RISKIQ®

RiskIQ i3:

COVID-19 Daily Update

04/28/2020

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.

Noteable Events in the Past 24 Hours

More than 3.4 million Americans are temporarily skipping their mortgage payments because they lost income during the COVID-19 pandemic. Many mortgage companies are asking borrowers to make balloon payments, meaning they would have to pay all the money for the skipped payments in a lump sum at the end of the forgiveness period.

JetBlue will be the first airline to require passengers to wear face masks while on flights. The policy change comes after the company announced all crew must wear face masks. Similarly, American Airlines said they would provide face masks for all passengers, but stopped short of requiring passengers to wear them.

Quest Diagnostics announced that customers can now skip visits to the doctor's office and request COVID-19 antibody tests online. The test, priced at $119, will be able to tell individuals if they have had the virus, and if they may have some level of immunity to future infection. Health officials have warned that having antibodies present in the body may not guarantee immunity.

House leaders announced they have reversed plans to return to Congress for in-person sessions, citing concerns about potential exposure to COVID-19. House Majority Leader, Steny Hoyer (D-MD) said that the House's physician warned that returning to Capitol Hill now would present a substantial risk to lawmakers. The Senate is still planning on reconvening next Monday according to Senate Majority Leader, Mitch McConnell.

U.S. COVID-19 fatality rates are increasing even though case totals are flattening due to a lag between initial diagnosis and death. Officials speculate that the wave of people dying now were likely infected between three and five weeks ago. The number of deaths will likely not decline until three to four weeks after the total number of cases diagnosed on a daily basis begins to decline.

Yoshiro Mori, president of the Tokyo Games, said the Olympics could possibly be cancelled if the pandemic is not brought under control by next year. The games have already been postponed until July 2021 as a result of the pandemic. Olympic officials have said no additional postponement of the games is possible.

Digital Exploitation

Australia's Ambassador for Cyber Affairs, Dr Tobias Feakin has called for an end to attacks on medical facilities, such as the recent cyber attack on one of the Czech Republic's biggest COVID-19 testing laboratories. He stated to ZDNet that "[w]e call on all countries to cease immediately any cyber activity inconsistent with their international commitments."

The cyberattackers behind the Shade ransomware (Troldesh) have shut down their operations, released over 750,000 decryption keys, and apologized for the harm they caused their victims, according to BleepingComputer. Shade Ransomware has been in operation since 2014 and predominantly targets people in Russia and Ukraine.

