RISKIQ®

RiskIQ i3:

COVID-19 Daily Update

05/15/2020

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.

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

Officials from the Southeastern Conference (SEC) will vote on whether to allow athletes back on campus June 1 or June 15. LSU Executive Deputy Athletic Director Verge Ausberry said the SEC is aiming to have student-athletes back on June 1.

The Food and Drug Administration (FDA) is cautioning the public about the reliability of COVID-19 tests made by Abbott Laboratories. A study released this week found that up to 48% of tests may produce false negative results. The tests can still be used to confirm COVID-19 cases, but further testing should be used after negative results for symptomatic patients.

The U.S. Centers for Disease Control and Prevention issued a warning to doctors to be on the lookout for a new syndrome that may be associated with COVID-19 infection. The condition, called multisystem inflammatory syndrome in children (MIS-C), has been reported in Europe and in eighteen states, plus the District of Columbia. The syndrome was initially identified as Kawasaki disease, but researchers determined that the frequency of cases was inconsistent with Kawasaki disease. Many, but not all, children with MIS-C tested for either current or prior COVID-19 infection.

The head of JBS USA Holdings Inc.—the nation's largest beef producer—said the COVID-19 pandemic will likely hamper meat production for several months. Several companies, including JBS, Cargill Inc., Tyson Foods, and Smithfield Foods, closed plants down last month as the virus spread. JBS has since reopened in Minnesota, Pennsylvania, Colorado, and Wisconsin; these plants are said to be operating between 70% to 95% of their normal capacity.

New York reversed a mandate that required nursing homes to take in discharged COVID-19 patients after thousands of residents in nursing homes died. As of 05/12/2020, there have been 5,398 presumed deaths in nursing homes relating to the virus. The original policy was initially put in place to help provide more hospital beds.

The government of Wuhan, China said it will be testing all 11 million residents for COVID-19 after a new cluster of infections raised fears of a second wave. Wuhan officials have so far tested 3 million individuals. Jiang Qingwu, former director of the Institute of Public Health at Fudan University, said testing every resident of Wuhan would cost $282 million.

Areas in South and Central America are experiencing a heavy toll from the pandemic. Death tolls in some areas of Brazil, Peru, and Ecuador are five times higher than normal, according to an analysis by the New York Times. Gravediggers in Lima, Peru are reportedly burying bodies in mass graves, with coffins stacked three layers deep.

Digital Exploitation

The Department of Homeland Security (DHS) is preparing to advise the U.S. telecom industry on steps it can take to prevent attacks on 5G cell towers following a rash of serious attacks in Western Europe fueled by conspiracy theories that the technology spreads coronavirus. The theory likely began with a doctor's interview in a Belgian newspaper in January, who mused that 5G cell towers might be linked to the spread of the virus. These comments went viral, spreading through social media, and have even been promoted by American celebrities. DHS's Cybersecurity and Infrastructure Security Agency (CISA) will issue the alert with advice on ways to reduce the risk of attack, including installing appropriate sensing and barriers, cyber intrusion detection systems, closed circuit television, and monitoring drone activity near towers.

Nigeria's SilverTerrier cyber crime group is targeting organizations on the front line in the fight against coronavirus, according to research by Palo Alto Networks' Unit 42. SilverTerrier is a loosely affiliated cyber criminal group specializing in business email compromise (BEC), a security exploit in which the attacker targets an employee who has access to company funds, and convinces the victim to transfer money into a bank account controlled by the attacker. In the past three months, three SilverTerrier actors have launched a series of COVID-19-themed malware campaigns, producing more than 170 distinct phishing emails aimed at organizations leading national responses to the pandemic such as government, healthcare, insurance, medical research and publishing, and utilities in Australia, Canada, Italy, the U.K., and the U.S.

Romanian law enforcement arrested four hackers from the group PentaGuard who were preparing to launch ransomware attacks against Romanian hospitals. Romania's Director for Investigating Organized Crime and Terrorism (DIICOT) and Romania's secret service agency (SRI) said the hackers intended to send emails with COVID-19 lures to hospitals to infect computers, encrypt files, and disrupt hospital activity. PentaGuard has been around since 2001, when it was involved in mass-defacements of several government and military websites, including Microsoft Romania.

