RISKIQ®

RiskIQ i3:

COVID-19 Daily Update
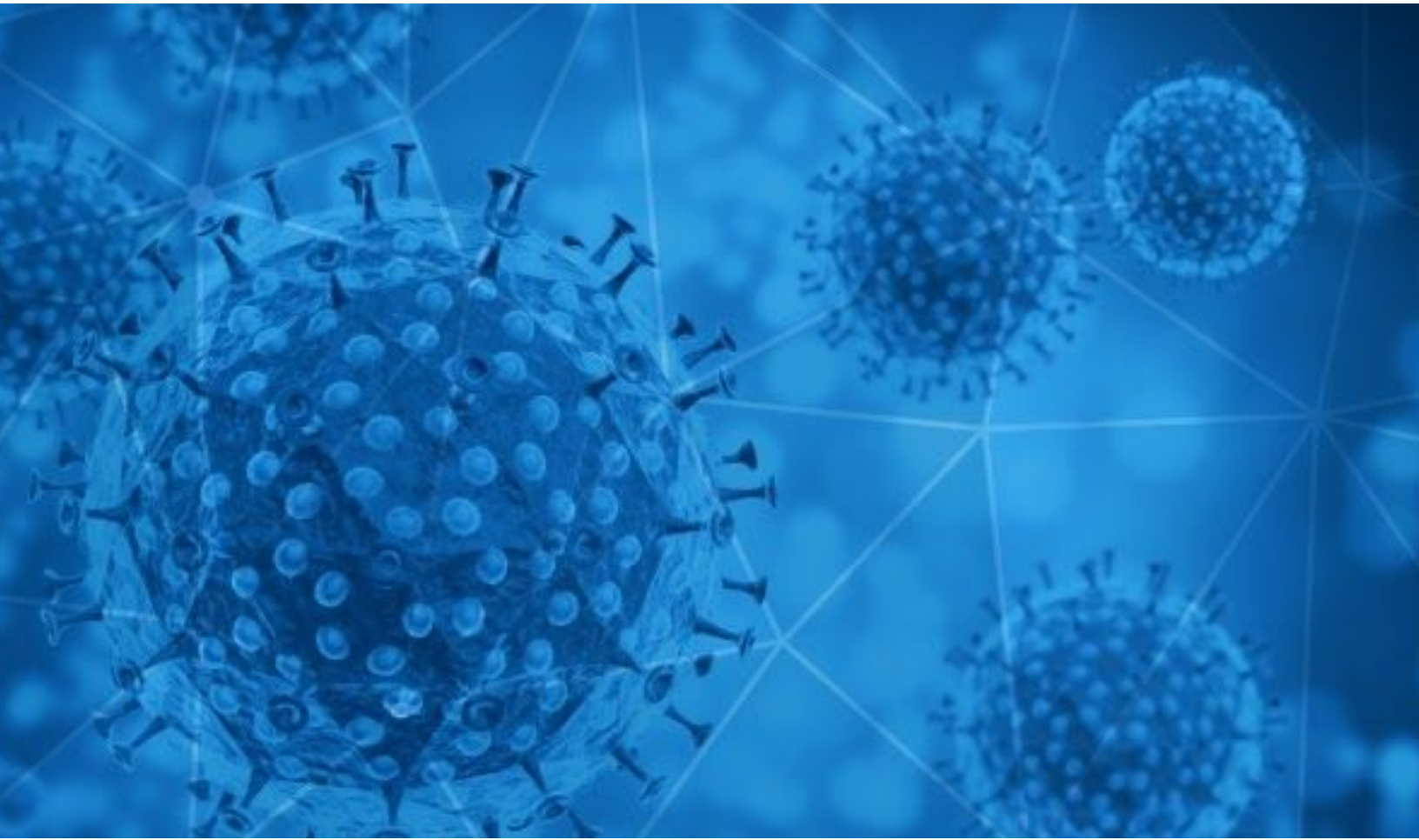
04/23/2020

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 in the Past 24 Hours

Las Vegas Mayor Carolyn Goodman called for the city's businesses to reopen, but did not provide any social distancing guidelines. Goodman further stated the responsibility to set safety guidelines and policies is on individual businesses, not the government.

Senate Majority Leader Mitch McConnell (R-KY) expressed a desire for businesses nationwide to reopen. In an interview with Fox News, McConnell said "all of us are going to be encouraging our states to begin to move in the direction of getting back to normal."

