



RiskIQ i3:

COVID-19 Daily Update

04/21/2020

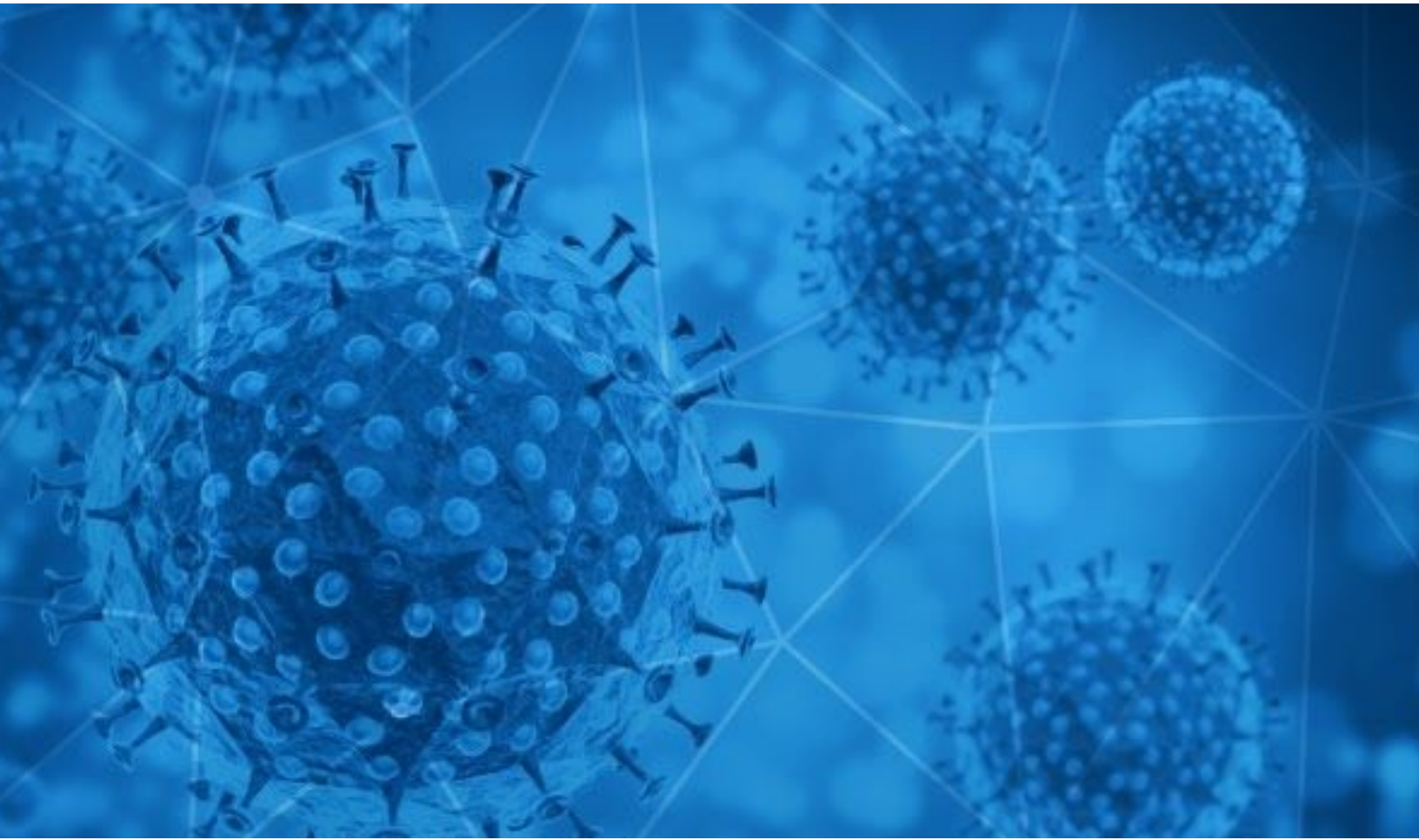


Table of Contents

Methodology	3
Disclaimer	3
Notable Events in the Past 24 Hours	4
Digital Exploitation	6
COVID-19 Email Spam Statistics	8
COVID-19 Host, Domain, and Mobile App Tracking	13
Facts and Figures at a Glance	14
Global	14
U.S.	14
Highest COVID-19 Case Count: U.S.	14
Stay-At-Home/Shelter-In-Place Orders	15
Governmental Guidance	16
State & Local Governments	16

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

The Senate passed a roughly [\\$480 billion relief package](#) that includes hundreds of billions of dollars in new funding for small businesses hurt by the coronavirus outbreak along with other priorities like money for hospitals and expanded Covid-19 testing. The bill goes to the House, which is expected to vote on the package Thursday.

