Beyond the Virus: A First Look at Coronavirus-themed Mobile Malware

Ren He  
Beijing University of Posts and Telecommunications, China

Haoyu Wang  
Beijing University of Posts and Telecommunications, China

Pengcheng Xia  
Beijing University of Posts and Telecommunications, China

Liu Wang  
Beijing University of Posts and Telecommunications, China

Yuanchun Li  
Microsoft Research Asia, China

Lei Wu  
Zhejiang University, China

Xiapu Luo  
The Hong Kong Polytechnic University, China

Yao Guo  
Peking University, China

Guoai Xu  
Beijing University of Posts and Telecommunications, China

ABSTRACT

As the COVID-19 pandemic emerges in early 2020, a number of campaigns have started capitalizing the topic. Although a few media reports mentioned the existence of coronavirus-themed mobile malware, the research community lacks the understanding of the landscape of the coronavirus-themed mobile malware, and there is no publicly accessible dataset that could be utilized to boost the related research.

In this paper, we present the first systematic study of coronavirus-themed mobile malware. We first make efforts to create a daily growing COVID-19 themed mobile app dataset, which contains 2,016 COVID-19 themed apps and 277 malware samples by the time of May 26, 2020. We then present an analysis of these apps from multiple perspectives including popularity and trends, installation methods, malicious behaviors and malicious campaigns. We observe that the growth of the number of COVID-19 themed apps is highly related to the number of confirmed cases of COVID-19 in the world. Most of them were released through distribution channels beyond app markets. A majority of the malicious apps (over 53%) are camouflaged as official apps using the same app identifiers and some of them use confusing similar app icons with the official ones to mislead users. Their main purposes are either stealing users’ private information or making profit by using the tricks like phishing and extortion. Furthermore, we find that only 40% of the COVID-19 malware creators are habitual developers who are active for a long time, while 60% of them are new emerging ones in this pandemic and only released COVID-19 themed malware. The malicious developers are mainly located in US, mostly targeting countries including English countries, Arabic countries, Europe and China. To facilitate future research, we have publicly released all the well-labelled COVID-19 themed apps (and malware) to the research community.

1 INTRODUCTION

As COVID-19 continues to spread across the world, a growing number of malicious campaigns are exploiting the pandemic. It is reported that COVID-19 is being used in a variety of online malicious activities, including Email scam, ransomware and malicious domains [5, 6, 9, 11, 20]. As the number of the afflicted cases continue to surge, malicious campaigns that use coronavirus as a lure are increasing.

Smartphone, as one of the most popular ways to keep track of the most up-to-date status of the pandemic and receive notifications, has always been the major target of the malicious campaigns. As the coronavirus outbreak increased in severity across the world, people tend to use mobile apps that can provide information on actions for avoiding infection, updates regarding COVID-19, as well as medical services. Thus, malicious developers take advantage of this opportunity to lure mobile users to download and install malicious apps. Indeed, some news reports [7, 8, 10, 16], show that COVID-19 related malicious apps have been observed, and thousands of mobile users have been affected in another way (by the virtual Virus) in this pandemic. For example, the malicious website (coronavirusapp.site) prompts users to download a malicious Android App that will give them access to a coronavirus map tracker that appears to provide tracking and statistical information about COVID-19. However, the app is indeed a ransomware that locks users’ screen, which requests $100 in Bitcoin to unlock the phone.

However, besides a few media reports, the coronavirus-themed mobile malware has not been well studied. Our community lacks of the comprehensive understanding of the
landscape of the coronavirus-themed mobile malware, and no accessible dataset could be used by our researchers to boost COVID-19 related cybersecurity studies.

This Work. To this end, this paper presents the first measurement study of COVID-19 related Android malware. We first make efforts to create a daily growing COVID-19 related mobile app dataset (see Section 2.2), by collecting samples from a number of sources, including app markets (both Google Play and alternative app markets), a well-known app repository (i.e., Koodous) and the COVID-19 related domains (apps downloaded or connected to these domains). By the time of paper writing, we have curated a dataset of 2,016 COVID-19 themed apps, and 277 of them are considered to be malicious. The growth of the number of COVID-19 themed apps is highly related to the number of confirmed infected cases in the world. A number of COVID-19 themed apps have shown discriminatory in app identifier naming (app name and package name).

