RiskIQ i3:

COVID-19 Daily Update

04/04/2020

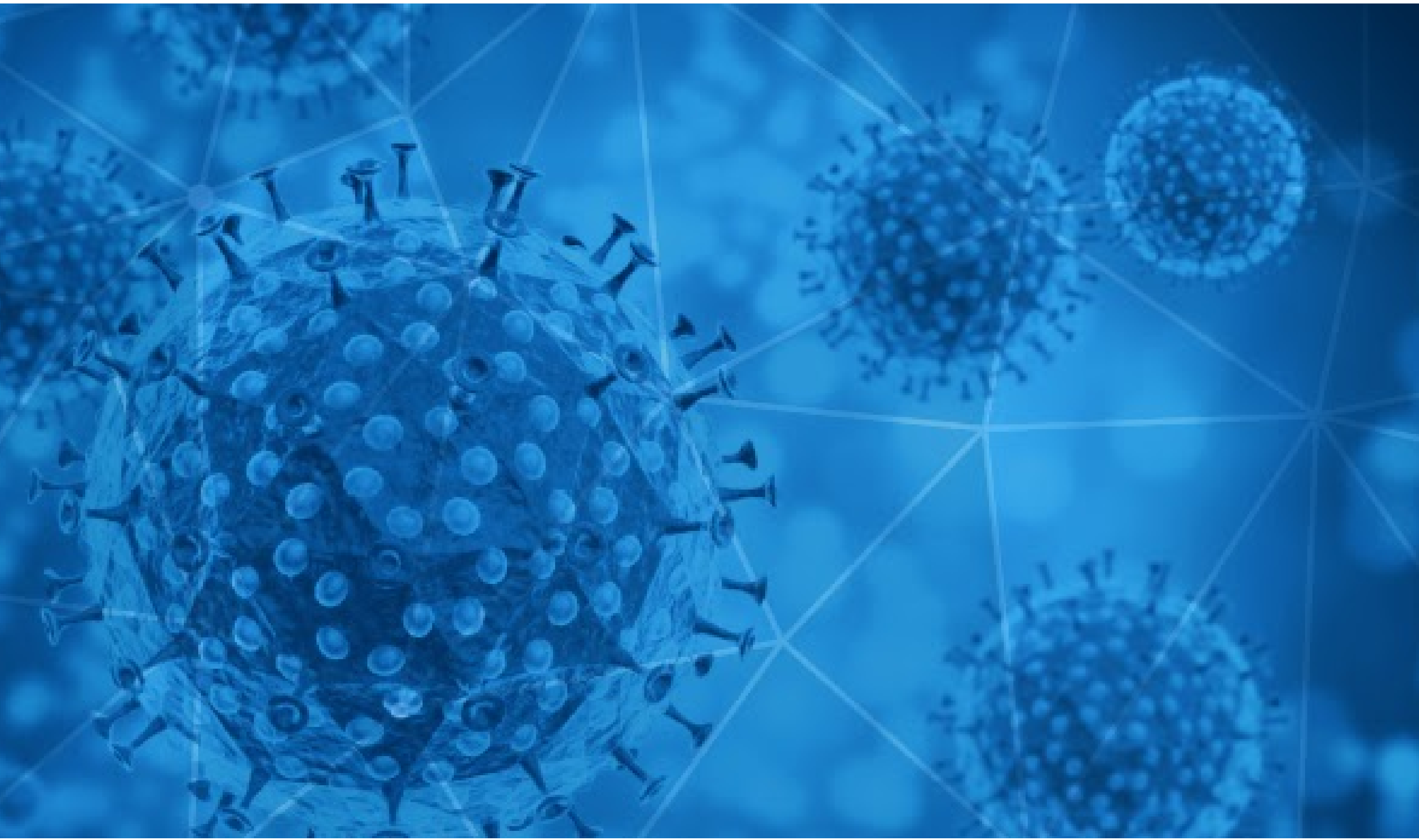


Table of Contents

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.