Researchers from the [University of Virginia](#) suggested that COVID-19 cases in Virginia could peak in mid-August, and the total case numbers may be higher than originally anticipated. Governor Ralph Northam warned that the model shows easing social distancing measures prematurely could overburden the state's healthcare system.

The state of Missouri filed a [federal lawsuit against the Chinese government](#) over the coronavirus, alleging that nation's officials are to blame for the global pandemic. The lawsuit alleges Chinese officials are "responsible for the enormous death, suffering, and economic losses they inflicted on the world, including Missourians."

The US Food and Drug Administration issued the first authorization for an [at-home COVID-19 test kit](#). LabCorp, the diagnostics company producing the tests, says it will give first access to health care workers and first responders. With this test, people who are eligible can collect a fluid sample, but they will still need to send it to a lab for testing. The test costs \$119.

Companies are [suspending or terminating business agreements](#) by leveraging force-majeure clauses, which typically spell out how extraordinary circumstances beyond one's control can nullify an agreement. Force-majeure declarations do not guarantee a speedy resolution to contract disputes, as many such cases have now been brought to court.

Many Americans are confused by the [relief payments](#) from the Internal Revenue Service (IRS). More than 80 million Americans have received funds provided by the CARES Act; however, millions more still await payment. One source of confusion stems from whether an individual leveraged a tax refund anticipation loan when they filed their taxes, which would route the payment to a temporary bank account instead of their personal account.

The House of Representatives is set to vote this week on [changing rules](#) for voting by proxy during the pandemic. Under the proposed rule change, absent members would be able to relay their vote to a member who is physically present on the floor, who would then place the vote on their behalf.

A Hill-HarrisX poll released Monday found that 74% of Americans [fear losing freedoms](#) during the COVID-19 pandemic. Still, more respondents—83%—fear becoming infected with

COVID-19. About 73% of respondents said they feared going to the hospital, and 48% reported fearing losing their jobs.

Facebook CEO Mark Zuckerberg said on Monday the platform would consider stay-at-home protests organized on Facebook as “[harmful misinformation](#)”, provided they violate social distancing guidelines. Zuckerberg said the social media platform would remove such posts and events, but would otherwise allow users to debate policies relating to stay-at-home orders.

President Trump announced on Twitter he would sign an executive order which will [suspend immigration](#). Trump did not clarify when the prohibition would go into effect or how long it would last.

WHO Director-General [Tedros Adhanom Ghebreyesus](#) cautioned leaders that the “worst is yet ahead of us.” Tedros added that the virus is a “dangerous combination,” comparing it to the 1918 Spanish Flu pandemic.

NFL team owner Jeffrey Lurie and the Philadelphia Eagles are [donating \\$1 million](#) to COVID-19 relief effort.

Digital Exploitation

The Federal Trade Commission on 04/20/2020 offered guidance for avoiding coronavirus [stimulus payment scams](#) including: only use irs.gov/coronavirus to submit information to the IRS; don't respond to anyone posing as an IRS representative via phone, email, text message, or social media; don't pay anyone to get your stimulus money for you; and, don't respond to anyone claiming you have to return money because your stimulus payment was more than what was owed you.

The Federal Bureau of Investigation on 04/21/2020 alerted medical providers to targeted email phishing attempts which leverage email subject lines and content related to COVID-19 in order to distribute malicious attachments. The attachments exploit Microsoft Word Document files, 7-zip compressed files, Microsoft Visual Basic Script, Java, and Microsoft Executables.