- **COVID-19 themed mobile apps and malware are prevalent.** We have identified over 2,000 COVID-19 theme Android apps by the end of May 1, and most of them were released after March 15, the time when coronavirus becomes a pandemic. Among them, 277 apps are considered to be malicious. The growth of the number of COVID-19 themed apps is highly related to the number of confirmed infected cases in the world. A number of COVID-19 themed apps have shown discriminatory in app identifier naming (app name and package name).

- **Fake app is the main way to lure users to install malware.** Most of the malicious apps (over 53%) are camouflaged as official apps using the same app identifiers (both app name and package name), and a number of them use confusing similar app icons to mislead users. However, app repackaging is no longer the main way to create COVID-19 themed Android malware, with only 18% of them are considered to be repackaged from official apps.

- **Information Stealing, Phishing and Extortion are the major behaviors of COVID-19 themed Android malware.** Trojan and Spyware are the two main categories for COVID-19 themed malware. Their purposes are either stealing users’ private information, or making profit using tricks like phishing, premium SMS/Phone calls, stealing bank accounts, and extortion. Besides, anti-analysis techniques are used by roughly 52% of these malicious apps.

- **COVID-19 themed malicious apps are created by experienced campaigns.** 40% of the COVID-19 themed malware developers are known malicious campaigns that released apps before this pandemic, and 60% of them are new emerging malicious developers. Coronavirus is used as a lure to attack unsuspicious users. We have collected over 125k apps released by these developers (from 2014 to 2020), and found most of them are malicious. Based on the information extracted from the malicious apps, these developers are mainly located in US, with rest of them are located in India, Turkey, etc. Besides English countries, the Arabic countries, Europe, and China are also the main targets of them.

To boost the research on coronavirus-themed cybersecurity threats, We have released a daily growing dataset to the research community at:

https://covid19apps.github.io

2 STUDY DESIGN

2.1 Research Questions

Our study is driven by the following research questions:

RQ1 **Popularity and Trends.** How many coronavirus-themed apps are there in the world and how many of them are considered to be potential harmful? Considering that the coronavirus pandemic is emerging since early 2020, it is thus interesting to investigate when the COVID-19 themed apps (and malware) are increasingly popular and whether they follow the similar trends with the confirmed infected COVID-19 cases over the time.

RQ2 **App Creation and Installation.** It is known to us that the COVID-19 themed malicious apps are taking advantage of the pandemic to attract and lure users to install them. However, it is still unknown to us how these apps are created and how they can get installed into users’ smartphones.

RQ3 **Malicious Behaviors** Considering the mobile malware has been widely studied, it is important to study the characteristics of the COVID-19 themed malware. What are the malicious behaviors of them? Do they apply any anti-analysis techniques to evade detection?

RQ4 **Attackers and Malicious Campaigns** Who create these malware? Who are their main targets? Can we identify the behind malicious campaigns?

2.2 Dataset Collection

2.2.1 **Dataset Collection Method.** To answer the aforementioned research questions, we first need to harvest a comprehensive dataset of coronavirus-themed apps. Considering that a number of malware may distributed through channels
beyond the general app markets [44], we have adopted a hybrid approach to collect COVID-19 themed apps, and further identify the malicious ones using VirusTotal.

**Collecting the Related Apps.** We collect coronavirus-themed apps from three main sources:

1. **App Markets.** App markets (including Google Play and alternative markets) are the general distribution channels for mobile apps. Previous research [44] suggested that malicious apps were concurrently found in app markets. Thus, we first manually crafted a set of 3 keywords (including 'coronavirus', 'COVID-19', and 'corona') and their squatting ones (e.g., cor'a'na, cor'a'nivirus, and coron'o'virus) as our keyword list. Then we use these keywords as the seeds to search related apps on Google Play and 5 alternative markets, including Apkpure [3], Uptodown [18], Appchina [4], Tencent MyApp Market [15], and Huawei Market [13]. Note that Apkpure and Uptodown are two most popular alternative app markets for western countries, while Huawei and Tencent Myapp are the most popular app markets in China. Based on the search results, we further manually check the app name, package name and app description to identify the truly related apps.