Some Sophos firewall products were attacked with a new Trojan malware, dubbed Asnarök, to steal usernames and hashed passwords, according to BleepingComputer. The malware exploits a zero-day SQL injection vulnerability that can lead to remote code execution on any unpatched physical and virtual firewalls it targets.
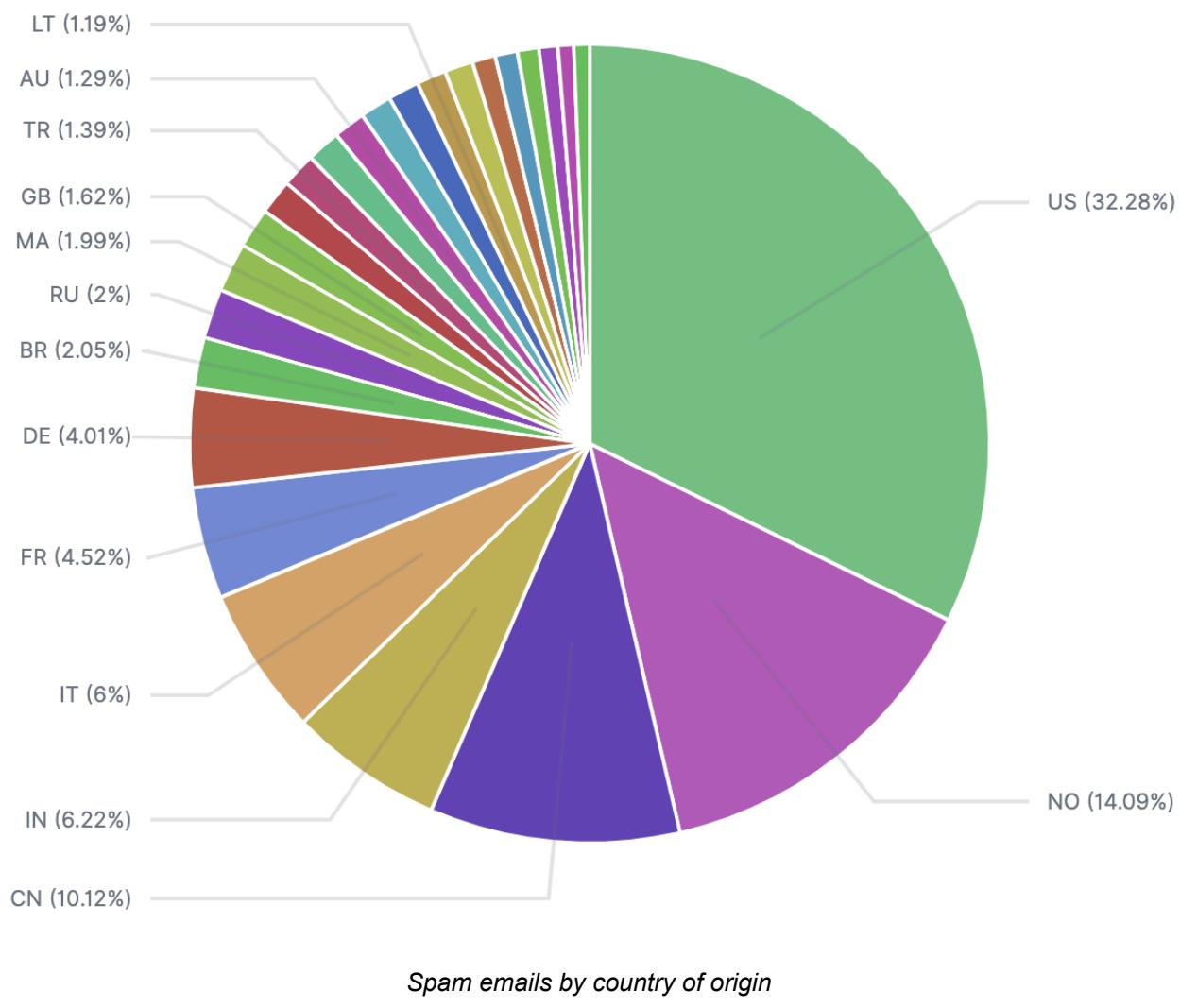
Zoom users are being targeted with a new phishing campaign that uses fake Zoom meeting notifications to threaten those who work in corporate environments that their contracts will either be suspended or terminated. When users click on the link they are redirected to a phishing landing page that mimics a Zoom sign-in page and scammers are able to steal the victims credentials.
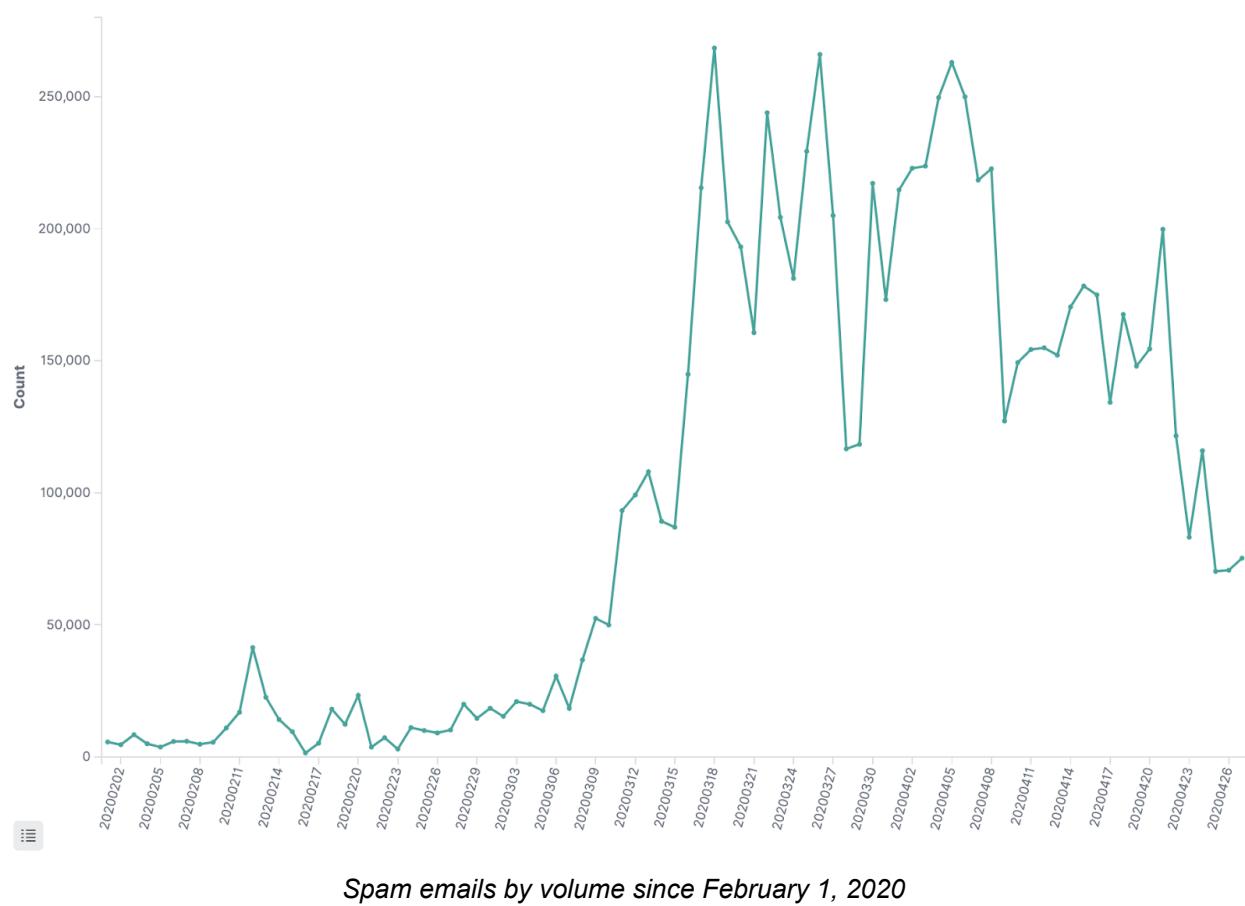
Cybercriminals are creating new scams using COVID-19 delivery issues as a lure to get people to visit malicious links or open malware, according to BleepingComputer. In one example, the scammer sends an email that pretends to be from FedEx stating that due to the Coronavirus "lock-down," a package is being held at the warehouse. They then prompt the user to click on a phishing link to reschedule for pick up.

