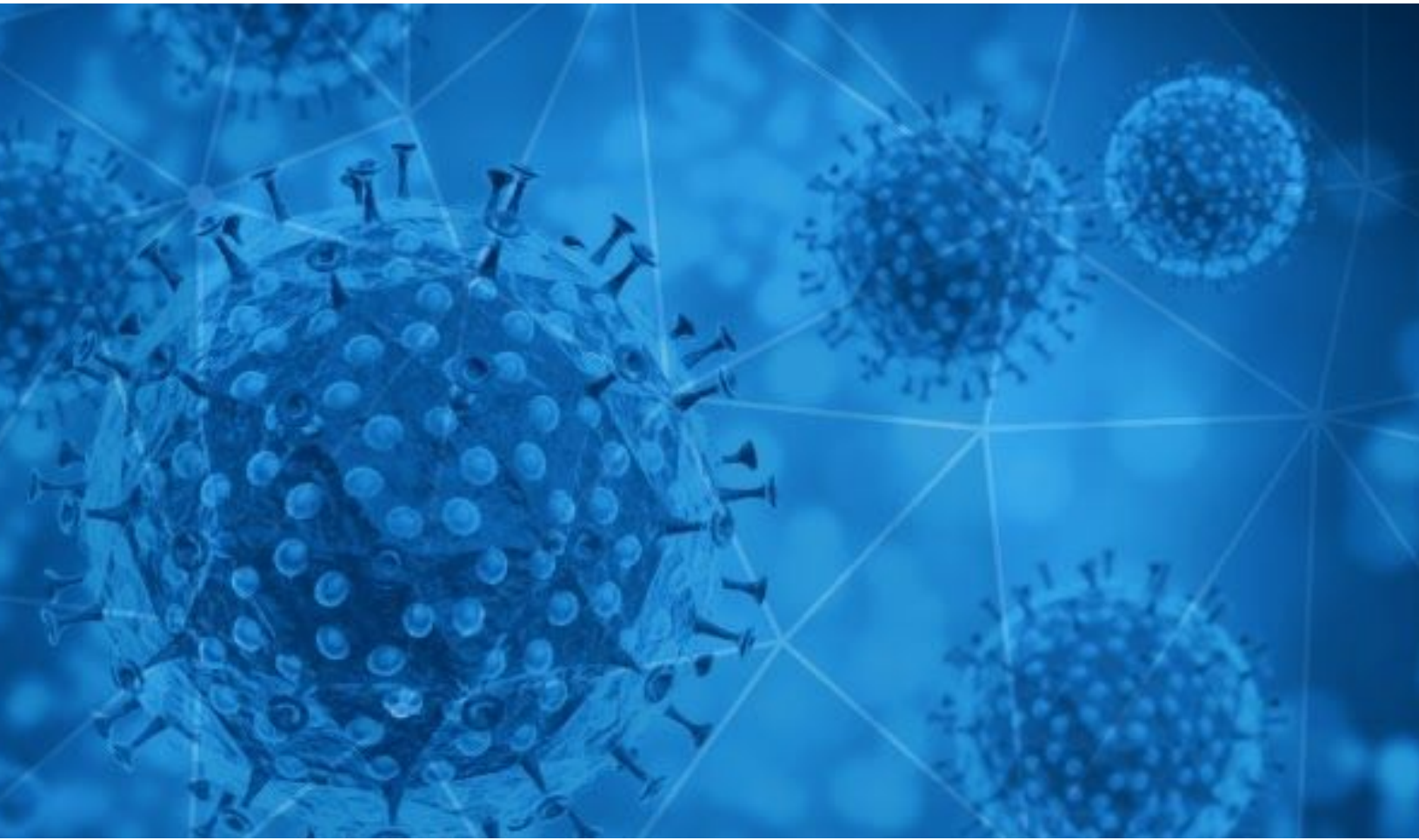
RISKIQ®

RiskIQ i3:

COVID-19 Daily Update

05/02/2020



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

Digital Exploitation

As reported on 05/01/2020 in the last few weeks, there has been an upswing in people receiving threatening, extortion email messages, demanding payment to avoid release of sensitive information. According to research by Malwarebytes Labs, the messages are fake, there is no malware involved, and the most important response is to change your password.

