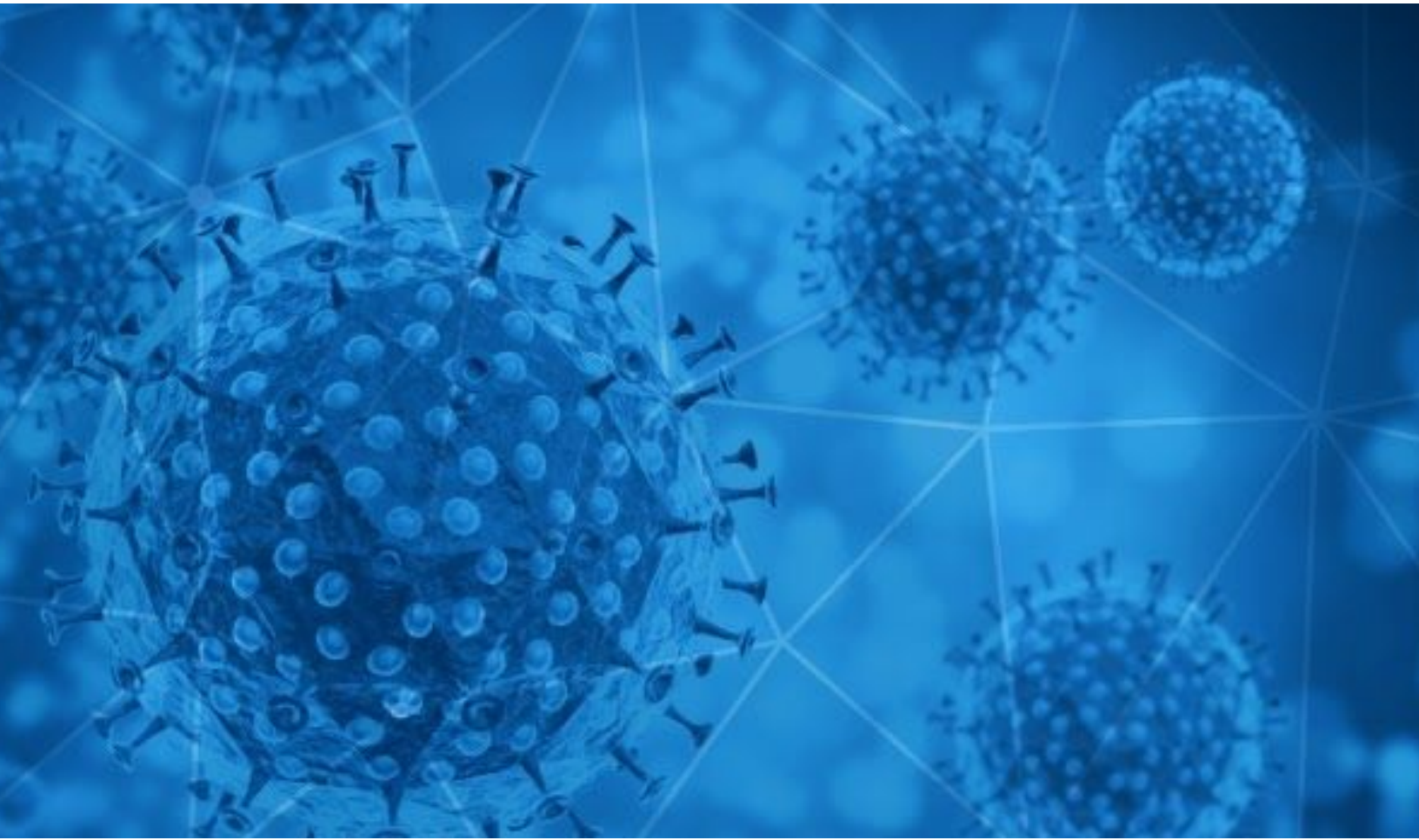
RISKIQ®

RiskIQ i3:

COVID-19 Daily Update

05/14/2020



RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

Table of Contents

RiskIQ
22 Battery, 10th Floor
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. Customer agrees that RiskIQ shall not have any liability resulting from Customer's use of this information.