2. **Existing App Repositories.** Prior work [30, 31] suggested that app market is not the only way to distribute apps, especially for malware. Malicious apps can be distributed through online forum, Email, SMS, social network, mobile advertisement, and other channels. Thus, some app repositories are created and maintained to provide us a chance to analyze apps beyond app markets. To the best of our knowledge, Koodous [14] is by far the largest Android app repository, with over 58 million apps in total, and the number is growing rapidly daily. The samples on Koodous are collected from various resources, including app markets, webpages, and thousands of researchers. Thus, we use the aforementioned keywords to crawl related apps from Koodous, and keep only the apps have at least one keyword in their app names or package names.

3. **Apps related to the known COVID-19 themed domains.** Some apps are distributed through COVID-19 related websites (e.g., www.covid19-app.com). Thus, we take advantage of URLScan [19], a URL and website scanner for potentially malicious websites, to collect coronavirus-themed domains first. We use the aforementioned keywords to identify related domains from URLScan, and we have collected 175,966 domains. Then, we use VirusTotal [21], an online-service to analyze all the collected domains, to get the files related to these domains. For each domain, VirusTotal provides the useful information including files downloaded from this domain, files connected to this domain, and files referred to this domain (the domain name was hard-coded in the files). We have collected over 1 million related files associated with these domains. Note that we only keep the Android apk files whose name or package name contains one of our keywords. We further use VirusTotal to collect the metadata information of these apps, e.g., app name, package name, apk file hashing, released date and developer signature, etc.

**Filtering the False Positives.** Our keyword-based collection may cause false positives, e.g., Corona Beer app would appear in our search results. Thus, we further remove the irrelevant apps based on following two criteria: (1) **release date must be later than December 2019**, as the first confirmed COVID-19 case was in Dec 2019. Therefore, no coronavirus-themed apps would be released earlier than this time; (2) **the apps should not have identical names with well-known brands**. The official apps released by two famous brands would appear in our search results. The name 'Corona' is both the name of a beer brand and a car brand. Thus, we manually remove apps related to this two brands.

| Source       | # Apps | # Malware | # Malicious developers | # Families |
|--------------|--------|-----------|------------------------|------------|
| App Markets  | 24     | 0         | 0                      | 0          |
| Koodous      | 1,882  | 251       | 60                     | 31         |
| Domain       | 243    | 48        | 31                     | 12         |
| **Total**    | 2,016  | 277       | 68                     | 34         |

**Dataset Overview.** Finally, we have collected 2,016 coronavirus-themed apps, released January 2020 to May 2020. Only 24 of them were collected from app markets (6 of them were from Google Play), 243 of them were collected from COVID-19 related domains, and 1,882 of them were collected from Koodous. Note that, we have downloaded all the binary files of these apps, as well as their meta-information (if available). Our binary files are collected based on the premium services provided by Koodous and VirusTotal. The overall distribution of our dataset is shown in Table 1.

**Labelling the maliciousness of the apps.** In order to identify the malware, we upload all the 2,016 apps to VirusTotal, a widely-used online service aggregated with over 60 anti-virus engines. There are 277 apps in our dataset flagged by at least one engine on VirusTotal, which will be regarded as the malicious apps in this paper. We know that using this
method to label malware might not be reliable according to previous studies, however, without loss of generality, we define the maliciousness of an app by the number of AVs that recognize it as malware (i.e., short for AV-rank), following previous measurement studies [32, 43, 44]. Then we take advantage of AVClass [39], a widely used malware labelling tool to get their malware family names (see Section 5). After these steps, we identity 277 malware samples (with AV-rank ≥ 1) that belong to 34 different families.

3 GENERAL OVERVIEW

For each app, we define its appear time as the earliest time we found from the various data sources. For example, we have crawled the app upload time from Koodous, the app scan time (first and latest) from VrusesTotal, and app upload time from app markets. The earliest one would be regarded as its appear time. The distribution of the appear time for the 2,016 COVID-19 themed apps and the 277 malware (with AV-rank ≥ 1) is shown in Figure 1.