Related, hackers have deployed [ransomware](#) on U.S. hospital and government systems using stolen Active Directory credentials, according to Bleeping Computer. The attacks occurred months after exploiting a known remote code execution (RCE) vulnerability in their Pulse Secure VPN servers. Even though the vulnerability tracked as CVE-2019-11510 was patched by Pulse Secure last year, the U.S. Cybersecurity and Infrastructure Security Agency reminded organizations in January 2020 to patch their Pulse Secure VPN servers against ongoing attacks.

Hackers are sending emails offering COVID-19 testing but are encrypted with hidden tracking malware called "[Trickbot](#)" which is engineered to record passwords and bank data, according to Microsoft Security Intelligence. According to Microsoft Security, 60,000 of the malware-laden emails are stopped daily before they can attack an unwary recipient.

The '[Covid19 Alert](#)' mobile application leaks user data. Experts found the issue after its code was published online on 04/18/2020. The source files included a database from another application that was part of a project of the software house Immotef, which contains data from Dutch users of that app, according to Security Affairs reporting.

Within minutes of the U.K. government's furlough plan going live, it was targeted by [hackers](#) impersonating HM Revenue and Customs, the country's tax collection agency. According to CNBC reporting, hundreds of phishing emails landed in people's inboxes inviting them to click on a link that takes them to what looks like an HMRC furlough claim website. The fraudulent website asks people to fill in their personal, card and bank account details. But instead of going to HMRC, the details go to the hackers.

New Blacklist Data

hxxp://nxt27893[.]nextadmin[.]hu/wp-content/plugins/salem/amex/American-Express-Covid-19-Stay-at-home/home/