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

Notice

RiskIQ will be changing the format and frequency of the COVID-19 Daily Update beginning Friday, 05/15/2020. The report will be released every Friday rather than every day. The report will compile the week's major stories and events and present them in the Notable Events and Digital Exploitation sections. RiskIQ has established a microsite for COVID-19 coverage, located at https://www.riskiq.com/covid19-cybersecurity/. Thank you for your continued readership.

Notable Events in the Past 24 Hours

Some countries that have opened up are closing down again as cases of COVID-19 spike. Lebanon ordered a four-day, near-complete lockdown to give officials time to assess the recent spike in cases. South Korea reversed course on allowing bars and clubs to reopen as the President warned citizens to brace for the second wave of the pandemic. Germany is warning that there may need to be renewed restrictions in areas with localized spikes in cases. Conversely, some countries, such as India and Russia, are easing lockdown restrictions despite evidence the disease is on the rise.

Moncef Slaoui has been selected to lead President Trump's "Operation Warp Speed" effort to develop a vaccine. Army General Gustave Perna has been selected to be the chief operating officer overseeing logistics. The vaccine development goal is to make 100 million doses available by November, 200 million doses available by December, and 300 million doses available by January. However, Dr. Anthony Fauci told Congress on Tuesday that a vaccine could possibly be developed in a year or two.

A report released by the U.N. warns of a looming mental illness crisis as millions of people cope with death and disease and face isolation, poverty, and anxiety caused by the pandemic. The report highlighted sections of people who are more at-risk of adverse mental health consequences, such as children and young people isolated from friends, and healthcare workers dealing with the disease.

On Thursday, whistleblower Rick Bright told a U.S. House of Representatives panel that the country could face its "darkest winter" of recent times if the pandemic response does not improve. Bright said he feared the pandemic would be prolonged and worsened if the nation does not improve its response, further stating that, "our window of opportunity is closing."

Senator Richard Burr (R-NC) has stepped aside as Chairman of the Senate Intelligence Committee. Burr reportedly turned his phone over to FBI agents after they served a search warrant on his residence. The warrant is part of a Justice Department investigation into Burr potentially selling millions of dollars in stocks after attending coronavirus briefings. Senator Dianne Feinstein (D-CA) was questioned last month about the sale of stocks, which Feinstein says have been in a blind trust since she came to the Senate. Sen. Kelly Loeffler (R-Ga.), who also sold stocks early in the pandemic, did not give a response to if she was questioned by the FBI.

Digital Exploitation

Research by VMware Carbon Black shows that the coronavirus pandemic is correlated with a 238% surge in cyberattacks against banks. It also found upticks in financially-motivated attacks around pinnacles in the news cycle, such as when the U.S. confirmed its first case of COVID-19 as well as the first COVID-19 death.

On 13 May, the Federal Bureau of Investigation (FBI) and U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued a public service announcement warning organizations researching COVID-19 of likely targeting and network compromise by the People's Republic of China (PRC). The alert cautioned healthcare, pharmaceutical, and research sectors working on COVID-19 response to be aware of their status as targets and take the necessary steps to protect their systems. The FBI also requests organizations who suspect suspicious activity to contact their local FBI field office.

One of Britain's most powerful academic supercomputers, ARCHER, was the victim of a cyberattack that rendered the network unavailable to users on Tuesday and may have compromised user logins and SSH keys. Sources told The Register that ARCHER is an obvious resource for research work by computational biologists as well as those modelling the potential further spread of the novel coronavirus, and is therefore a target for hostile states. According to ARCHER admins, they now believe this to be a major issue across the academic community as other computers were compromised in the U.K. and elsewhere in Europe. The group has been working with the National Cyber Security Centre (NCSC) in order to better understand the situation.