3.1 Popularity and trends

The earliest app in our dataset was released on January 26, which is indeed a COVID-19 themed ransomware. We can observe that, the number of coronavirus related apps is quite low before March 15 (261 COVID-19 related apps and only 21 of them are considered to be malicious with AV-rank ≥ 1). After March 15, the number of COVID-19 themed apps is increasing rapidly. To further analyze whether they have strong correlation with the confirmed COVID-19 cases over the time, Figure 1 presents the number of confirmed cases around the world for comparison, which is provided by Johns Hopkins University. It is interesting to see that, the number of COVID-19 related apps shows a rapid growth trend with the sharp increase in the number of confirmed people. As of March 15, the COVID-19 is beginning to explode globally and the number of confirmed people has risen sharply. Meanwhile, the number of COVID-19 related apps is increasing and the number of malware also shows the same trend. To be specific, we calculate the Pearson Correlation Coefficient [17] between the number of COVID-19 related apps (malware) and the number of confirmed infected cases around the world, based on the following definition:

\[ r = \frac{\sum(X - \bar{X})(Y - \bar{Y})}{\sqrt{\sum(X - \bar{X})^2}(\sum(Y - \bar{Y})^2)} \]

The Pearson correlation coefficient is 0.954 between the number of released apps and the number of confirmed cases, and 0.965 between the number of released malware and the number of confirmed cases. The Pearson correlation coefficient indicates that the closer the correlation coefficient is to 1, the stronger the positive correlation. We further calculate the confidence interval. The confidence interval values of the two data are 8.79e-10 and 1.0e-10 respectively. A confidence interval value of less than 0.05 indicates that the two sets of data are significantly related and have statistical significance. Thus, it suggests that the growth of the number of COVID-19 related apps (malware) and the growth of the number of confirmed infected cases around the world are highly correlated.

3.2 The discriminatory in app naming

The World Health Organization (WHO) stated that the naming of the new virus should avoid carrying discriminatory information such as country names or city names [23]. On February 11, WHO officially named the new coronavirus as "COVID-19". However, there are 20 apps in our collected dataset contain discriminatory names in their app names or package names. For example, 19 of them contain "Wuhan" discriminatory names, e.g., Wuhan Corona Live Statistics. Most of them were released later than February and 4 of them were flagged as malware by anti-virus engines.

3.3 Relation with COVID-19 domains.

For the 48 malicious apps that are correlated with 37 COVID-19 related domains (see Table 1), we further analyze their relations. Two kinds of app-domain relations are considered in this paper: (1) downloading relationship, i.e., the malicious app can be downloaded from the corresponding domain and (2) communicating relationship, i.e., the malicious app communicates with the domain. Based on these two relations, we have classified malicious apps and their corresponding domains into the following four categories (see Figure 2).
For the 37 COVID-19 themed domains, 26 of them (70%) are flagged as malicious by VirusTotal. The remaining of them are websites that APIs that provide COVID-19 related information and statistics (e.g., https://corona.lmao.ninja/), which could be integrated by any apps.

**RQ #1:** There are over 2,000 COVID-19 related apps by the time of our study, and 277 of them are considered to be malicious (with AV-rank ≥ 1). Most of them were released through channels beyond app markets, e.g., COVID-19 themed domains are used to distribute malware. Most of them were released after March 15, the time when the coronavirus becomes a pandemic. The growth rate of the number of COVID-19 themed apps is highly related with the number of confirmed cases all over the world. Furthermore, a number of COVID-19 themed apps have shown discriminatory in app naming.

### 4 APP CREATION AND INSTALLATION

We further investigate how these COVID-19 themed malicious apps were created and how do they trick users to install them. Based on previous studies [44, 47, 48], we consider two kinds of tricks here: (1) **fake apps**, and (2) **repackaged apps**. Previous work [30, 48] suggested that they are the main ways to trick users to install malicious apps. A ‘fake app’ masquerades as the legitimate one by mimicking the look or functionality. As suggested by previous studies [30, 34], fake apps usually have identical app names, package names or app icons to the original ones. While a “repackaged app” often shares a large portion of the code with the original app (e.g., by decompiling the original app and inserting a
malicious payload), they are obviously signed by different developers.

