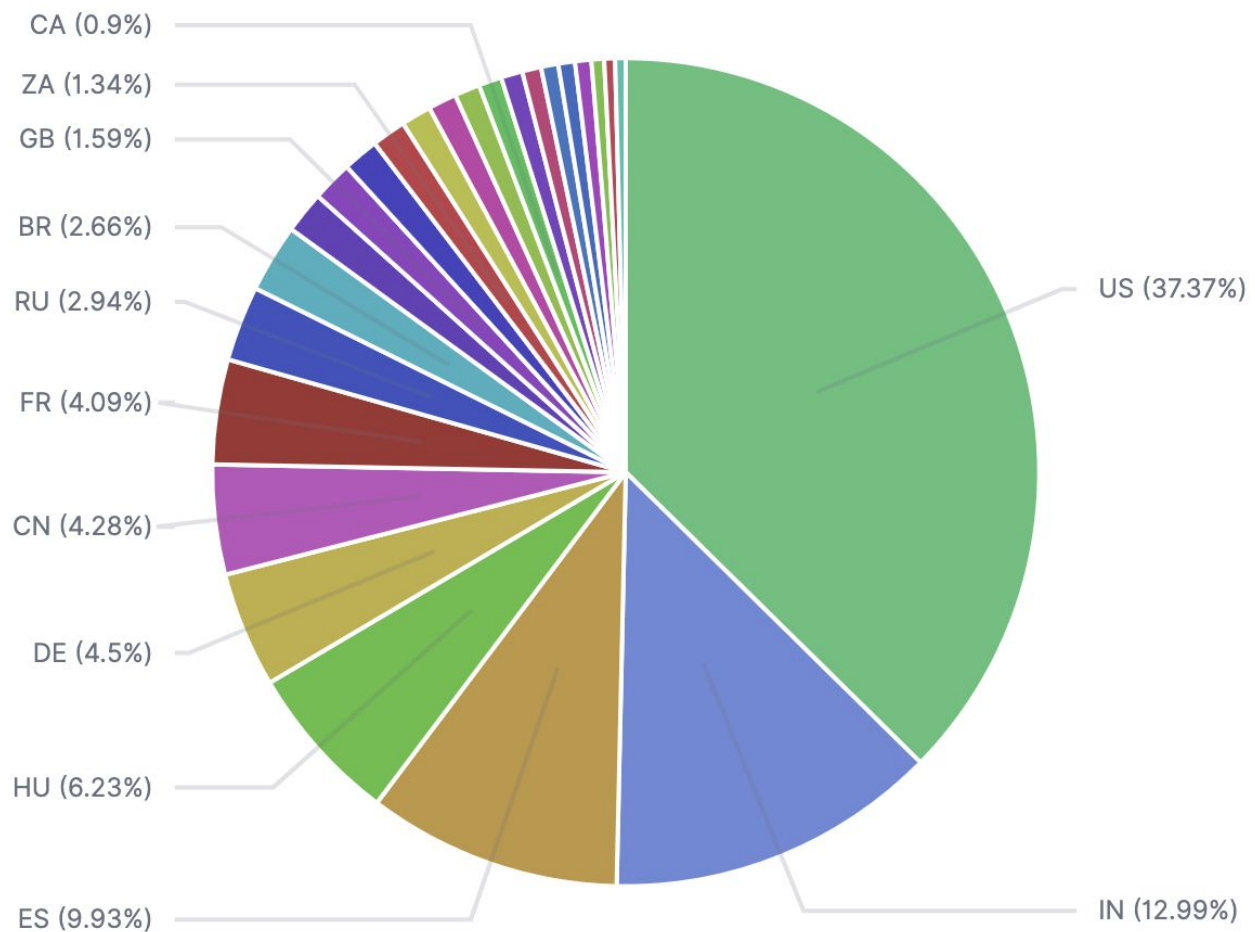
Spam emails by country of origin

Top 25 Subjects

1. 19,783 - The Mask that can prevent Coronavirus now

2. 15,095 - UPDATE: Fight The Coronavirus The Natural Way

3. 10,320 - ATEMMASKE zur Bändigung des Coronavirus - Sicherheit auf FFP2-Ebene

4. 10,257 - Hast du Angst vor dem Corona-Virus? Neue Atemmaske, schütze deine Lieben

5. 10,227 - Würdest du das CORONAVIRUS stoppen? Die Atemmaske schützt auch vor neue Infektion

6. 10,177 - Droht CORONAVIRUS? Mit Atemmaske können Probleme vorgebeugt werden

7. 10,138 - Kann das CORONAVIRUS vorgebeugt werden? Atemmaske für wirksamen Schutz

8. 10,097 - Coronavirus, Grippe? Hier ist die Atemmaske mit einem speziellen Filter

9. 9,811 - Coronavirus is spreading, this specialized mask can control it

10. 5,210 - The 3 plants you need to throw in your shopping cart to fight coronavirus

11. 3,510 - The Corona Letter: Is it time for everyone to mask up?