A few new COVID-19 related scams in the underground web marketplace include scammers offering an Israel-created 'vaccine' for $99. Another scammer posted a malicious MP3 file and informed users they needed to listen to it 3-6 times per day to eliminate COVID-19, according to Tripwire. Related, the United Kingdom's National Cyber Security Centre (NCSC) reportedly took down over 2,000 COVID-19 ploys in March, including 471 fake online shops, according to the BBC.

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 04/27/2020-04/28/2020. During this period, RiskIQ analyzed 75,253 spam emails containing either "*corona*" or "*covid*" in the subject line. There were 14,525 unique subject lines observed during the reporting period. The spam emails originated from 12,145 unique sending email domains and 8,678 unique SMTP IP Addresses. Analysts identified 102 emails which sent an executable file for Windows machines.

Spam emails by country of origin

Spam emails by volume since February 1, 2020

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: 73,475
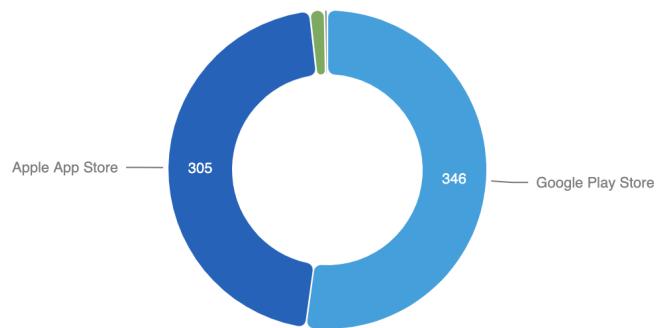Hosts: 83,612
Hosts and Domains with Potential Mail Servers: 285
Email-Capable Domains and Hosts: 26,670
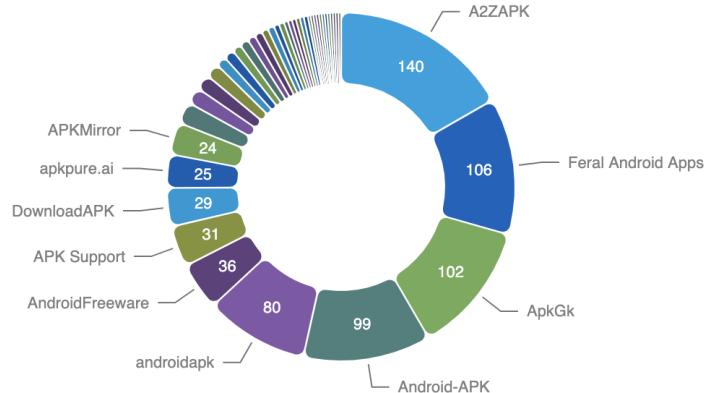Live Hosts and Domains Not Parked: 33,935