Table 2: The Targets of Fake Apps with the Same Identifier Names.

| App Name      | Package Name               | Downloads On GPlay | # Fake apps |
|---------------|----------------------------|--------------------|-------------|
| COVID-19      | com.Eha.covid_19            | 100,000+           | 75          |
| Coronavirus   | br.gov.datasus.guardihoes  | 1,000,000+         | 51          |
| COVID Tracker | com.joinzoe.covid_zoe      | 500,000+           | 20          |

4.1 Fake Apps

To quantify the presence of fake apps among our collection, our study was performed based on app identifiers and app icons respectively.

Fake Apps with the Same App Identifiers. We take the following approach: if a malicious app shares the same app name or package name with an official COVID-19 related app in the official market (i.e., Google Play) but with different developer signatures, we will regard it as a fake app. This approach is widely used in previous studies [43, 44]. To this end, we have identified 146 fake apps out of 277 malicious apps (53%). This result is inline with the previous Android malware study. These fake apps are targeting three official apps published in Google Play, as shown in Table 2. These three official apps are released by the governments of British, Brazilian, and Vietnamese respectively, which are used to inform the public about the real-time situation of the outbreak, official announcements, and health notices, etc. All of these three official apps have received more than 100,000 downloads on google play. In our collection, 75 malware samples have the name "COVID-19", and 51 samples have the name "Coronavirus", and 20 of them have the name "COVID Tracker".

Fake Apps with Same/Similar App Icons. We further extract the icons of all the 277 coronavirus-themed malware (with AV-rank \( \geq 1 \)), and compare these icons with the officially apps to explore whether the attackers used icons to deceive users. In this study, on one hand, we take advantage of Dup Detector\(^9\) to identify similar icons. This tool is proved to

\(^9\)https://www.keronsoft.com/dupdetector.html
be effective in finding duplicate and similar images by comparing image pixel data, and used in many other research studies. On the other hand, the first three authors of this paper perform manually examination of all the icons to identify the similar ones.

For the 227 malware, we obtain 121 unique app icons, which are shown in Figure 3. To save space, we only shown 82 different app icons of COVID-19 themed malware. Most malicious apps use coronavirus themed icons to induce users to download, which makes them appear more professional and credible. Besides, there are 43 malicious apps use Android’s default icon. After comparing with the official app icons, 19 of them use similar app icons to one official app\textsuperscript{10} (app name: Coronavirus), which is released by the Brazilian government to notify the outbreak situation. Besides, some apps are posing as other trusty organizations, e.g., some of them use the WHO logo as their icons to deceive users\textsuperscript{11}, while some of them use the Google Play icons.

4.2 Repackaged Apps

We further analyze how many of the malicious apps were repackaged from the official/benign apps, and whether the malicious developers reuse the same malicious payload to create a number of malware.

Code Similarity We use FSquaDRA2\textsuperscript{28} tool to calculate code similarity between apk files and cluster them, which is widely adopted by previous studies [31]. FSquaDRA2 uses Jaccard distance to measure the bytecode of two apps. Jaccard distance, also known as Jaccard similarity coefficient, is used to compare the similarity and difference between limited sample sets. The higher the Jaccard coefficient value, the higher the sample similarity. We empirically set the similarity threshold as 80% to cluster apps into groups based on previous work [31]. Note that, for apps with multiple versions (released by the same developer), we randomly leave one app during the app clustering phase. In other words, each cluster contains at least 2 different apps (with different package name or developed by different developers).

Finally, we cluster 344 apks into 28 clusters and 1,564 isolated apps, as shown in Figure 4. Each node represents a coronavirus-themed app, where red node indicates the malicious app (with AV-rank ≥ 1) and blue one indicates the benign app. For each cluster, we randomly select one app and use edges to represent its similarity with other apps in the same cluster, i.e., the shorter the edge, the more similar they are.

Note that, only 50 malicious apps (18%) have been grouped into 13 clusters, which means that most of the malicious apps are not repackaged based on existing COVID-19 benign apps.