Bam Construct and Interserve, two British construction firms that helped build emergency hospitals to cope with the COVID-19 pandemic, have been hit by cyberattacks. Though details on the attacks are sparse, Bam Construct's spokesman shared that several systems were offline, including its website, while the company neutralizes the attack. He also said that there has been a wave of attacks on firms that are helping the nation's fight against coronavirus. Interserve confirmed that it was working closely with the National Cyber Security Centre (NCSC) and Strategic Incident Response teams to investigate the attack.

Cybercrime in India continues to soar amidst the country's coronavirus lockdown, with both independent and state-sponsored cyber criminals targeting private citizens' wallets and personal data. According to India's National Cyber Security Coordinator (NCSC), criminals have launched

thousands of “fraud portals” related to the virus that lure Indians eager to contribute to the fight against coronavirus into making donations. Many of these sites are virtually indistinguishable from their genuine counterparts. State actors are also using COVID-19 as a pretext to launch attacks on India’s key sectors to include defense and national security, as evidenced by last month’s Pakistan-sponsored ransomware and phishing attacks aimed at stealing India’s highly sensitive defense, security, and diplomatic information under the guise of coronavirus health advisories.

Adding fuel to the ongoing privacy and security debate over contact-tracing, a Subway employee used information from the company’s contract-tracing forms to stalk a customer in Auckland, New Zealand. The customer was required to provide personal information such as name, home address, email address, and phone number prior to placing a food order. Subway suspended the employee and planned to roll out a new digital contact-tracing system in all restaurants as of 13 May, which they claimed would hold information more securely.