12. 3,296 - Spéciale Covid-19 n° 3 (en accès libre pour tous)

13. 2,714 - Coronavirus-Krise: Wir arbeiten für Sie

14. 2,606 - Message from Airtel CEO - Keeping you connected during COVID - 19

15. 2,600 - Message from Airtel CEO – Keeping you connected during COVID - 19

16. 2,536 - Ethical Covid-19 Pandemic Supplier

17. 2,502 - Anti Coronavirus Disease COVID-19!

18. 2,485 - COVID-19: These tech companies took the no-layoffs pledge | How Twitter ditched Hadoop and migrated to Google Cloud

19. 1,966 - U.S. medical stockpile is running low, how long the coronavirus lives on clothes, and more from Apple News

20. 1,909 - Tous mobilisés pour lutter contre le COVID-19

21. 1,570 - Covid-19 relief fund payment by Indian government

22. 1,207 - Re: CF and FDA covid-19 certificate test kits

23. 1,198 - This Mask Stops Coronavirus

24. 890 - Payment Assistance Due To Covid-19 Pandemic

25. 884 - IMPORTANTE - COVID-19 (CORONA VIRUS)

Top Subjects Containing Attachments with Executable Files for Windows Machines (PE/EXEs)

1. 113 - Important Notice to Our Corporate Clients & Partners - COVID -19

2. 81 - COVID-19 UPDATE !!!

3. 58 - Your shipment was returned to our office!!! BECAUSE OF COVID-19 OUTBREAK(TNT Express Notification)

4. 38 - nCov-19 _CoronaVirus_Safety__Precautionary_Measure.pdf

5. 20 - URGENT NEED: U.S. Department of Health & Human Services/COVID-19 Face Mask/ Forehead thermometers..

6. 3 - Fwd:Wellmien COVID-19 Supplies (Masks

Top Countries Sending SPAM - Covid/Coronavirus Contained in Subjects (by Geolocation on SMTP IP Address)

1. 75,509 US
2. 26,259 IN
3. 20,079 ES
4. 12,602 HU
5. 9,107 DE
6. 8,664 CN
7. 8,275 FR
8. 5,936 RU
9. 5,382 BR
10. 3,300 VN
11. 3,206 GB
12. 2,832 IT
13. 2,704 ZA
14. 2,378 AR
15. 2,247 NL
16. 2,007 KR
17. 1,823 CA
18. 1,702 UA
19. 1,500 ID
20. 1,361 CO
21. 1,316 BE
22. 1,285 SG
23. 999 BD
24. 855 HK
25. 831 PL

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.

Domains and Hosts

Domains: 47,926
Hosts: 53,919
Hosts and Domains with Potential Mail Servers: 232
Email-Capable Domains and Hosts: 17,177
Live Hosts and Domains Not Parked: 21,469

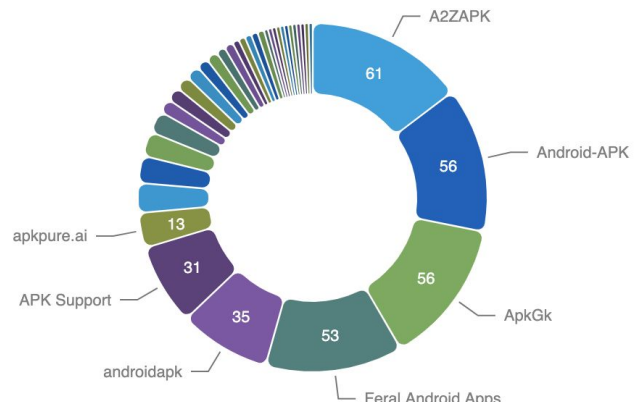## Mobile Apps

1. Apps in Official Stores: 229 (See Graph)
   a. Google Play Store: 114
   b. Apple App Store: 107
   c. Windows Phone: 7
   d. Amazon: 1

Apps on Official Stores

2. Apps in Secondary/Hybrid Stores: 399 (See Graph)

3. Blacklisted Mobile Apps by Store Type:
   a. Secondary: 16
   b. Hybrid: 1
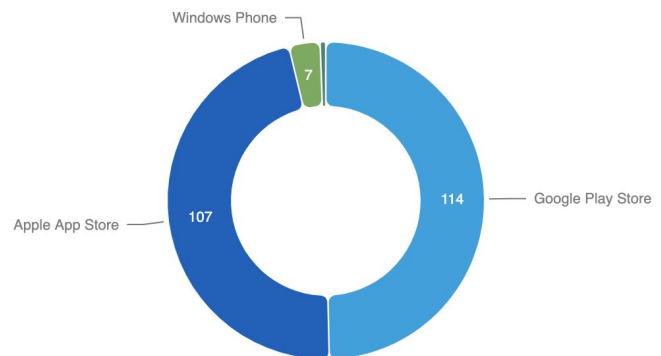
Apps on Secondary and Hybrid Stores by store

Facts and Figures at a Glance

Data is from [Johns Hopkins Coronavirus Resource Center](#).