New Blacklist Data

*Note: No new updates. Please see the COVID-19 Daily Update (dated 05/14/2020) for the most recent data.*

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 05/14/2020-05/15/2020. During this period, RiskIQ analyzed 89,658 spam emails containing either "*corona*" or "*covid*" in the subject line. There were 7,691 unique subject lines observed during the reporting period. The spam emails originated from 5,244 unique sending email domains and 8,940 unique SMTP IP Addresses. Analysts identified 147 emails which sent an executable file for Windows machines.
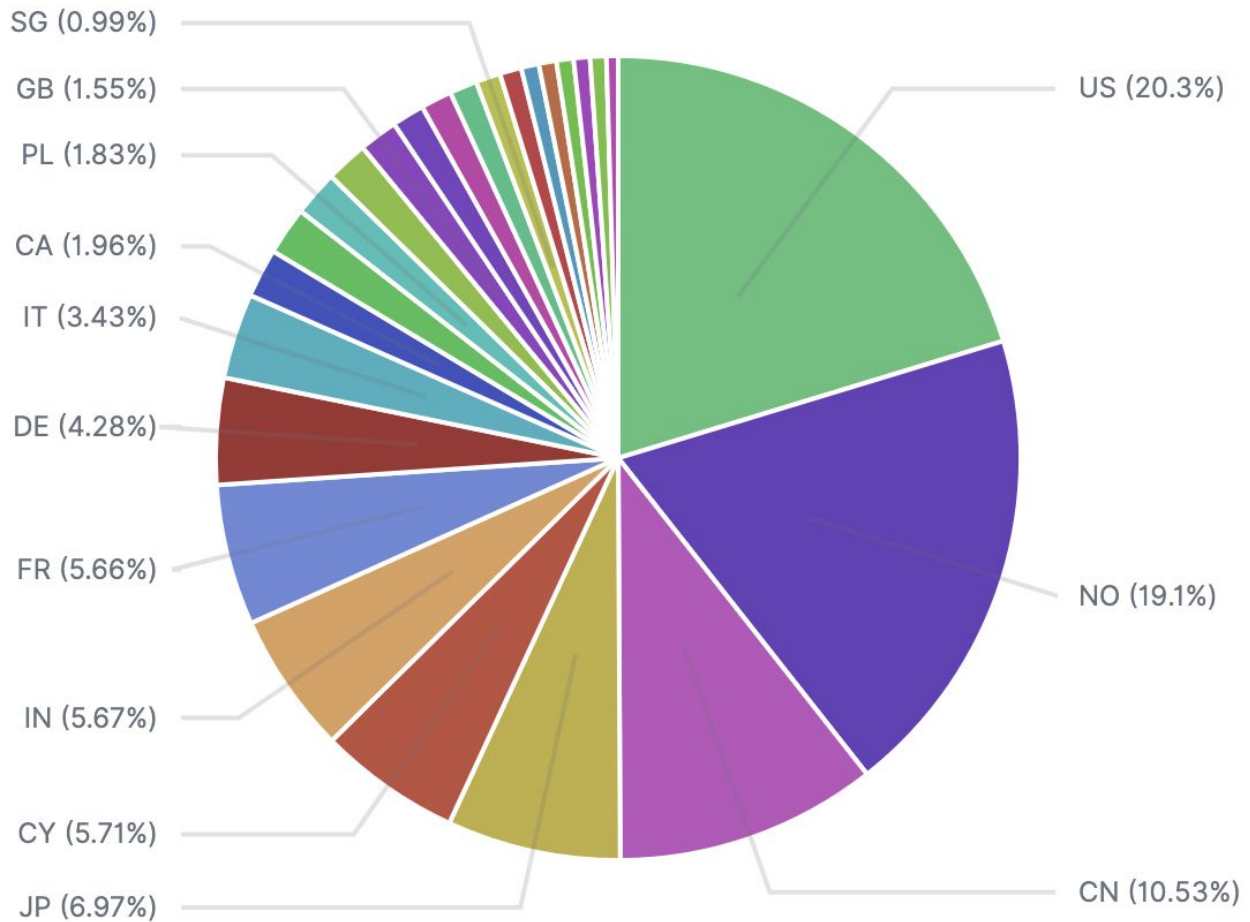
Spam emails by country of origin
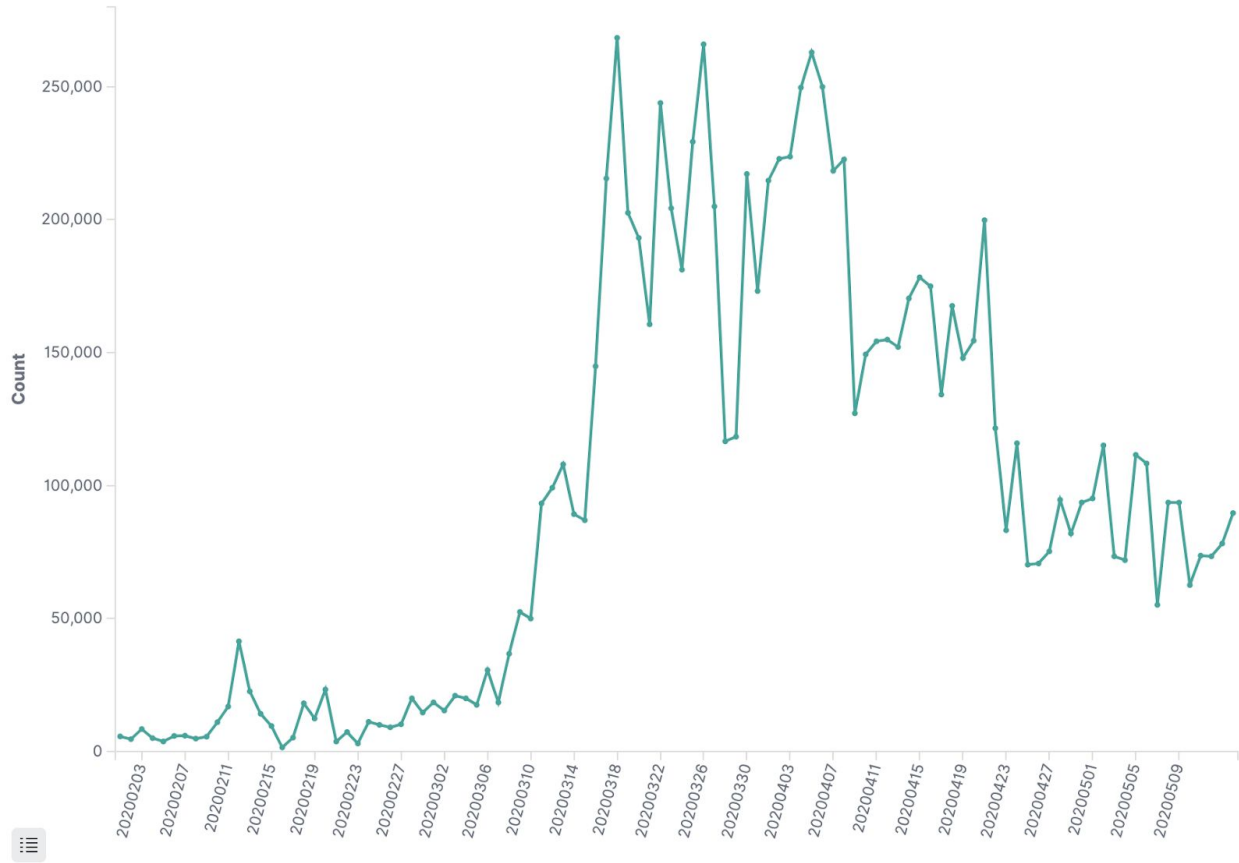
Spam emails by volume since February 1, 2020