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

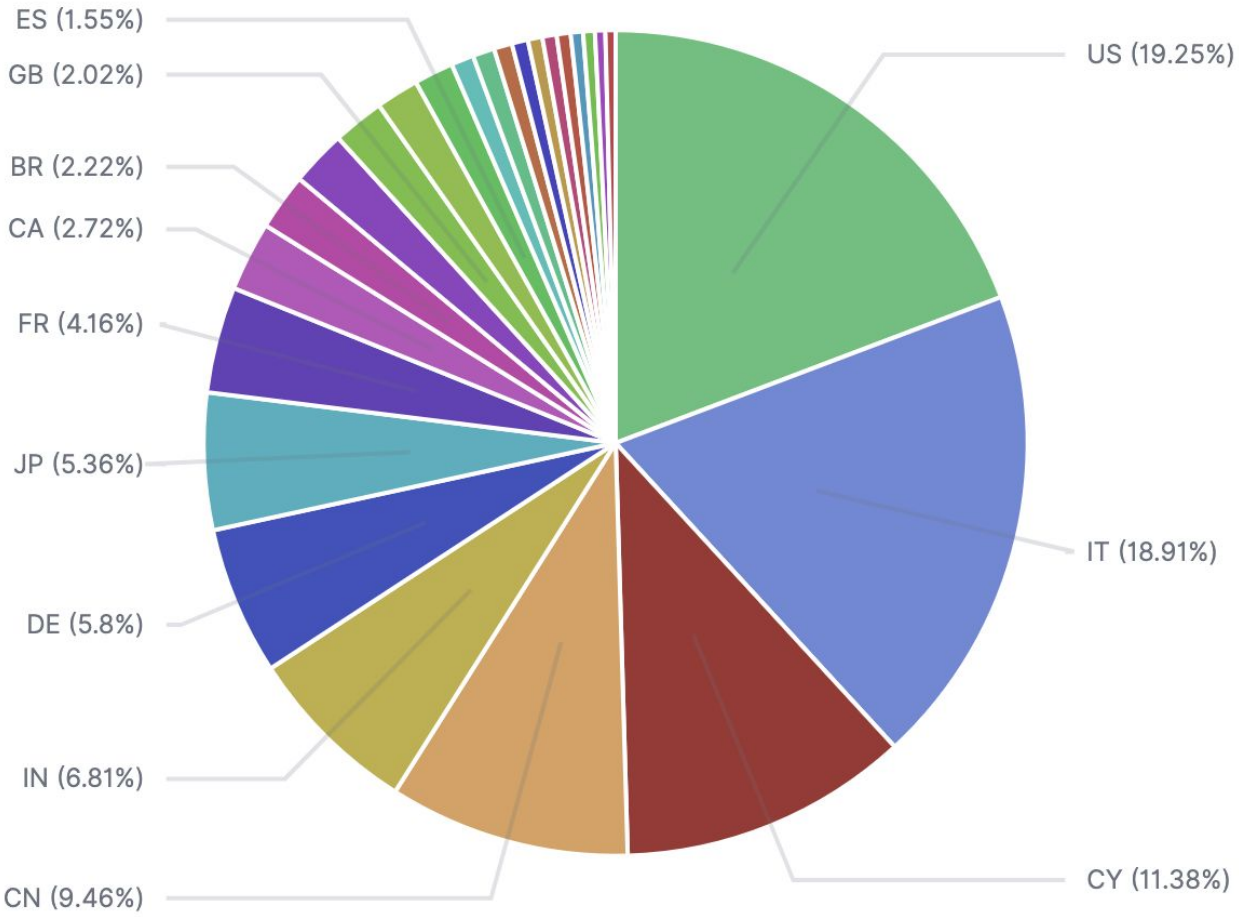
New Blacklist Data

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

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

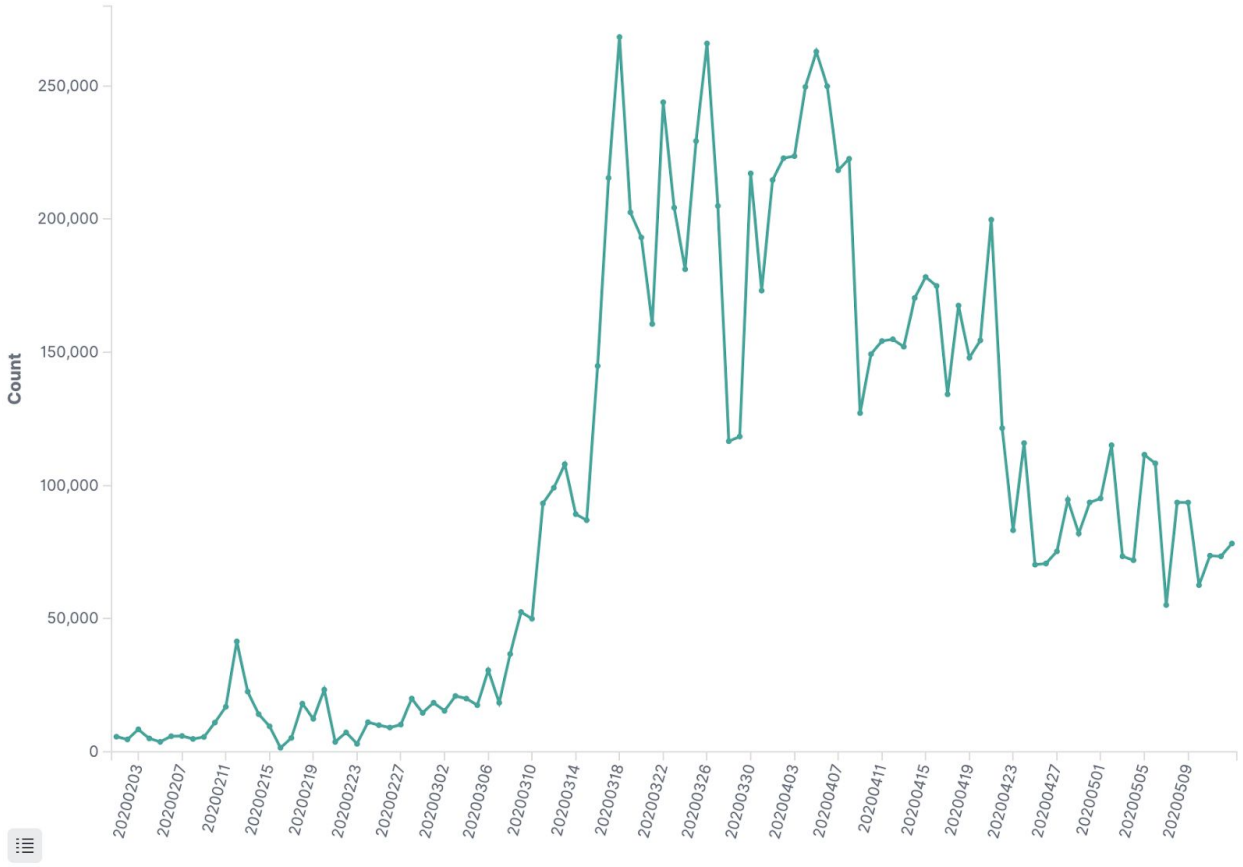
COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 05/13/2020-05/14/2020. During this period, RiskIQ analyzed 78,200 spam emails containing either “*corona*” or “*covid*” in the subject line. There were 7,096 unique subject lines observed during the reporting period. The spam emails originated from 4,971 unique sending email domains and 9,126 unique SMTP IP Addresses. Analysts identified 146 emails which sent an executable file for Windows machines.