Digital Exploitation

In a financial disclosure form filed with the U.S. Securities and Exchange Commission Wednesday 04/01/2020, 10x Genomics Inc. said it experienced an attempted ransomware attack that also involved the theft of company data, according to Cyberscoop reporting. A 03/13/2020 tweet from the Israeli security firm Under the Breach reports that attackers using the REvil/Sodinokibi ransomware claimed to steal one terabyte from 10x Genomics.

Trend Micro recently investigated an incident involving a company that was hit by the Nefilim ransomware, which was initially discovered in March 2020. The threat actors using Nefilim in the past have threatened to post the victim's stolen data on an online leak site.

Thousands of potential phishing sites have been created to target Zoom users as usage increases, according to Information Age reporting. According to the report there have been over 3,300 new domain names created containing the word "Zoom" since the beginning of 2020. Over 30% of these new websites have activated an email server which is an indication of these sites being used to process phishing attacks.

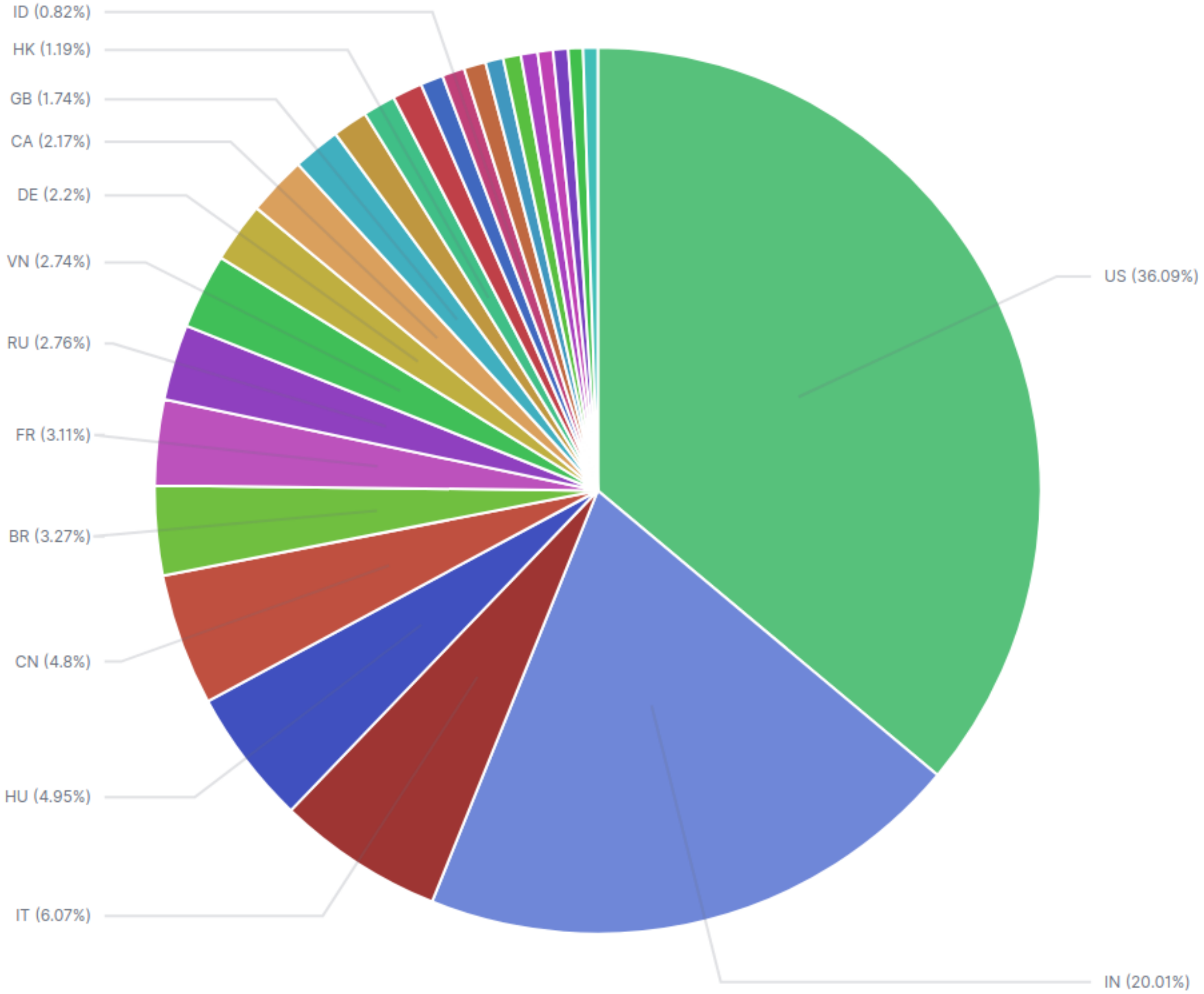
The Internal Revenue Service has seen a wave of new and evolving phishing schemes against taxpayers. On 04/04/2020, the IRS sent out a warning urging taxpayers to be on the lookout for calls and email phishing attempts about COVID-19 which can lead to tax-related fraud and identity theft. According to the warning, taxpayers should also watch out for text messages, websites, and social media attempts that request money or personal information.