Oklahoma Governor Kevin Stitt said the state will begin reopening in phases since they have flattened the curve and have made progress in obtaining personal protective equipment. In phase one, everyone will be encouraged to follow social distancing guidelines, but only the elderly and otherwise at-risk individuals will be told to continue following social distancing guidelines in phase two.

Jeffrey Shaman, an epidemiologist at Columbia University, warned that it is not a matter of whether infections will increase after easing up on stay-at-home orders, but rather how much infections will increase. As many states move to relax or end stay-at-home restrictions, experts warn that such actions will likely lead to an increase in case numbers. Epidemiological models suggest the best strategy for reopening the country would be to push the case numbers as low as possible before easing restrictions, which would allow time to react during new case surges.

President Trump signed a proclamation that placed restrictions on immigration for sixty days. The order does not shut off applications for permanent residence, despite earlier claims it would do so. The order will block some entrants who do not already have visas or other travel documents, but will leave in place a number of exemptions for foreign workers and employers.

Dr. Anthony Fauci appeared to contradict President Trump after Trump suggested that the virus may not come back at all. Fauci stated the virus will be back in the fall, but stressed what happens with the resurgence of cases will be determined by how the country is able to contain the virus.

In a paper published in the Journal of the American Medical Association, researchers found that 20% of those hospitalized with COVID-19 in New York died from the disease. The researchers also found that 88% of patients placed on a ventilator died, which is about 8% higher than when patients were placed on ventilators prior to the COVID-19 pandemic.

Digital Exploitation

Zoom on 04/22/2020 announced a series of security improvements designed to address many of the concerns raised in recent weeks. Zoom reported that account administrators will be able to choose which data center regions they want to use for real-time meeting traffic. The vendor also said the upcoming Zoom 5.0, scheduled for release within the next week, will introduce AES 256-bit GCM encryption, which should provide better protection for meeting data.

Members of the Cyber Threat Coalition reported on 04/20/2020 a change in tactics from malicious actors that leverage the COVID-19 pandemic. As the US and European countries instituted social distancing measures, threat actors registered domains that included themes of the pandemic. Now, threat actors appear to be switching their focus to spreading scams, phishing, or malware and focusing on leveraging existing domains for more lucrative techniques, according to LookingGlass reporting.

Iran's Charming Kitten and other nation-state actors are using the coronavirus pandemic to their advantage, for espionage, according to ThreatPost reporting. According to Google's Threat Analysis Group (TAG), more than a dozen nation-state-backed APTs are using the COVID-19 pandemic as a cover for their various cyberespionage and malware activities.

Cybercriminals continue to tailor their attack methods to take advantage of fears stemming from the COVID-19 pandemic, targeting medical providers with directed email phishing attacks, according to Health IT Security reporting. Cyber attackers are launching double extortion ransomware, hijacking video conferencing, targeting Virtual Private Networks (VPNs), and ramping up business email compromise schemes and fraud attempts.

The Small Business Administration admitted their online application portal may have been compromised in late March affecting nearly 7,900 Economic Injury Disaster Loans. The information believed to be leaked includes applicants' social security numbers, contact information, addresses, and more. The issue has been addressed and the portal has been relaunched, according to LookingGlass reporting.