Spam emails by country of origin

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States



Spam emails by volume since February 1, 2020

Top 25 Subjects

1. 8,391 - Covid-19-Hilfsdarlehensangebot…
2. 8,309 - Covid-19: non fermiamoci adesso
3. 4,205 - Offerta Dedicata ai lavoratori impegnati alla lotta contro il Covid-19
4. 3,789 - URGENT REPLY ON INESTMENT FUND-ON COVID-19
5. 3,246 - The Corona Letter: Lockdown isn't good for well-being
6. 1,074 - Contra el COVID, juntos lograremos más
7. 856 - Reife Frauen treffen trotz Corona
8. 850 - Gospel Artist Killed in Police Shooting + Railworker DEAD After Man Infected with CORONA Spat On Her
9. 840 - Informacion COVID-19
10. 837 - CUIDADO DE ADULTOS MAYORES /// PROTOCOLO ANTE EL COVID19
11. 829 - ComputerVault: Stops Coronavirus with Remote Work
12. 752 - CORONA-VIRUS DONATION
13. 740 - ¿Quieres protegerte del CORONAVIRUS? - Paneles Anticovid / Comprale al Perú
14. 691 - MiSeguro - Insumos Covid-19 Despachos a Todo Chile
15. 584 - Productos eficientes para combatir y prevenir el Covid-19
16. 453 - ALERT: Compensation For Coronavirus (COVID-19) Coverage Approval
17. 429 - Manejo de contratos, Mitigación de COVID en lugares de trabajo
18. 427 - COVID-19 - Custom Projects | Mobile Application | SEO !! -etc <redacted>
19. 410 - LOMBARDIA CREDITO ADESSO 2020: emergenza Covid-19, la Regione amplia la platea di professionisti e imprese per il finanziamento del capitale circolante che può arrivare fino al 25% della media dei ricavi. Domande fino ad esaurimento fondi.
20. 392 - Going Concern - Key Considerations for Auditors amid COVID-19
21. 388 - Re:Covid-19 Face Mask
22. 386 - USAID MONETARY DONATION FOR COVID-19
23. 368 - Re: Vanity upon Vanity, COVID -19
24. 360 - COVID-19) Unterstützung

25. 351 - Sale Masks , Breathing machine and Corona Virus test Kit with good price.

Top 10 IP Addresses

1. 8,385 - 82.102.95.84
2. 3,789 - 153.127.29.31
3. 1,067 - 78.40.35.234
4. 1,042 - 46.231.112.226
5. 855 - 46.20.37.30
6. 837 - 181.46.136.165
7. 829 - 100.0.45.37
8. 809 - 130.193.83.66
9. 791 - 130.193.88.146
10. 752 - 194.169.211.47

Top 10 Domains (RDNS)