\textsuperscript{10}https://play.google.com/store/apps/details?id=br.gov.datasus.guardioes
\textsuperscript{11}An example app with MD5: 15e5a00c5d4ec8b4bbd0ebc70f0806aa

This result is different with previous malware study [48] that over 80% of malware samples are created based on app repackaging. It is further interesting to observe that, for the 13 clusters that contains malware, 11 of them contains both benign and malicious apps, and two clusters contains only malicious apps. Thus, we further select representative clusters for manually examination.

Cluster A. In cluster A, these are 65 coronavirus-themed apps and 4 of them are detected as malware. These three malicious apps are detected as spyware, belonging to the spyagent family. The repackaged malware request more than 20 permissions (the average request permissions of benign apps in the same cluster is 13), including some sensitive permissions such as READ_CALL_LOG, READ_SMS, ACCESS_FINE_LOCATION, USE_CREDENTIALS, etc. Meanwhile, the developer add functions to obtain user privacy data, send text messages, and make phone calls in the original apps, which makes them a spyware.

Cluster B. There are 58 benign apps and 2 malicious apps in cluster B. These two malware samples are very similar to other benign apps at the code level, and the Jaccard coefficient exceeds 0.9. After further analysis, we find that all the 40
Table 3: Top 10 COVID-19 themed malware with the highest malicious rank.

| App Name                | MD5                                      | AV-RANK | Family |
|-------------------------|------------------------------------------|---------|--------|
| Corona Safety Mask      | d7d43c0bf6d4828f1545017f34b5b54c         | 36      | piombo |
| Covid19                 | e8296fc617498c8a8db88db0f0cfa           | 34      | anubis |
| Covid19                 | 9ac81fa4ecce1ca6f6dc27883f2521           | 33      | anubis |
| Coronavirus             | dad9d0c3f968dc1c12c53bb851bb            | 29      | cerberus |
| V-Aler COVID-19         | b24ae9e8b4d4dc1ced5db33e6683            | 29      | hawpar |
| Coronavirus             | c8328a55e1c340c1b4c7ca62ad7f949          | 29      | hawpar |
| Coronavirus             | 3b5eb6cded604c1828d03096b73e59953eb      | 28      | locker |
| Coronavirus Tracker     | 3a7070a1fa932fe1ccc189e89e3a799fd        | 28      | anubis |
| Coronavirus Tracker 69  | 8937b7070a1fa932fe1ccc189e89e3a799fd     | 28      | hawpar |

apps have similar package names "org.chromium.webapk.". The two malware are created by a different developer (with different certificate hashes). The malicious developer repackages the benign apps and add a third-party advertising library, which is detected as adware.

**Cluster E.** All 17 apps in the cluster E are detected as malware. The app names of these apps are identical (named "Coronavirus"), but their package names are different. We find that their package names are meaningless, which seems to be obfuscated, such as "rnwjzlri.qiapwncqriqy.oyfsuikw", "bqehzgygllllhs.kupgk-ubu.erpwzdnhfmtqwy", etc. We further extract the developer certificates of these malware and find that these apps are signed by the same developer signature. However, the developer certificate is an Android common key and cannot be traced. As to their malicious behaviors, these malware use phishing window coverage and keystroke recording to steal victim’s bank account information and credentials, which belong to the Cerberus family, a well-known banking Trojan.

**RQ #2:** We investigate two main social-engineering based techniques (fake apps and repackaged apps) that are used by malware to trick users to install them. Most of the malicious apps (over 53%) are camouflaged as official apps using the same app identifiers, and a number of them use confusing similar app icons to mislead users. However, only a few of them (18%) are repackaged from existing COVID-19 benign apps.

5 MALICIOUS BEHAVIORS

As aforementioned, 277 covid-19 themed apps were flagged by at least one anti-virus engine on VirusTotal (with AV-rank ≥ 1). Among them, 145 samples were flagged as malware by at least 10 engines on VirusTotal (with AV-rank ≥ 10). Table 3 shows top-10 of them ranked by the number of flagged engines. We next investigate the malicious behaviors of these 277 apps from malware category, malware family and anti-analysis techniques.