# New Blacklist Data

hxxp://covidhelptips[.]com/Covid-19updates/

hxxp://hardfastlife[.]com/rack/rackspace-Covid-19/racksp/

hxxp://thechristianwardrobe[.]us/Covid-19/Ontario/Governement/

hxxps://www[.]im4free[.]com/wp-admin/Quarantine/Covid-19/Rich/main/

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 04/22/2020-04/23/2020. During this period, RiskIQ analyzed 121,539 spam emails containing either "*corona*" or "*covid*" in the subject line. There were 15,655 unique subject lines observed during the reporting period. The spam emails originated from 20,927 unique sending email domains and 11,718 unique SMTP IP Addresses. Analysts identified 0 email which sent an executable file for Windows machines.
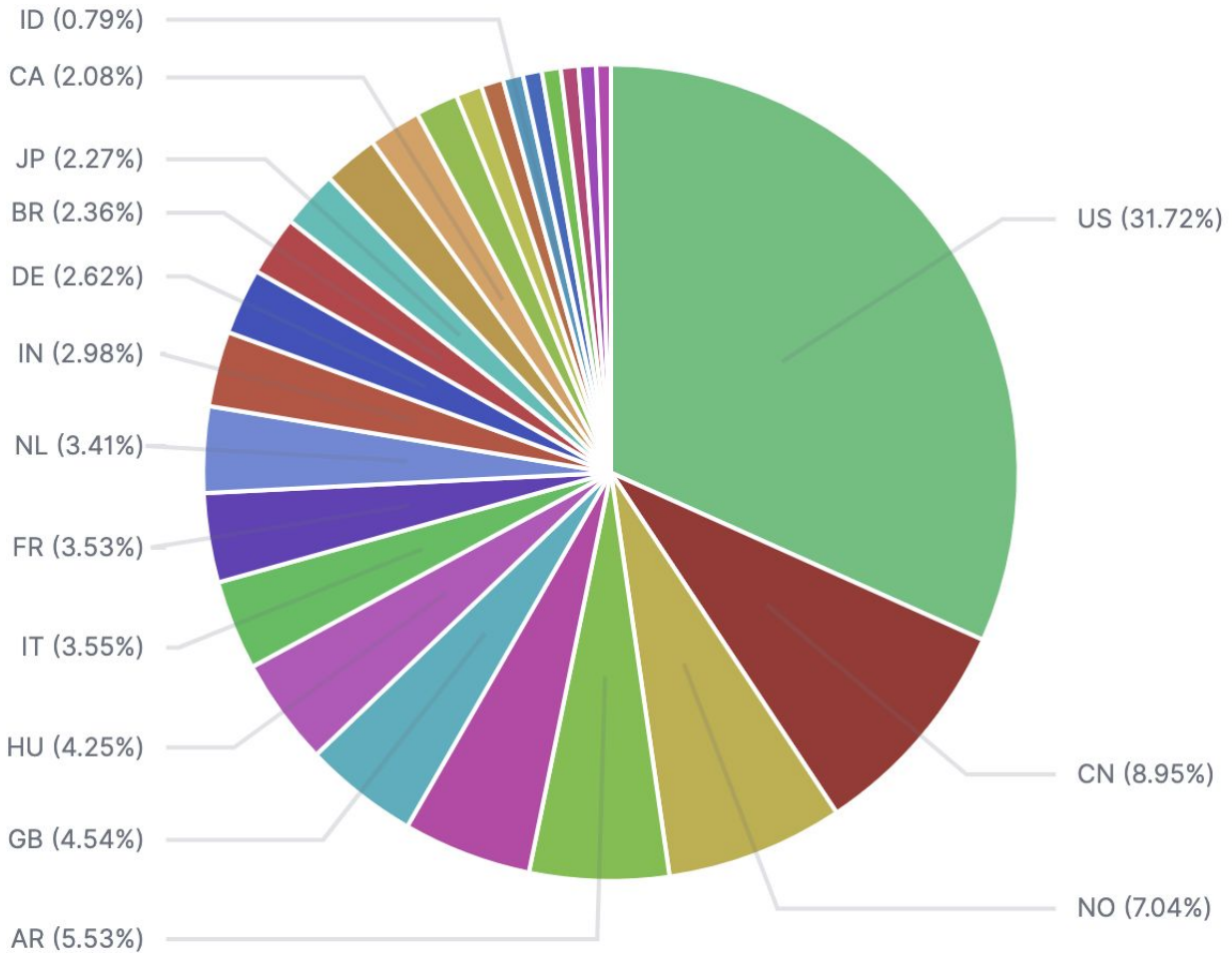
Spam emails by country of origin
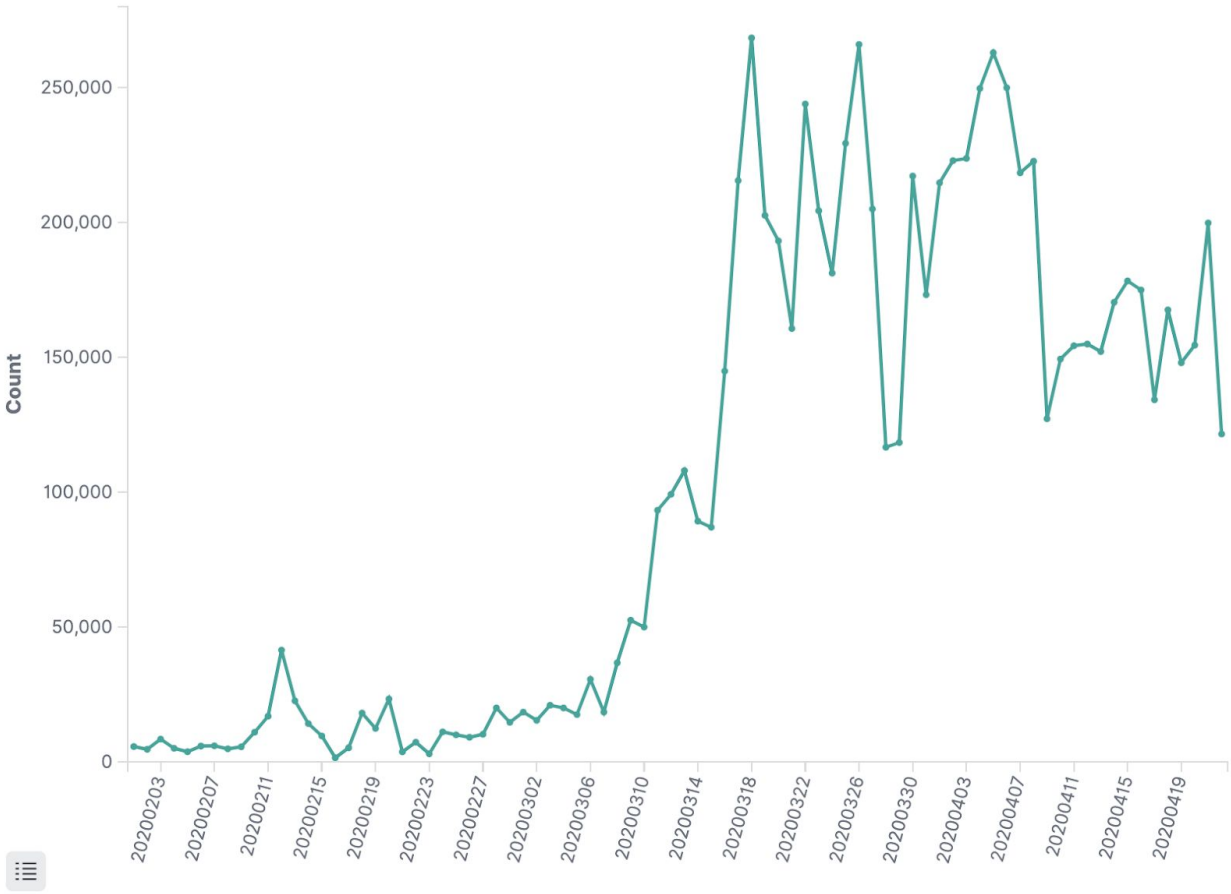
Spam emails by volume since February 1, 2020