1. 8,385 - mail[.]digitalheritagelab[.]eu
2. 3,789 - ik1-412-38277[.]vs[.]sakura[.]ne[.]jp
3. 1,067 - svm40354[.]vps[.]tagadab[.]it
4. 1,042 - svm43646[.]vps[.]tagadab[.]it
5. 855 - data2web[.]de
6. 829 - generacity[.]com
7. 809 - svm45164[.]vps[.]tagadab[.]it
8. 791 - svm39632[.]vps[.]tagadab[.]it
9. 773 - cpe-181-46-136-165[.]telecentro-reversos[.]com[.]ar
10. 752 - marbis[.]nitrado[.]net

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

1. 127 - URGENT TENDER#675320 (covid19 kits)

2. 19 - Payment Assistance Due To Covid-19 Pandemic

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

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

1. 14,186 US
2. 13,940 IT
3. 8,385 CY
4. 6,970 CN
5. 5,022 IN
6. 4,277 DE
7. 3,948 JP
8. 3,066 FR
9. 2,002 CA
10. 1,636 BR
11. 1,606 AR
12. 1,488 GB
13. 1,240 MX
14. 1,140 ES
15. 654 NL
16. 631 CL
17. 527 VN
18. 468 RO
19. 419 RU
20. 413 AT
21. 400 BE
22. 355 ZA
23. 339 CH
24. 299 PL
25. 294 AU

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

COVID-19 Host, Domain, and Mobile App Tracking

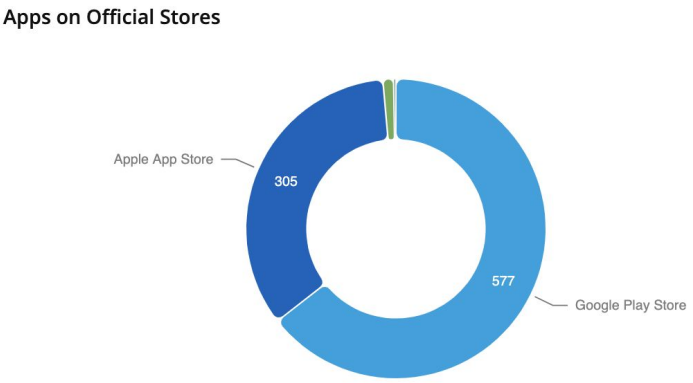
RiskIQ gathers data relating to newly-observed hosts and domains containing COVID-19, COVID19, or Coronavirus in the host or domain name and mobile apps containing COVID-19, COVID19, or Coronavirus in the title or description. A summary of data collected is contained in this section.

Domains and Hosts

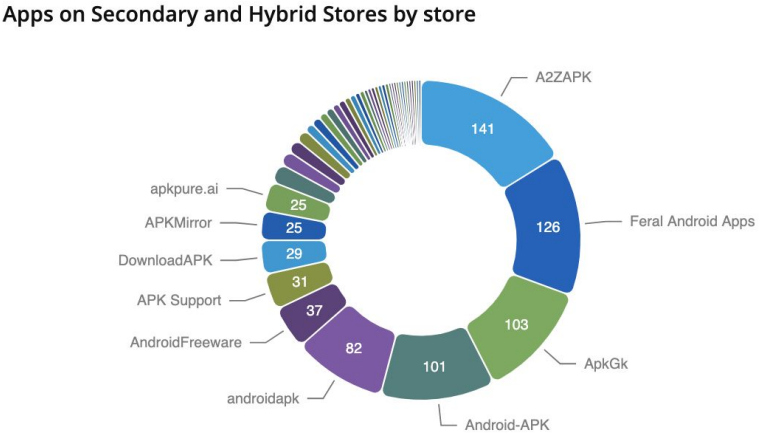
Domains: 80,692
Hosts: 92,081
Hosts and Domains with Potential Mail Servers: 295
Email-Capable Domains and Hosts: 29,236
Live Hosts and Domains Not Parked: 37,301

Mobile Apps

1. Apps in Official Stores: 892 (See Graph)
    a. Google Play Store: 577
    b. Apple App Store: 305
    c. Windows Phone: 9
    d. Amazon: 1



2. Apps in Secondary/Hybrid Stores: 826 (See Graph)



3. Blacklisted Mobile Apps by Store Type:
    a. Secondary: 34
    b. Hybrid: 1
    c. Official: 2

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

Facts and Figures at a Glance

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

Global

Total Cases: 4,379,973
Total Fatalities: 298,185
Countries w/ Confirmed Cases: 187

U.S.