5.1 Malware Category

We follow the malware categories provided by Microsoft for malware category classification. Based on the AV-labels provided by VirusTotal and the family labels generated by AV-Class, we have classified the malware samples into five main categories, including Trojan, Ransomware, Adware, Riskware and Spyware.

**Trojan.** Trojans that run on the Android operating system are usually either specially-crafted programs that are designed to look like desirable software, or copies of legitimate programs that have been repackaged or trojanized to include harmful components. For example, the malware (app name: CORONA TAKIP) is a banking Trojan targeting Turkish users that belongs to the Anubis family. This malware disguises as an app to provide coronavirus information. However, it requires excessive permissions when it is installed and activated. Furthermore, it shows a phishing user interface (i.e., a bank login UI) at runtime to steal the victim’s bank account, as shown in Figure 6 (a).

**Riskware.** Riskware is created by malicious developers to delete, block, modify or copy the victim’s data, and destroy the performance of the devices or the network. For example, 16
the malware\(^{17}\) (app name: Covid-19 Visualizer) is detected as Fakeapp family, which disguises as a normal software that provides real-time query of the COVID-19 outbreak. Once it launched, the malware will remind user to install the "Adobe Flash" plugin to display the entire content. After obtaining user authorization, the malware will run in the background and leak user’s privacy data, intercept phone calls and SMS messages.

Spyware. Android Spyware is the apps that record information about mobile users or what mobile users do on their phones without users’ knowledge. RAT (remote administration tool) is a kinds of popular spyware on Android, and there are a number of RAT frameworks can be used to create spyware. Android Spyware usually collects victim’s privacy data, call record, message record and photo and sends to the hackers secretly. For example, the malware (package name: kg.cdt.-stopcovid\(^{18}\)) is detected as Datacollector family, which steals the user’s personal privacy and sends it to the attacker.

Adware. Adware is a form of malware that hides on user’s device and serves aggressive (or fraudulent) advertisements. Some adware also monitors users’ behavior online so it can target users with specific ads. For example, the adware named "Coronavirus Tracker"\(^{19}\) is detected as the Hiddenads family. Once launched, it informs the user "not available in your country" and uninstall itself. Actually, it just hides the app icon and keeps running in the background. The malware pops up some aggressive advertisements at intervals, as shown in Figure 6 (b).

Ransomware. Once it launched, the ransomware will lock the victim’s devices or files and force the user to pay a ransom to protect their important data. As shown in Figure 6 (c), the malware\(^{20}\) disguises as the Coronavirus Tracker app to provide information about the COVID-19. In fact, it is a ransomware that locks the victim’s file system and asks for Bitcoin. Specifically, the Bitcoin address\(^{21}\) is not hardcoded in the APK file. Once clicking the button shown on the locking UI, it will redirect users to an external page that shows the real Bitcoin address.

5.2 Malware Family

We further use AVClass [39], a widely used malware family tagging tool to label the malware family name for each sample. These malicious apps are classified into 34 families. Note that, AVClass cannot label the family name for all the flagged apps. In our study, only 137 apps can be labelled with family names. As shown on Table 4, we list the distribution of all the malware families.

For each malware family, we manually select two apps from our dataset (if there are more than two apps in this family) and perform manually examination to label their malicious behaviors. Our manually analysis consists of two parts: (1) Static analysis. Our static analysis includes extracting the declared permissions and component information from the Manifest file, analyzing the embedded third-party libraries based on LibRadar [37], pinpointing the sensitive API invocation, and analyzing the sensitive information flow using FlowDroid [24]. Based on these information, we can know whether the malicious apps perform SMS/CALL related activities, invoke aggressive advertising libraries, release private information, and other sensitive behaviors. (2) Dynamic analysis. We first install these apps on the real smartphone, and check their behaviors by interacting with them using both DroidBot [35] (a widely used automated testing tool for Android) and manually clicking. During runtime, we can check whether the malicious apps show aggressive and annoying advertisement, redirect users to malicious and fraudulent websites, and lock users’ phone. Besides, we have recorded all the the network traffic to check whether the malware communicates with the remote server.
Table 4: Malicious Behaviors of the COVID-19 Themed Malware (Classified by Malware Family).