Mobile Apps

1. Apps in Official Stores: 661 (See Graph)
   a. Google Play Store: 346
   b. Apple App Store: 305
   c. Windows Phone: 9
   d. Amazon: 1

Apps on Official Stores

2. Apps in Secondary/Hybrid Stores: 795 (See Graph)

3. Blacklisted Mobile Apps by Store Type:
   a. Secondary: 28
   b. Hybrid: 1
   c. Official: 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: 3,060,152
Total Fatalities: 212,056
Countries w/ Confirmed Cases: 185

U.S.

Total Tests Conducted: 5,593,495
Total Cases: 988,469
Total Fatalities: 56,256
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: 291,996
2. New Jersey: 111,188
3. Massachusetts: 56,462

Counties

1. New York City (NY): 160,489
2. Nassau County (NY): 34,865
3. Suffolk County (NY): 32,470
4. Cook County (IL): 31,953
5. Westchester County (NY): 28,007
6. Los Angeles County (CA): 20,460
7. Wayne County (MI): 15,872
8. Bergen County (NJ): 15,104
9. Hudson County (NJ): 13,925
10. Essex County (NJ): 13,047

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	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	05/08
Michigan	03/24	05/15	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	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	05/04			
New Hampshire	03/27	05/04			

Governmental Guidance

State & Local Governments

California

As of 04/28/2020, California has 45,200 confirmed cases of COVID-19, and 1,788 fatalities.
Six counties in the Bay Area – Alameda, Contra Costa, Marin, San Francisco, San Mateo, and Santa Clara – plus the city of Berkeley announced on Monday that their shelter-in-place protocols, set to expire May 3, will be extended through at least the end of May. Conversely, Elected officials from six rural north state counties urged Governor Newsom on Monday to let them reopen for business.

Illinois

As of 04/28/2020, Illinois has 45,883 confirmed cases of COVID-19, and 1,983 fatalities. Governor J.B. Pritzker filed an appeal on Tuesday to reverse a judge's ruling in favor of Republican State Representative, Darren Bailey. Representative Bailey sued Governor Pritzer last week over the extension of the stay-at-home orders. Additionally, City View Multicare Center has reported a cluster of COVID-19 cases, including 163 residents and 31 staff members testing positive. The nursing home, located in west suburban Cicero, has also been cited for ten COVID-19 safety violations.

New York

As of 04/28/2020, New York has 291,996 confirmed cases of COVID-19, and 22,668 fatalities. NYC Mayor, Bill de Blasio announced a new grading policy for virtual learning due to COVID-19. The plan includes removing letter grades for K-5, remedial assistance for middle schoolers, and the option for high schoolers to use pass/fail for lower grades.

Texas

As of 04/28/2020, Texas has 25,321 confirmed cases of COVID-19, and 666 fatalities. Texas Governor, Greg Abbott outlined phase one to reopen Texas, and announced a testing program designed to efficiently identify and test Texans who contract COVD-19. Additionally, the state offered relaxed restrictions related to health care professions & announced amended requirements related to hospital capacity. Finally, the Texas Supreme Court extended the moratorium on eviction proceedings until May 18. This extension provides a few more weeks of relief to renters who would otherwise face eviction proceedings.

Washington, DC

As of 04/28/2020, the Washington, D.C. region has a total of 36,917 confirmed cases of COVID-19, with 19,487 in Maryland, 13,538 in Virginia, and 3,892 in the District of Columbia. Maryland has 945 fatalities, Virginia has 460 fatalities, and the District of Columbia has 185 fatalities. House Majority Leader, Steny H. Hoyer says the House is dropping plans to return due to COVID-19 risks. The Virginia chapter of the American Academy of Pediatrics after surveying over 100 Pediatricians reported a 30 percent decrease in infant vaccination rates and a 76 percent decrease in adolescent vaccination rates.

End Report