RISKIQ®

Top 25 Subjects

1. 16,180 - COVID-19 Stimulus Package Grant(s)

2. 5,597 - URGENT REPLY ON INESTMENT FUND-ON COVID-19

3. 4,824 - Covid-19-Hilfsdarlehensangebot…

4. 3,537 - The Corona Letter: Are AC trains safe to travel?

5. 1,732 - Informacion COVID-19

6. 1,528 - ComputerVault: Stops Coronavirus with Remote Work

7. 1,523 - COVID19 Offer -85%

8. 1,254 - Medical supplies for counter COVID-19 virus

9. 1,213 - Alergia czy COVID19? Pro bono konsultacja medyczna online 24/7

10. 1,188 - The COVID-19 Solidarity Response Fund

11. 877 - Subject: You Can Apply For COVID-19 RELIEF FUNDING Relief Funding Directly

12. 861 - Watch for these COVID-19 symptoms

13. 853 - Paneles Divisorios Anti Covid para Atencion de Publico.

14. 733 - COVID-19 symptoms

15. 731 - Welche Maske sollten Sie gegen das Coronavirus tragen? Hier die Informationen und alles Wissenswerte

16. 677 - MiSeguro - Insumos Covid-19 Despachos a Todo Chile

17. 603 - COVID-19 Stimulus Package Grant Beneficiary

18. 560 - Reife Frauen treffen trotz Corona

19. 549 - CUIDADO DE ADULTOS MAYORES   /// PROTOCOLO ANTE EL COVID19

20. 538 - Fw: Covid19 Grants

21. 527 - Re: Defeat Coronavirus, non contact fever alarm device

22. 512 - Mitigación de COVID en lugares de trabajo

23. 510 - Contactless infrared body temperature thermometer defeat Coronavirus

24. 432 - Касается каждого! Включение фотографов в перечень отраслей, пострадавших от COVID-19

25. 417 - (COVID-19) Actualización de noticias

Top 10 IP Addresses

1. 16,135 - 82.134.25.158
2. 5,596 - 153.127.29.31
3. 4,823 - 82.102.95.84
4. 1,528 - 100.0.45.37
5. 1,183 - 23.254.202.134
6. 1037 - 61.141.77.193
7. 974 - 80.211.76.14
8. 959 - 51.77.33.44
9. 877 - 37.120.145.213
10. 833 - 80.211.174.185

Top 10 Domains (RDNS)

1. 16,135 - 158[.]82-134-25[.]bkkb[.]no
2. 5,596 - ik1-412-38277[.]vs[.]sakura[.]ne[.]jp
3. 4,823 - mail[.]digitalheritagelab[.]eu
4. 1,528 - generacit[.]com
5. 1,183 - hwsrv-727635[.]hostwindsdns[.]com
6. 974 - srv14[.]venitas[.]lt
7. 959 - ip44[.]ip-51-77-33[.]eu
8. 833 - srv185[.]venitas[.]lt
9. 831 - 5330[.]niebieski[.]net
10. 675 - triton246[.]startdedicated[.]com

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

1. 69 - COVID-19 UPDATE. EASING OF LOCKDOWN.

2. 47 - URGENT TENDER#675320 (covid19 kits)

3. 31 - URGENT TENDER#775320 (covid19 kits)

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

1. 17,162 US
2. 16,149 NO
3. 8,901 CN
4. 5,897 JP
5. 4,826 CY
6. 4,795 IN
7. 4,788 FR
8. 3,620 DE
9. 2,893 IT
10. 1,660 CA
11. 1,628 AR
12. 1,548 PL
13. 1,431 RO
14. 1,314 GB
15. 1,101 ES
16. 1,055 RU
17. 937 BR
18. 837 SG
19. 736 NL
20. 603 PY
21. 596 ZA
22. 581 HU
23. 554 CZ
24. 538 BE
25. 396 MY

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: 81,010
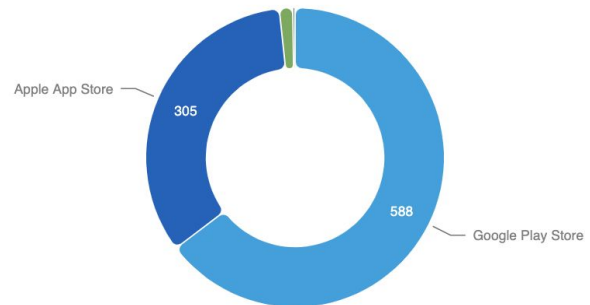Hosts: 92,562
Hosts and Domains with Potential Mail Servers: 298
Email-Capable Domains and Hosts: 29,539
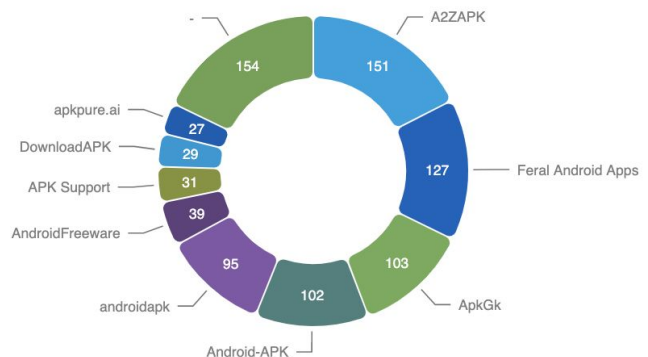Live Hosts and Domains Not Parked: 37,501