Total Tests Conducted: 9,974,831
Total Cases: 1,391,238
Total Fatalities: 84,144
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: 340,661
2. New Jersey: 141,560
3. Illinois: 84,694

Counties

1. New York City (NY): 187,250
2. Cook County (IL): 56,406
3. Nassau County (NY): 38,587
4. Suffolk County (NY): 37,305
5. Los Angeles County (CA): 34,552
6. Westchester County (NY): 31,611
7. Philadelphia County (PA): 18,779
8. Wayne County (MI): 18,389
9. Middlesex (MA): 18,201
10. Hudson County (NJ): 17,451

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

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

Note: States followed by an asterisk (*) have allowed their orders to expire. Please see the updated link for each state including restrictions following the expiration of stay-at-home orders.

State	Start	End	State	Start	End
California	03/19	TBD	Montana*	03/28	04/24
Illinois	03/21	05/30	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	05/08
Kentucky	03/23	TBD	Maryland	03/30	TBD
Louisiana	03/23	05/15	Virginia	03/30	06/10
Ohio	03/23	05/29	Arizona	03/31	05/15
Oregon	03/23	TBD	Tennessee*	03/31	04/30
Washington	03/23	05/31	Washington, DC	04/01	05/15
Delaware	03/24	05/15	Nevada	04/01	05/15
Indiana*	03/24	05/01	Pennsylvania	04/01	06/04
Michigan	03/24	05/15	Oklahoma*	04/01	04/30
New Mexico	03/24	05/15	Texas*	04/02	04/30
Massachusetts	03/24	05/18	Maine	04/02	05/31
West Virginia	03/24	TBD	Florida*	04/03	05/04
Hawaii	03/25	05/31	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	05/18			
New Hampshire	03/27	05/31			

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

Governmental Guidance

State & Local Governments

California

As of 05/14/2020, California has 73,144 confirmed cases of COVID-19 and 2,974 fatalities. Most retail businesses in San Mateo and San Francisco counties are expected to reopen on Monday for curbside pickup and delivery. Both counties are easing restrictions after seeing no spikes in cases and a flattening of hospitalizations.

Illinois

As of 05/14/2020, Illinois has 84,694 confirmed cases of COVID-19 and 3,792 fatalities. Governor JB Pritzker had a stern warning for towns looking to defy his stay-at-home order as Illinois reported its deadliest day yet from the COVID-19 pandemic with 192 deaths. Pritzker said there will be consequences, suggesting state-regulated businesses could lose their licenses and local governments could have federal dollars withheld.

New York

As of 05/14/2020, New York has 340,661 confirmed cases of COVID-19 and 27,477 fatalities. The Office of Court Administration announced Wednesday that courthouses in some parts of New York will begin reopening to the public next week. Starting next Monday, judges and staff will return to courthouses in upstate counties that have met Gov. Cuomo's reopening benchmarks and new cases can be filed in five judicial districts electronically.

Texas

As of 05/14/2020, Texas has 43,020 confirmed cases of COVID-19 and 1,172 fatalities. Texas reported that it conducted 49,259 tests Wednesday, the highest one-day total reported since the pandemic began. According to a Texas Department of State Health Services spokesperson, the department received a large batch of tests results from laboratories.

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

Washington, DC

As of 05/14/2020, the Washington, D.C. region has a total of 66,346 confirmed cases of COVID-19, with 34,812 in Maryland, 26,746 in Virginia, and 6,584 in the District of Columbia. Maryland has 1,809 fatalities, Virginia has 928 fatalities, and the District of Columbia has 358 fatalities. Maryland Governor Larry Hogan is moving the state from a stay-home order to a "safer-at-home" advisory. Beginning at 5 p.m. Friday. D.C. Mayor Muriel E. Bowser extended the city's stay-at-home order to June 8.

RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

End Report