hxxps://taikisushi[.]com/COVID-19/

hxxp://www[.]covid-19-uk-relieve[.]com/

hxxp://jayalbertandassociates[.]com/sector/who/COVID-19/

hxxp://www[.]interacservcovid-19[.]com/

hxxp://COVID-19-shop[.]rf[.]gd/?ebay[.]co[.]uk/VAT

hxxp://freeeasy-life[.]com/en/wordpress/wp-includes/Covid-19/onedrive4D/

hxxp://clearvale53[.]com/amex/American-Express-Covid-19-Stay-at-home/home/

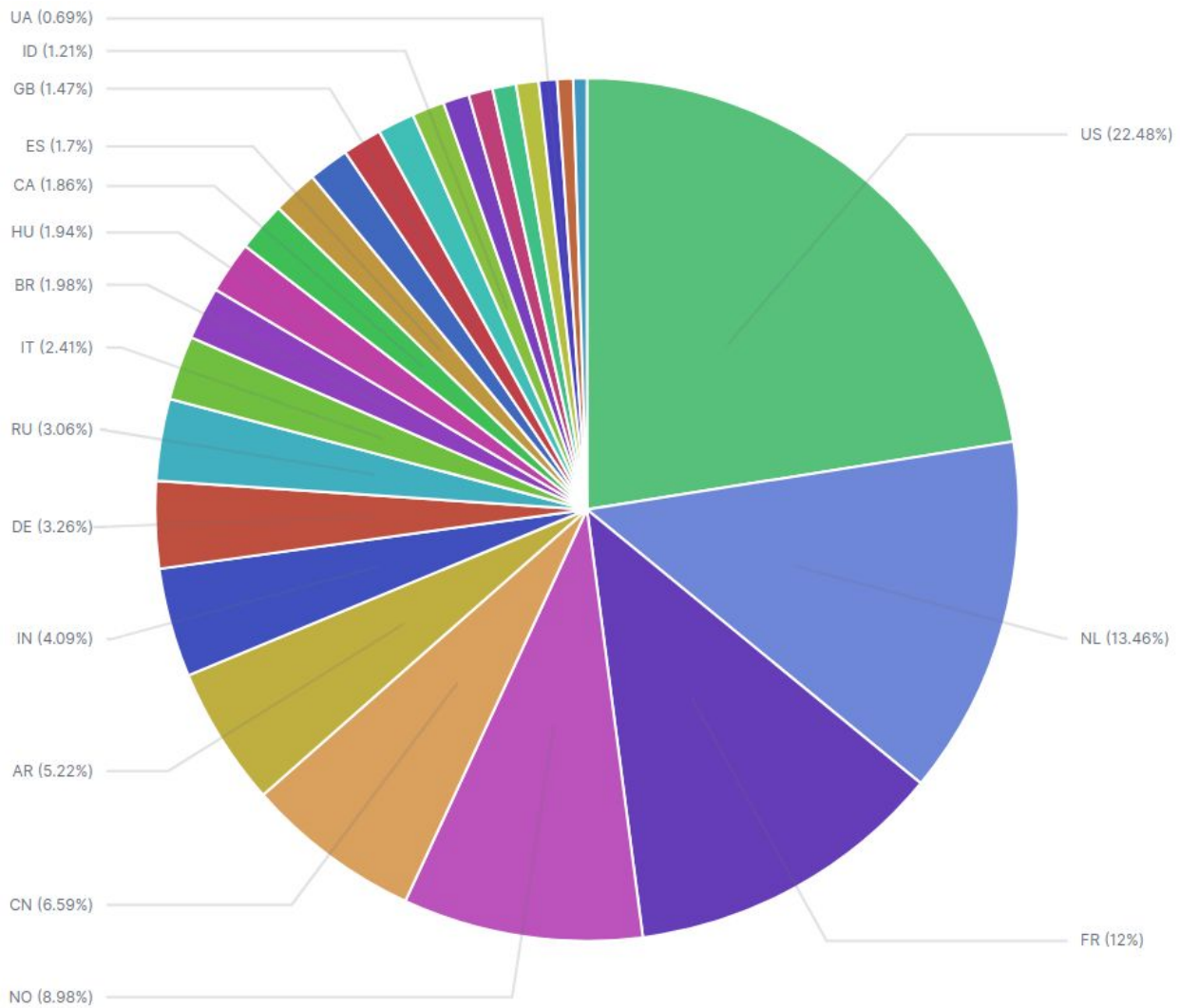
hxxp://www[.]plantingvelve[.]com/UpdatesCOVID-19/