IBM X-Force discovered actors targeting email recipients with fake messages that claim to be from the department to inform people of changes to the FMLA, which gives employees the right to family-leave medical benefits. Instead, the emails include malicious attachments aimed at installing TrickBot malware which can allow attackers to gain complete control of the device.

Threat actors are using the COVID-19 pandemic to impersonate financial institutions on Instagram, according to Security Boulevard reporting. The threat actor creates a private Instagram account referencing COVID-19 using the financial institution's name, its logo, and a link to its legitimate website. The victims receive a direct message from the fake account claiming their profile has been selected to receive a gift and subsequently requests account and password information.

Newly published telemetry data collected by the researchers at Bitdefender suggests that U.S. reports of coronavirus-themed malware threat activity have been heaviest in states where testing has increased and the total number of confirmed infections has grown. According to SC Media reporting, the same trend holds for countries that have been hit hardest by the pandemic.

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

New Blacklist Data

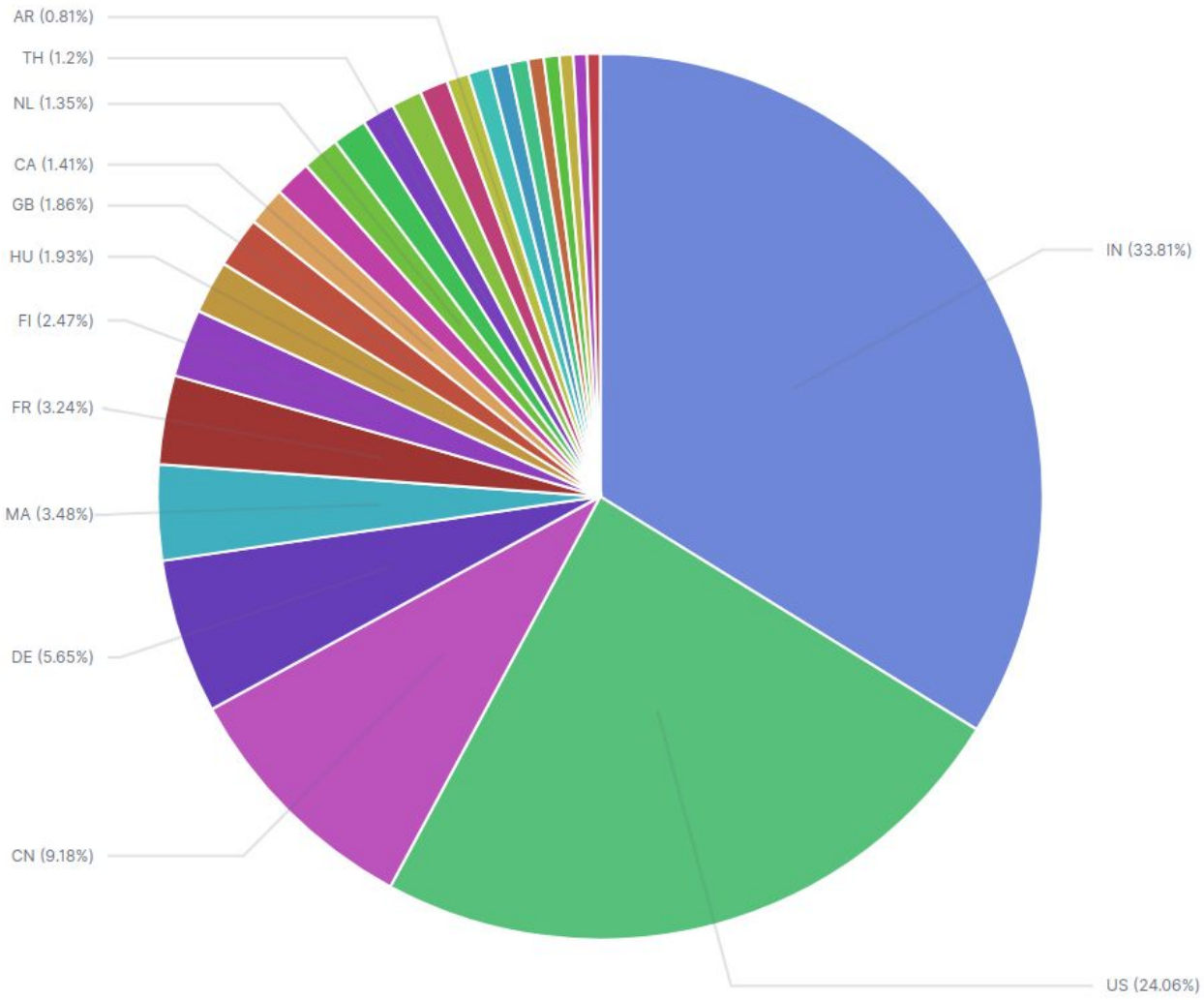
hxxps://streammarket[.]co[.]uk/covid-19

hxxps://covid19healthstores[.]com/

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

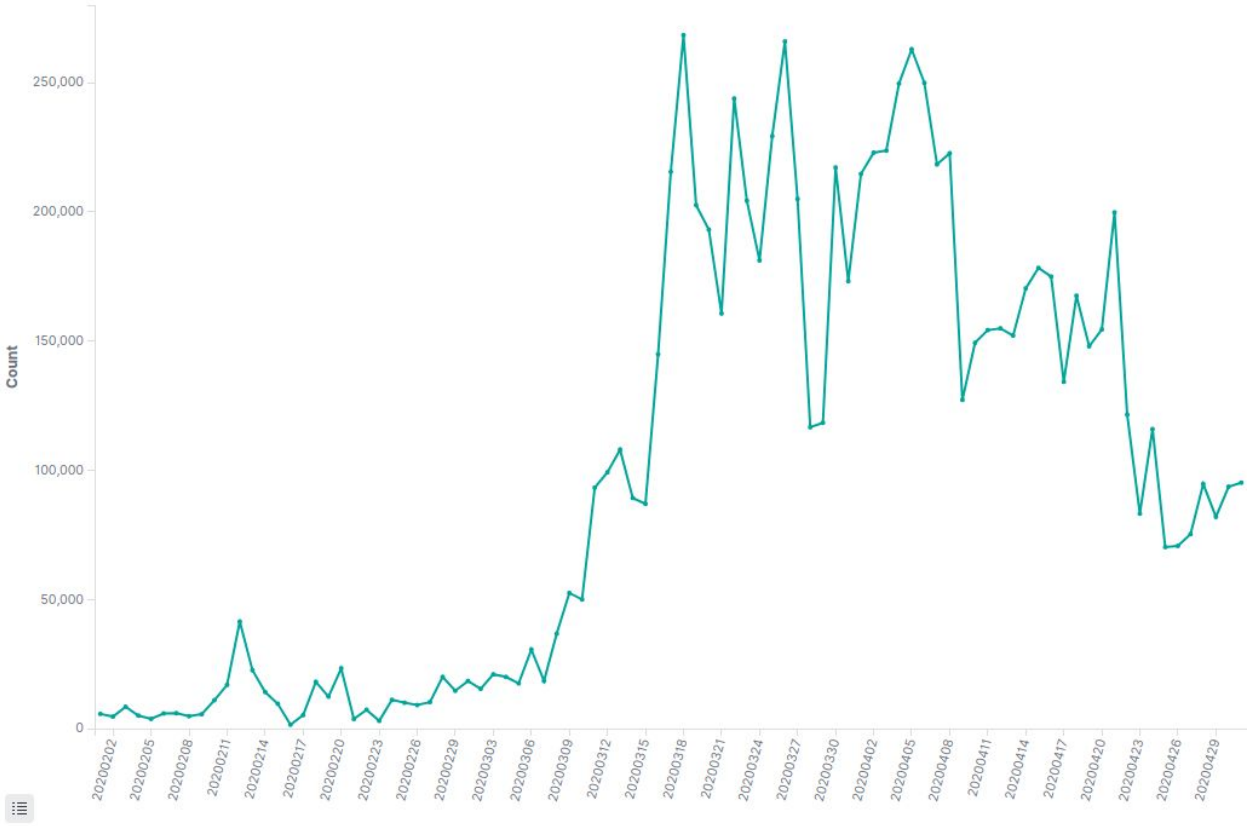
COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 05/01/2020-05/02/2020. During this period, RiskIQ analyzed 95,173 spam emails containing either “*corona*” or “*covid*” in the subject line. There were 11,008 unique subject lines observed during the reporting period. The spam emails originated from 7,184 unique sending email domains and 9,571 unique SMTP IP Addresses. Analysts identified 0 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