New Blacklist Data

Note: No new updates. Please see the COVID-19 Daily Update (dated 04/03/2020) for the most recent data.

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 04/03/2020-04/04/2020. During this period, RiskIQ analyzed 223,697 spam emails containing either "*corona*" or "*covid*" in the subject line. There were 20,779 unique subject lines observed during the reporting period. The spam emails originated from 10,536 unique sending email domains and 18,565 unique SMTP IP Addresses. Analysts identified 241 emails which sent an executable file for Windows machines.



Spam emails by country of origin

Top 25 Subjects

1. 20,997 - The Mask that can prevent Coronavirus now
2. 12,515 - Contribute your bit in fight against COVID-19
3. 10,361 - Coronavirus is spreading, this specialized mask can control it
4. 7,289 - Coronavirus in Italia: il nostro intervento
5. 7,111 - Droht CORONAVIRUS? Mit Atemmaske können Probleme vorgebeugt werden
6. 7,109 - Coronavirus, Grippe? Hier ist die Atemmaske mit einem speziellen Filter
7. 7,083 - Hast du Angst vor dem Corona-Virus? Neue Atemmaske, schütze deine Lieben
8. 7,073 - ATEMMASKE zur Bändigung des Coronavirus - Sicherheit auf FFP2-Ebene
9. 7,065 - Kann das CORONAVIRUS vorgebeugt werden? Atemmaske für wirksamen Schutz
10. 6,980 - Würdest du das CORONAVIRUS stoppen? Die Atemmaske schützt auch vor neue Infektion
11. 4,071 - Ethical Covid-19 Pandemic Supplier
12. 3,931 - TIMES TOP10: Domino effect of Covid-19 healthcare crisis
13. 3,637 - Message from Airtel CEO - Keeping you connected during COVID - 19
14. 3,182 - The Corona Letter: A mammoth task at Dharavi
15. 2,255 - Coronavirus Protection Face Mask (Must See)
16. 2,160 - Re: UN COVID-19 Stimulus
17. 2,063 - The 3 plants you need to throw in your shopping cart to fight coronavirus
18. 2,026 - This Mask Stops Coronavirus
19. 2,020 - COVID19 Offer -85%
20. 1,895 - H-1B woes: US body requests Trump to suspend the visa program | COVID-19: These tech companies took the no-layoffs pledge
21. 1,843 - Myschool Give-Away: COVID-19 Stay-at-Home CBT and Essay Challenge + 2 JAMB Updates
22. 1,808 - Global coronavirus cases top 1 million, what you need to know about masks, and more from Apple News
23. 1,769 - ✅ Corona Virus Reusable Protective Mask for Adult and Kids

24. 1,271 - Anti Coronavirus Disease COVID-19!

25. 889 - New Corona-virus Shield Mask!

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

1. 95 - COVID-19 UPDATE !!!