hxxps://rijosfoods[.]com[.]br/Covid-19/Gouvernement/

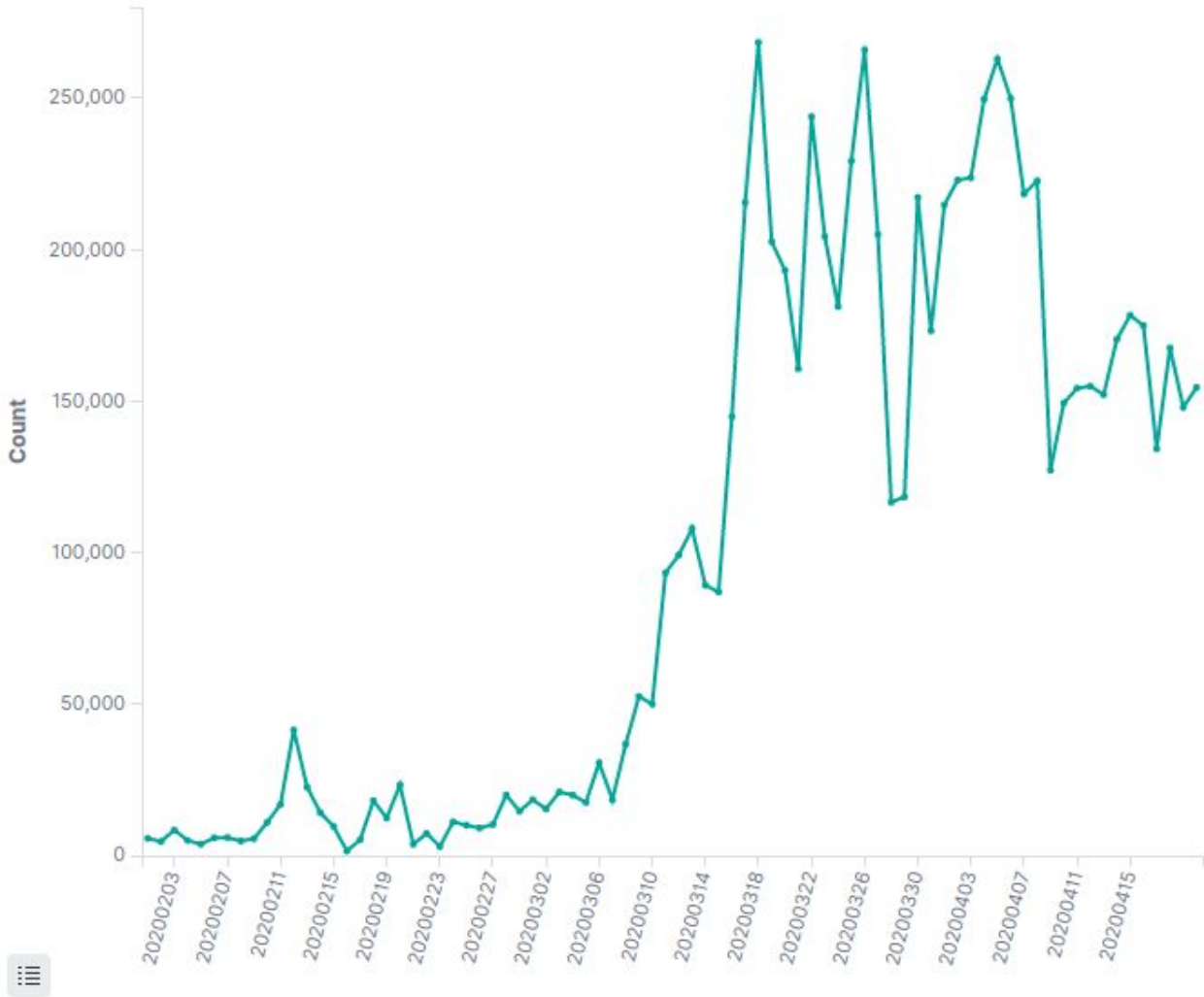
hxxps://covid-19update[.]zap515988-1[.]plesk10[.]zap-webspace[.]com/QWE/CDI/

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 04/20/2020-04/21/2020. During this period, RiskIQ analyzed 154,477 spam emails containing either “*corona*” or “*covid*” in the subject line. There were 15,453 unique subject lines observed during the reporting period. The spam emails originated from 8,085 unique sending email domains and 16,005 unique SMTP IP Addresses. Analysts identified 8 emails 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. 10,930 - Achtung, Jetzt Corona-Schutzmasken bestellen - sicher gegen Corona!
2. 10,299 - COVID-19 STIMULUS PACKAGE GRANT BENEFICIARY
3. 6,577 - The Mask that can prevent Coronavirus now
4. 6,224 - RE:COVID-19 IgM - IgG Test Quotation
5. 4,299 - COVID-19 Face Mask & Safety Products
6. 4,184 - coronavirus.mascarilla de proteccion facial
7. 3,392 - The Corona Letter: An answer to outbreak's unknowns
8. 3,255 - Coronavirus is spreading, this specialized mask can control it
9. 2438 Welche Maske sollten Sie gegen das Coronavirus tragen? Hier die Informationen und alle - s Wissenswerte
10. 2,401 - Spende fir Covid 19-Pandemie
11. 2,110 - Re: Payee advise : Updated value date due to COVID-19 Lockdown
12. 2,071 - This Mask Stops Coronavirus
13. 2,025 - Account Alert: Due To The Covid-19 Epidemic Review Your Accounts
14. 2005 (Quick delivery/Today's quotation) Protective mask and Diagnostic kit for C,OVI - D-19, goggles, infrared thermometer, protective clothing
15. 1,685 - Covid-19: ampliato l'intervento di MSF
16. 1,643 - ATTN: COVID-19 STIMULUS PACKAGE GRANT BENEFICIARY
17. 1,538 - COVID19 Offer -85%
18. 1,253 - Covid-19 Stay-at-Home Puzzle Challenge Begins - Enter Now
19. 1124 Don't let the COVID19 stop you. Learn free information about unemployment assistance.
20. 1,122 - Standard Bank Fee: COVID-19 Payment Relief Funds Approved
21. 1,108 - Be prepared. Use our unemployment guide to help during the COVID19 crisis
22. 1,107 - COVID-19 Asesoramiento contable para tu empresa
23. 1,098 - ATENCION COVID-19 Estudio Contable, Legal e Impositivo para tu negocio
24. 1,096 - Need Unemployment information because of the coronavirus?
25. 1,095 - Are you prepared for a potential job loss due to COVID19