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

Top 25 Subjects

1. 22,801 - Let's fight Corona with Aarogya Setu! Download Now!
2. 4,028 - Welche Maske sollten Sie gegen das Coronavirus tragen? Hier die Informationen und alles Wissenswerte
3. 4,011 - Corona is not controllable
4. 3,332 - We fight together against COVID-19
5. 3,038 - <redacted>, Collect ""COVID-19"" Aid Now
6. 2,973 - The Corona Letter: Aarogya for all
7. 1,409 - COVID-19:Earning from Home while we Stay safe and Away from the Coronavirus..
8. 975 - CENTRAL BANK OF NIGERIA (DEAR BENEFICIARY YOUR ABANDON FUNDS WILL BE USE FOR COVID 19 FUNDING BY THE WORLD GOVERNOR BODIES.... CLAIM YOUR FUNDS)
9. 967 - For those who fight against COVID-19
10. 953 - อิ่มช้อป...อิ่มบุญ! ช้อปสินค้าศิลปินดังมากมาย ""ปันน้ำใจ สู้ภัย Covid-19"" ได้แล้ววันนี้!!
11. 921 - Messaggio importante - COVID-19
12. 800 - COVID-19 EMERGENCY DELIVERY OF YOUR CONSIGNMENT BOX TODAY.
13. 761 - Material Médico & Prevención Covid 19
14. 726 - Covid-19-Hilfsspende von Frances und Patrick Connolly.
15. 600 - Relief Funds For Covid 19
16. 595 - Implementación y protocolos de prevención del Coronavirus en Seguridad Salud en El Trabajo
17. 559 - Mask factory / covid19 protective products Sales
18. 554 - Redeem Your SBSA COVID-19 Financial Relief Funds Today!
19. 496 - Covid-19 Relief Donation From Frances and Patrick Connolly
20. 467 - Protect yourself and your family during the COVID-19 outbreak
21. 459 - Ultra Wifi Provides Faster Internet during COVID-19
22. 450 - Efektywny zarząd w dobie kryzysu i COVID-19 - PRIORYTETY działania

23. 445 - Covid-19 Reliefdonatie van Frances en Patrick Connolly.
24. 430 - SASB-COVID-19 Payment Relief Funds Approved
25. 409 - Sheryll Goedert - - Covid-19 Aid

Top 10 IP Addresses

1. 4,010 - 50.3.104.55
2. 3,038 - 81.192.231.96
3. 2,055 - 95.217.93.176
4. 1,416 - 164.100.13.81
5. 1,409 - 45.95.168.90
6. 1,367 - 164.100.13.85
7. 1,365 - 164.100.13.82
8. 1,360 - 164.100.13.83
9. 1,307 - 164.100.13.84
10. 1,071 - 164.100.13.94

Top 10 Domains (RDNS)

1. 3,038 - adsl-96-231-192-81[.]adsl2[.]iam[.]net[.]ma
2. 2,055 - static[.]176[.]93[.]217[.]95[.]clients[.]your-server[.]de
3. 1,416 - vastu13081[.]nic[.]in
4. 1,409 - ad[.]admindesk[.]email
5. 1,367 - vastu13085[.]nic[.]in
6. 1,365 - vastu13082[.]nic[.]in
7. 1,360 - vastu13083[.]nic[.]in
8. 1,307 - vastu13084[.]nic[.]in
9. 1,071 - vastu13094[.]nic[.]in
10. 1,069 - vastu13091[.]nic[.]in

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

There were no emails containing PE/EXEs discovered during the reporting period.