Top 25 Subjects

1. 11,524 - Protection From Corona Virus With Immunity Oil

2. 7,900 - The Mask that can prevent Coronavirus now

3. 3,973 - ATTENTION COVID-19 STIMULUS PACKAGE GRANT

4. 3,961 - coronavirus.mascarilla de proteccion facial

5. 3,910 - Coronavirus is spreading, this specialized mask can control it

6. 3,477 - COVID-19 STIMULUS PACKAGE GRANT BENEFICIARY

7. 3,400 - Welche Maske sollten Sie gegen das Coronavirus tragen? Hier die Informationen und alles Wissenswerte

8. 3,397 - Spende fï¿½r Covid 19-Pandemie

9. 2,533 - COVID-19 pandemic outbreak

10. 2,399 - This Mask Stops Coronavirus

11. 1,676 - Corona: Die Maskenpflicht kommt!

12. 1,512 - Spende fï¿½r die Covid-19-Pandemie

13. 1,494 - COVID-19 Face Mask & Safety Products

14. 1,227 - Day 3: Covid-19 Stay-at-Home Puzzle Challenge + New JAMB notice to candidates

15. 1,145 - The COVID-19 Solidarity Response Fund

16. 1,141 - COVID19 Offer -85%

17. 1,092 - The Corona Letter: China is failing the world

18. 885 - Achtung, Jetzt Corona-Schutzmasken bestellen - sicher gegen Corona!