Top 10 IP Addresses

1. 11,943 - 82.134.25.158
2. 10,767 - 51.15.102.215
3. 7,443 - 37.48.73.99
4. 6,224 - 95.211.209.158
5. 2,976 - 5.79.113.225
6. 2,401 - 72.172.137.80
7. 2,108 - 185.118.166.203
8. 1,894 - 181.22.2.233
9. 1,764 - 181.22.2.47
10. 1,578 - 81.95.112.26

Top 10 Domains (RDNS)

1. 12,127 - 158.82-134-25.bkkb.no
2. 11,107 - tele2.nl
3. 7,582 - Masken-Shopping-heute.live
4. 7,305 - Masken-Kaufen-heute.live
5. 6,349 - vps02.snhostings.com
6. 5,273 - omp.pharmacy.cvs.com
7. 3,952 - ambercattle.icu
8. 3,044 - Masken-Shopping-live.live
9. 2,593 - host-193.17.6.197.routergate.com
10. 2,402 - s80.n137.n172.n72.static.myhostcenter.net

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

1. 6 - COVID-19 UPDATE // MSC SINGAPORE BUSINESS CONTINUITY PLAN ANNOUNCEMENT
2. 1 - Presupuesto para productos Anti COVID-19
3. 1 - COVID-19 UPDATE // MSC AUSTRALIAN BUSINESS CONTINUITY PLAN ANNOUNCEMENT

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

- | | |
|--------------|--------------|
| 1. 30,112 US | 14. 2,280 ES |
| 2. 18,039 NL | 15. 2,033 BE |
| 3. 16,082 FR | 16. 1,972 GB |
| 4. 12,038 NO | 17. 1,854 VN |
| 5. 8,833 CN | 18. 1,626 ID |
| 6. 6,995 AR | 19. 1,309 PL |
| 7. 5,480 IN | 20. 1,212 KR |
| 8. 4,370 DE | 21. 1,181 TR |
| 9. 4,103 RU | 22. 1,130 JP |
| 10. 3,223 IT | 23. 922 UA |
| 11. 2,660 BR | 24. 791 ZA |
| 12. 2,600 HU | 25. 686 CO |
| 13. 2,494 CA | |

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: 67,615

Hosts: 77,287

Hosts and Domains with Potential Mail Servers: 277

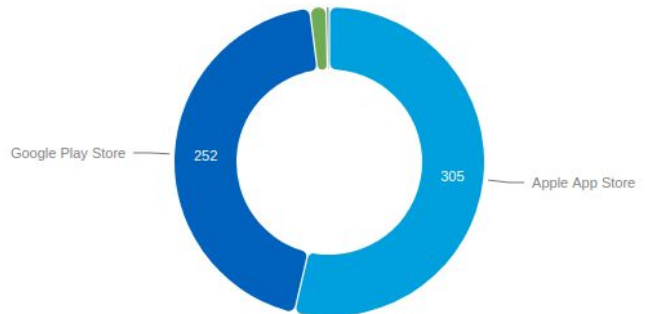
Email-Capable Domains and Hosts: 24,860

Live Hosts and Domains Not Parked: 31,921

Mobile Apps

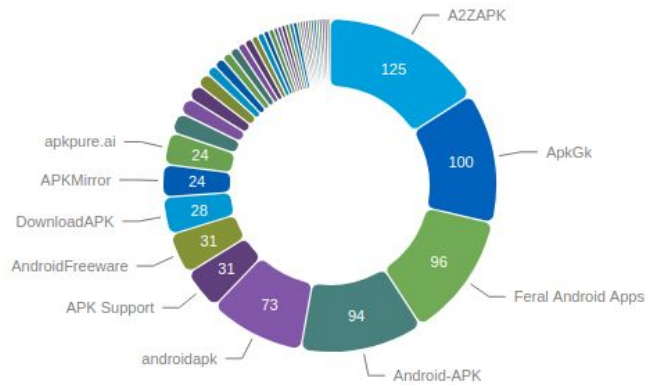
1. Apps in Official Stores:
 (See Graph)
 - a. Google Play Store: 252
 - b. Apple App Store: 305
 - c. Windows Phone: 9
 - d. Amazon: 1