Mobile Apps

1. Apps in Official Stores: 906 (See Graph)
   a. Google Play Store: 588
   b. Apple App Store: 305
   c. Windows Phone: 12
   d. Amazon: 1

Apps on Official Stores

2. Apps in Secondary/Hybrid Stores: 858 (See Graph)

3. Blacklisted Mobile Apps by Store Type:
   a. Secondary: 34
   b. Hybrid: 2
   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: 4,444,670
Total Fatalities: 302,493
Countries w/ Confirmed Cases: 188

U.S.

Total Tests Conducted: 10,341,775
Total Cases: 1,417,889
Total Fatalities: 85,906
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: 343,051
2. New Jersey: 142,704
3. Illinois: 87,937

Counties

1. New York City (NY): 188,545
2. Cook County (IL): 54,457
3. Nassau County (NY): 38,743
4. Suffolk County (NY): 37,544
5. Los Angeles County (CA): 35,392
6. Westchester County (NY): 31,792
7. Philadelphia County (PA): 19,093
8. Wayne County (MI): 18,770
9. Middlesex County (MA): 18,381
10. Hudson County (NJ): 17,602

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	06/13	Kansas*	03/30	05/03
Connecticut	03/23	05/20	North Carolina*	03/30	05/08
Kentucky	03/23	TBD	Maryland*	03/30	05/15
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	06/08
Delaware	03/24	05/31	Nevada*	04/01	05/15
Indiana*	03/24	05/01	Pennsylvania	04/01	06/04
Michigan	03/24	06/11	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	06/15	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			

Governmental Guidance

State & Local Governments

California

As of 05/15/2020, California has 74,871 confirmed cases of COVID-19 and 3,052 fatalities. Governor Gavin Newsom proposed $14 billion in budget cuts for California to fill a $54.3 billion budget deficit caused by the stay-at-home order. Public schools would take a major cut with the new proposed budget with a $7.5 billion loss compared to the budget proposed in January.

Illinois

As of 05/15/2020, Illinois has 87,937 confirmed cases of COVID-19 and 3,928 fatalities. Governor J.B. Pritzker announced that all of Illinois is on track to reopen at the end of May. Governor Pritzker stated that all regions are meeting metrics in order to move from Phase Two to Phase Three of the five stage plan for Illinois. This will move all regions from the "flattening" stage to the "recovery" stage.

New York

As of 05/15/2020, New York has 343,051 confirmed cases of COVID-19 and 27,641 fatalities. Governor Andrew Cuomo extended the stay-at-home order for the state of New York until 06/13/2020. A four-phased reopening plan will allow regions of New York to begin reopening independently of one another, but they must meet certain conditions in order to reopen.

Texas

As of 05/15/2020, Texas has 44,485 confirmed cases of COVID-19 and 1,235 fatalities. On Thursday, Texas recorded its highest single-day count of 58 fatalities, two weeks after Texas reopened the state. Within a three day period from Tuesday to Thursday this week, the state has seen 116 fatalities due to COVID-19.

Washington, DC

As of 05/15/2020, the Washington, D.C. region has a total of 70,452 confirmed cases of COVID-19, with 35, 903 in Maryland, 27,813 in Virginia, and 6,736 in the District of Columbia. Maryland has 1,911 fatalities, Virginia has 956 fatalities, and the District of Columbia has 368 fatalities. While the state of Maryland has chosen to lift the stay-at-home order and move into a reopening phase, Montgomery County has chosen to remain shut down. Montgomery County Executive Marc Elrich stated the County was not yet ready to open due to its number of COVID-19 cases in the county.

End Report