19. 856 - Covid-19 เราต้องรอด! กับบริการทำความสะอาดและฆ่าเชื้อเพื่อลดความเสี่ยง

20. 831 - COVID-19 Update: Critical information for [REDACTED_DOMAIN] Users

21. 802 - Redeem Your SBSA-COVID-19-Financial Relief Today

22. 799 - bit-tech Newsletter - March Case Modding update, Fractal Giveaway (enter now!), AMD donating EPYCs for Covid19 battle, palm sized Chuwi Win10 PC

23. 754 - Re: Personal & Business Funding (COVID-19)

24. 750 - Supplies for counter COVID-19 virus

25. 749 - SCAM VICTIMS/CORONA VIRUS PALLIATIVES

Top 10 IP Addresses

1. 7,450 - 82.134.25.158
2. 4,916 - 61.92.142.142
3. 3,961 - 181.22.3.165
4. 2,532 - 178.239.161.164
5. 1,230 - 184.107.73.137
6. 1,116 - 80.211.174.185
7. 1,052 - 23.254.209.146
8. 896 - 52.41.228.65
9. 876 - 217.112.128.146
10. 838 - 112.16.5.62

Top 10 Domains (RDNS)

1. 7,450 - 158.82-134-25.bkkb.no
2. 4,916 - 061092142142.static.ctinets.com
3. 3,961 - 181-22-3-165.speedy.com.ar
4. 2,532 - 164.161.239.178.baremetal.zare.com
5. 1,230 - host.webworksnigeria.com
6. 1,116 - srv185.venitas.lt
7. 1,052 - hwsrv-718421.hostwindsdns.com
8. 896 - ec2-52-41-228-65.us-west-2.compute.amazonaws.com
9. 876 - dream.kranbery.com
10. 833 - mail.thaiticketmajor.net

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

None

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

1. 33,690 US
2. 9,504 CN
3. 7,474 NO
4. 5,872 AR
5. 5,412 HK
6. 4,819 GB
7. 4,519 HU
8. 3,772 IT
9. 3,755 FR
10. 3,625 NL
11. 3,169 IN
12. 2,782 DE
13. 2,509 BR

14. 2,416 JP
15. 2,327 RU
16. 2,207 CA
17. 1,791 TH
18. 1,098 ES
19. 944 UA
20. 844 ID
21. 803 ZA
22. 794 PH
23. 748 PL
24. 733 CO
25. 614 EC

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: 69,223
Hosts: 79,033
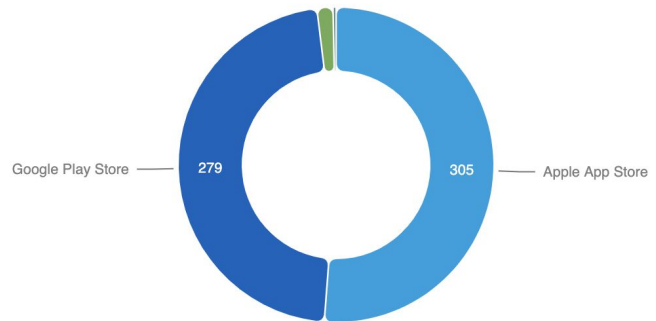Hosts and Domains with Potential Mail Servers: 281
Email-Capable Domains and Hosts: 25,391
Live Hosts and Domains Not Parked: 31,877

Mobile Apps

1. Apps in Official Stores:
   (See Graph)
      a. Google Play Store: 279
      b. Apple App Store: 305
      c. Windows Phone: 9
      d. Amazon: 1
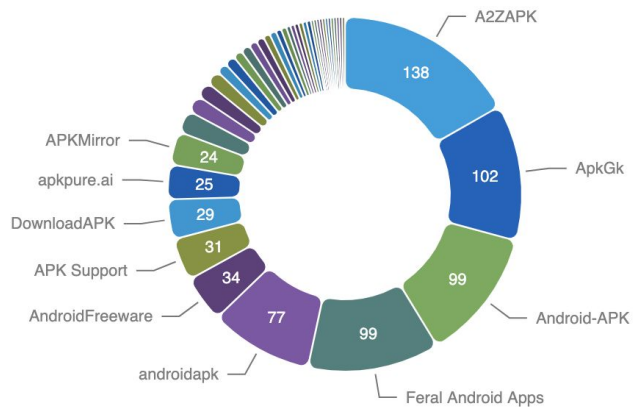
Apps on Official Stores

2. Apps in Secondary/Hybrid Stores: 781 (See Graph)

3. Blacklisted Mobile Apps by Store Type:
      a. Secondary: 28
      b. Hybrid: 1
      c. Official: 2

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: 2,649,680
Total Fatalities: 184,643
Countries w/ Confirmed Cases: 185

U.S.