Apps on Official Stores



2. Apps in Secondary/Hybrid Stores: 748 (See Graph)

Apps on Secondary and Hybrid Stores by store



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

Facts and Figures at a Glance

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

Global

Total Cases: 2,499,723
Total Fatalities: 171,718
Countries w/ Confirmed Cases: 185

U.S.

Total Tests Conducted: 4,026,572
Total Cases: 787,960
Total Fatalities: 42,374
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: 253,400
2. New Jersey: 88,806
3. Massachusetts: 39,643

Counties

1. New York City (NY): 141,235
2. Nassau County (NY): 30,677
3. Suffolk County (NY): 28,332
4. Westchester County (NY): 24,306
5. Cook County (IL): 22,101
6. Wayne County (MI): 13,912
7. Los Angeles County (CA): 13,823
8. Bergen County (NJ): 13,011
9. Hudson County (NJ): 11,221
10. Essex County (NJ): 10,729

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

State	Start	End	State	Start	End
California	03/19	TBD	Montana	03/28	04/24
Illinois	03/21	04/30	Rhode Island	03/28	05/08
New Jersey	03/21	TBD	Alaska	03/28	04/21
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	05/13
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			
New Hampshire	03/27	05/04			

Governmental Guidance

State & Local Governments

California

As of 04/21/2020, California has 33,866 confirmed cases of COVID-19, with 1,229 deaths. Protesters [rallied](#) around the State Capitol on Monday afternoon in a push to lift stay-at-home restrictions. The group received a protest permit for the event and encouraged participants to drive around the Capitol in their cars and honk their horns. They said they did not want people to walk there or get out of their vehicles. However, video showed groups of people clustered together outside and holding signs in defiance. A majority of people were not wearing masks or practicing physical distancing. Similar demonstrations have happened in other U.S. cities in recent days.

Illinois

As of 04/21/2020, Illinois has 31,508 confirmed cases of COVID-19, with 1,349 deaths. Battelle, a nonprofit research firm in Waukegan, has [developed](#) a system to sterilize N95 masks for up to 20 reuses at a rate of up to 80,000 masks a day, company officials said.

New York

As of 04/21/2020, New York has 253,400 confirmed cases of COVID-19, with 18,653 deaths. The Metropolitan Transportation Authority [says](#) its subway service should soon be back on track, as its workforce continues to recover. More than 5,000 MTA employees have returned to work, while more than 4,000 are still in quarantine. Since the pandemic started, nearly 3,000 workers have tested positive for COVID-19.

Texas

As of 04/21/2020, Texas has 20,087 confirmed cases of COVID-19 and 520 deaths. Governor Greg Abbott [announced](#) Monday that 1,200 members of the Texas National Guard will be mobilized throughout the state to operate mobile coronavirus testing sites. In total, 25 teams will be deployed to locations based on an assessment by the Texas Department of State Health Services. Each site will each initially be able to test 150 people per day.

Washington, DC

As of 04/21/2020, the Washington, D.C. region has a total of 25,601 confirmed cases of COVID-19, with 13,684 in Maryland, 8,990 in Virginia and 2,927 in the District. The District of Columbia has a total of 105 deaths, Virginia has 300 deaths, and Maryland has 582 deaths. Maryland has [obtained](#) 500,000 tests from LabGenomics in South Korea following weeks of negotiations, Governor Larry Hogan confirmed on Monday. The governor added that he would release his plan to reopen the state later this week, and he emphasized these additional tests will play a vital role in safely restarting the economy.

End Report