Global

Total Cases: 1,033,478
Total Fatalities: 54,369
Countries w/ Confirmed Cases: 181

U.S.

Total Cases: 245,601
Total Fatalities: 6,058
Jurisdictions Reporting Cases: 54 (50 states, District of Columbia, Puerto Rico, Guam, and U.S. Virgin Islands)

Highest COVID-19 Case Count: U.S.

States
1. New York: 92,743
2. New Jersey: 25,590
3. California: 11,126

Counties
1. New York City (NY): 51,809
2. Westchester County (NY): 11,567
3. Nassau County (NY): 10,587
4. Suffolk County (NY): 8,746
5. Cook County (IL): 5,575
6. Wayne County (MI): 5,069
7. Bergen County (NJ): 4,099
8. Los Angeles County (CA): 4,045
9. Rockland County (NY): 3,751
10. Orleans Parish (LA): 3,148

Stay-At-Home/Shelter-In-Place Orders

State	Start	End	State	Start	End
California	03/19	TBD	New Hampshire	03/27	05/04
Illinois	03/21	04/30	Montana	03/28	04/10
New Jersey	03/21	TBD	Rhode Island	03/28	04/13
New York	03/22	TBD	Alaska	03/28	04/11
Connecticut	03/23	04/22	Kansas	03/30	04/19
Kentucky	03/23	TBD	North Carolina	03/30	04/29
Louisiana	03/23	04/13	Maryland	03/30	TBD
Ohio	03/23	04/06	Virginia	03/30	06/10
Oregon	03/23	TBD	Arizona	03/31	04/30
Washington	03/23	04/06	Tennessee	03/31	04/14
Delaware	03/24	05/15	Washington, DC	04/01	04/24
Indiana	03/24	04/06	Nevada	04/01	04/30
Michigan	03/24	04/13	Pennsylvania	04/01	04/30
New Mexico	03/24	04/10	Oklahoma	04/01	04/30
Massachusetts	03/24	05/04	Texas	04/02	04/30
West Virginia	03/24	TBD	Maine	04/02	04/30
Hawaii	03/25	04/30	Florida	04/03	04/30
Wisconsin	03/25	04/24	Georgia	04/03	04/13
Vermont	03/25	04/15	Mississippi	04/03	04/20
Idaho	03/25	04/15			
Colorado	03/26	04/11			
Minnesota	03/27	04/10			

Governmental Guidance

State & Local Governments

California

As of 04/03/2020, California has 11,126 confirmed COVID-19 cases and 244 deaths. Governor Newsom announced yesterday, 04/02/2020, a financial relief package for small businesses amid the COVID-19 pandemic. The package allows small businesses with less than $5 million in taxable sales to defer payment up to $50,000 for one year. Newson also announced a new job search tool for Californians who are out of work due to the pandemic.

Illinois

As of 04/03/2020, Illinois has 7,697 confirmed cases of COVID-19 and 167 deaths. Governor J.B. Pritzker announced Thursday, 04/02/2020, Illinois will receive 15 machines to process rapid results for COVID-19 tests. Pritzker stated the first shipment was expected Thursday night. These rapid tests, developed by North Chicago-based Abbott Labs, deliver positive results within five minutes and negative results within 13 minutes.

Massachusetts

As of 04/03/2020, Massachusetts has 8,966 confirmed cases of COVID-19 and 154 deaths. Governor Charlie Baker announced yesterday, 04/02/2020, Massachusetts will soon hit a peak in COVID-19 cases. Baker stated models show the peak is expected to hit between April 10 and April 20, with expected confirmed cases totaling between 47,000 and 172,000. Massachusetts officials are planning to prepare for the surge based on these models.

New York

As of 04/03/2020, New York has 9,243 confirmed COVID-19 cases and 2,468 deaths. Governor Cuomo stated Thursday, 04/02/2020, in a Press Conference that New York has a total of 2,200 ventilators. This stockpile is expected to last about six days at the current rate of the pandemic. Cuomo stated there are other measures in place if it is necessary, including transporting ventilators from hospitals.

Washington, DC

As of 04/03/2020, the Washington, D.C. region has a total of 4,580 confirmed COVID-19 cases with 1,706 in Virginia, 2,331 in Maryland, and 653 in the District. Washington D.C. is expected to hit its peak of COVID-19 cases around April 15. Mayor Muriel Bowser is expected to announce medical plans today to prepare for the surge. Maryland is expected to hit its surge around April 29, and Virginia is not expected to surge until May 20.

End Report