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. 29,677 IN
2. 21,118 US
3. 8,054 CN
4. 4,956 DE
5. 3,056 MA
6. 2,845 FR
7. 2,171 FI
8. 1,692 HU
9. 1,632 GB
10. 1,242 CA
11. 1,185 JP
12. 1,182 NL
13. 1,101 IT
14. 1,050 TH
15. 971 LT
16. 906 VN
17. 713 AR
18. 703 IE
19. 624 BD
20. 610 KR
21. 501 ES
22. 495 BR
23. 441 BE
24. 435 CL
25. 419 RU

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

COVID-19 Host, Domain, and Mobile App Tracking

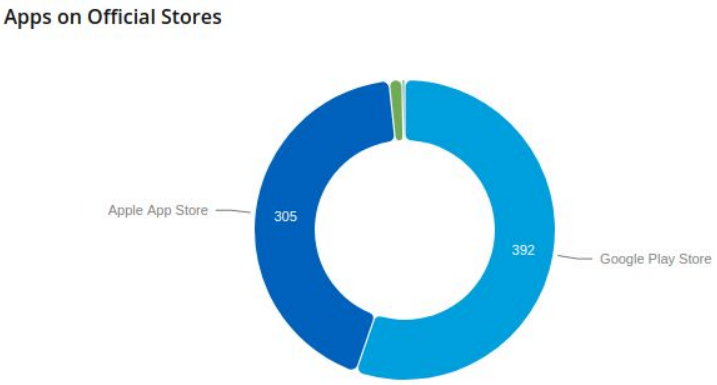
RiskIQ gathers data relating to newly-observed hosts and domains containing COVID-19, COVID19, or Coronavirus in the host or domain name and mobile apps containing COVID-19, COVID19, or Coronavirus in the title or description. A summary of data collected is contained in this section.

Domains and Hosts

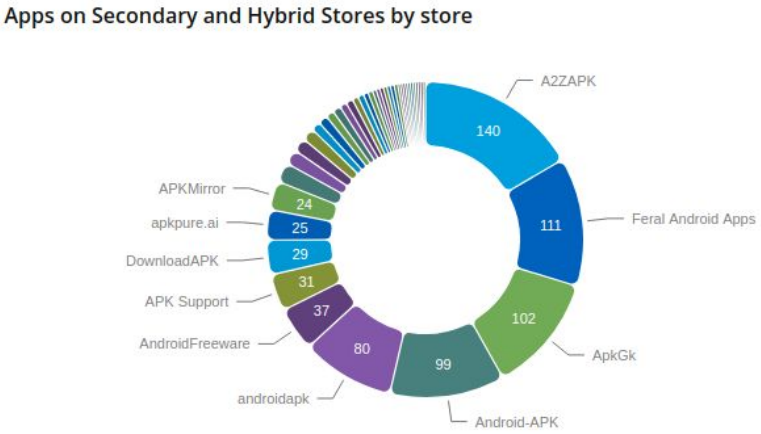
Domains: 75,638
Hosts: 6,132
Hosts and Domains with Potential Mail Servers: 287
Email-Capable Domains and Hosts: 27,463
Live Hosts and Domains Not Parked: 34,905

Mobile Apps

1. Apps in Official Stores: 707 (See Graph)
    a. Google Play Store: 392
    b. Apple App Store: 305
    c. Windows Phone: 9
    d. Amazon: 1



2. Apps in Secondary/Hybrid Stores: 802 (See Graph)



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

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

End Report