Total Tests Conducted: 4,482,434
Total Cases: 842,624
Total Fatalities: 46,785
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: 263,754
2. New Jersey: 95,914
3. Massachusetts: 42,944

Counties

1. New York City (NY): 147,297
2. Nassau County (NY): 31,555
3. Suffolk County (NY): 28,854
4. Westchester County (NY): 25,276
5. Cook County (IL): 24,546
6. Los Angeles County (CA): 16,449
7. Wayne County (MI): 14,561
8. Bergen County (NJ): 13,686
9. Hudson County (NJ): 12,088
10. Essex County (NJ): 11,387

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	04/24
New Jersey	03/21	TBD	Rhode Island	03/28	05/08
New York	03/22	05/15	Kansas	03/30	05/03
Connecticut	03/23	05/20	North Carolina	03/30	04/29
Kentucky	03/23	TBD	Maryland	03/30	TBD
Louisiana	03/23	04/30	Virginia	03/30	06/10
Ohio	03/23	05/01	Arizona	03/31	04/30
Oregon	03/23	TBD	Tennessee	03/31	04/30
Washington	03/23	05/04	Washington, DC	04/01	05/15
Delaware	03/24	05/15	Nevada	04/01	04/30
Indiana	03/24	05/01	Pennsylvania	04/01	04/30
Michigan	03/24	04/30	Oklahoma	04/01	04/30
New Mexico	03/24	04/30	Texas	04/02	04/30
Massachusetts	03/24	05/04	Maine	04/02	04/30
West Virginia	03/24	TBD	Florida	04/03	04/30
Hawaii	03/25	04/30	Georgia	04/03	04/30
Wisconsin	03/25	05/26	Mississippi	04/03	04/27
Vermont	03/25	05/15	Alabama	04/04	04/30
Idaho	03/25	04/30	Missouri	04/06	05/03
Colorado	03/26	04/26	South Carolina	04/07	TBD
Minnesota	03/27	05/04			

Governmental Guidance

State & Local Governments

California

As of 04/23/2020, California has 37,710 confirmed cases of COVID-19, with 1,440 deaths. Governor Gavin Newsom gave an update Wednesday on efforts to eventually reopen California's economy and begin to ease shelter-in-place restrictions. Governor Newsom focused his remarks on the need to dramatically expand testing before the state would see widespread reopening.

Illinois

As of 04/23/2020, Illinois has 35,109 confirmed cases of COVID-19, with 1,565 deaths. On Thursday, Evanston joined nearly 20 suburbs requiring masks or face coverings to be worn in public to help prevent the spread of COVID-19. The Evanston order goes into effect at 8 a.m., and requires all persons working in essential businesses and operations to wear face coverings. The order does list some exceptions, which can be found here.

New York

As of 04/23/2020, New York has 263,754 confirmed cases of COVID-19, with 19,453 deaths. Seven more big cats at the Bronx Zoo have tested positive for the novel coronavirus after a tiger at the zoo contracted the virus, according to wildlife officials. Officials say four more tigers and three African lions tested positive for COVID-19, according to the Wildlife Conservation Society, which runs the zoo.

Texas

As of 04/23/2020, Texas has 21,774 confirmed cases of COVID-19 and 569 deaths. The first Walmart coronavirus testing site in Texas will be in Lubbock and is scheduled to open Friday. Walmart has 12 testing locations open in Chicago, Shreveport, Albuquerque and in Bentonville, Ark., where it's headquartered. Walmart plans to have more than 20 sites in at least 10 states

by the end of April. The retailer is partnering with Quest Labs and the U.S. Department of Health and Human Services to set up the locations.

Washington, DC

As of 04/23/2020, the Washington, D.C. region has a total of 28,247 confirmed cases of COVID-19, with 14,775 in Maryland, 10,266 in Virginia, and 3,206 in the District. The District of Columbia has a total of 127 deaths, Virginia has 349 deaths, and Maryland has 698 deaths.

D.C. Mayor Muriel E. Bowser expressed alarm Wednesday about the harsh impact of the novel coronavirus on the poor, sick and elderly in the nation's capital, as officials reported 15 new fatalities. Gov. Bowser is urging older residents and those who live in long-term-care facilities or group homes to get tested if they feel ill, particularly if they have underlying health problems. Officials are also expanding the criteria for testing to include people without symptoms who are in high-risk groups and likely to have been exposed.

End Report