2. 82 - Pending Delivery Status for Shipment of Goods (International transport - COVID-19 - Update March 31

3. 42 - nCov-19 _CoronaVirus_Safety__Precautionary_Measure.pdf

4. 20 - Re: CF&FDA FOB MOQ Test Kits covid-19

5. 1 - URGENT NEED: U.S. Department of Health & Human Services/COVID-19 Face Mask/ Forehead thermometer

6. 1 - Orientações Sindicais COVID 19

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

1. 70,864 US
2. 39,282 IN
3. 11,924 IT
4. 9,710 HU
5. 9,426 CN
6. 6,427 BR
7. 6,109 FR
8. 5,419 RU
9. 5,380 VN
10. 4,320 DE
11. 4,252 CA
12. 3,409 GB
13. 2,512 AR
14. 2,330 HK
15. 2,142 UA
16. 1,622 ES
17. 1,617 ID
18. 1,568 KR
19. 1,278 ZA
20. 1,274 MY
21. 1,198 CO
22. 1,096 BD
23. 1,078 NL
24. 1,048 IL
25. 1,045 SG

COVID-19 Host, Domain, and Mobile App Tracking

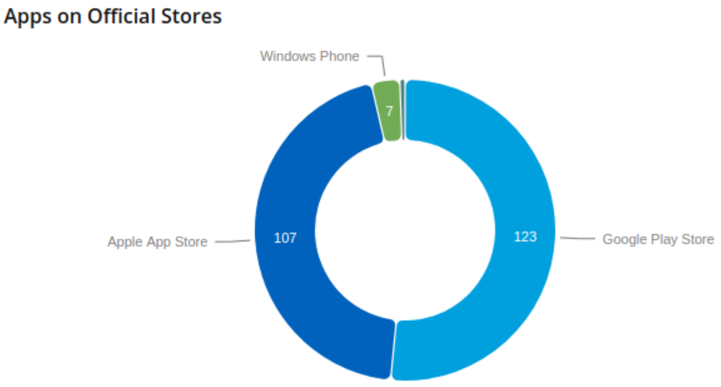
RiskIQ gathers data relating to newly-observed hosts and domains containing COVID-19, COVID19, or Coronavirus in the host or domain name and mobile apps containing COVID-19, COVID19, or Coronavirus in the title or description. A summary of data collected is contained in this section.

Domains and Hosts

Domains: 49,336
Hosts: 55,392
Hosts and Domains with Potential Mail Servers: 243
Email-Capable Domains and Hosts: 17,529
Live Hosts and Domains Not Parked: 22,504

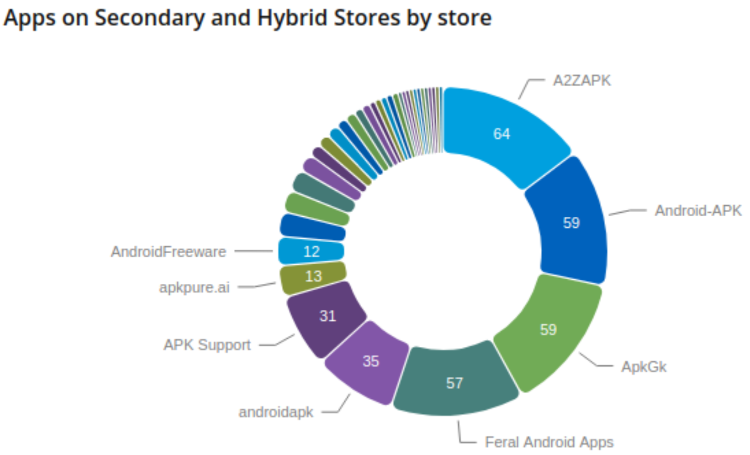
Mobile Apps

1. Apps in Official Stores: 238 (See Graph)
   a. Google Play Store: 123
   b. Apple App Store: 107
   c. Windows Phone: 7
   d. Amazon: 1



2. Apps in Secondary/Hybrid Stores: 416 (See Graph)

3. Blacklisted Mobile Apps by Store Type:
   a. Secondary: 16
   b. Hybrid: 1



End Report