| Family Name | # Malware | Malware Category | Malicious Behaviour |
|-------------|-----------|------------------|---------------------|
|             |           |                  | Privacy Stealing   | SMS/Phone Calls | Remote Control | Bank Stealing | Ransom | Ads |
| hqwar       | 29        | Trojan           | ✓                   | ✓               | ✓              |             |        |     |
| spynote     | 22        | Spyware          | ✓                   | ✓               | ✓              |             |        |     |
| frdt        | 15        | Trojan           | ✓                   | ✓               | ✓              |             |        |     |
| anubis      | 13        | Trojan           | ✓                   | ✓               | ✓              | ✓            |        |     |
| cerberus    | 7         | Trojan           | ✓                   | ✓               | ✓              |             |        |     |
| locker      | 5         | Ransom           | ✓                   | ✓               | ✓              |             |        | ✓   |
| hiddad      | 4         | Adware           | ✓                   | ✓               | ✓              |             |        |     |
| svpeng      | 3         | Trojan           | ✓                   | ✓               | ✓              | ✓            | ✓       |     |
| fhab        | 3         | Trojan           | ✓                   | ✓               | ✓              |             |        |     |
| fftm        | 3         | Trojan           | ✓                   | ✓               | ✓              |             |        |     |
| fakeapp     | 3         | Riskware         | ✓                   | ✓               | ✓              |             | ✓       |     |
| metasploit  | 3         | Ransom           | ✓                   | ✓               | ✓              |             |        | ✓   |
| fooz        | 2         | Trojan           | ✓                   | ✓               | ✓              |             | ✓       |     |
| boogr       | 2         | Trojan           | ✓                   | ✓               | ✓              |             | ✓       |     |
| dnotua      | 2         | Trojan           | ✓                   | ✓               | ✓              |             | ✓       |     |
| spyagent    | 2         | Spyware          | ✓                   | ✓               | ✓              |             | ✓       |     |
| bodegun     | 2         | Adware           | ✓                   | ✓               | ✓              |             | ✓       |     |
| flug        | 1         | Trojan           | ✓                   | ✓               | ✓              |             | ✓       |     |
| fnad        | 1         | Trojan           | ✓                   | ✓               | ✓              |             | ✓       |     |
| fazn        | 1         | Trojan           | ✓                   | ✓               | ✓              |             | ✓       |     |
| uten        | 1         | Trojan           | ✓                   | ✓               | ✓              |             | ✓       |     |
| piom        | 1         | Trojan           | ✓                   | ✓               | ✓              |             | ✓       |     |
| piom        | 1         | Trojan           | ✓                   | ✓               | ✓              |             | ✓       |     |
| casdet      | 1         | Spyware          | ✓                   | ✓               | ✓              |             | ✓       |     |
| sandr       | 1         | Spyware          | ✓                   | ✓               | ✓              |             | ✓       |     |
| ahmyth      | 1         | Spyware          | ✓                   | ✓               | ✓              |             | ✓       |     |
| datacollector | 1     | Spyware          | ✓                   | ✓               | ✓              |             | ✓       |     |
| cgw         | 1         | Spyware          | ✓                   | ✓               | ✓              |             | ✓       |     |
| utilcode    | 1         | Spyware          | ✓                   | ✓               | ✓              |             | ✓       |     |
| xploitspy   | 1         | Spyware          | ✓                   | ✓               | ✓              |             | ✓       |     |
| hiddenapp   | 1         | Riskware         | ✓                   | ✓               | ✓              |             | ✓       |     |
| lockscreen  | 1         | Ransom           | ✓                   | ✓               | ✓              |             | ✓       |     |
| ewind       | 1         | Adware           | ✓                   | ✓               | ✓              |             | ✓       | ✓   |

Based on the aforementioned exploration, we have classified the malicious behaviors into six major categories (see Table 4), including Privacy Stealing, Send SMS/Phone Calls, Remote Control, Ransom, and Aggressive Advertisement. We can observe that most of the COVID-19 related malware families have the privacy stealing behaviors, i.e., over 91.3% of them illegally steal user personal data without declaring the proper purposes of permission use. To be specific, we have investigated how COVID-19 malicious apps request sensitive permissions. Figure 7 shows the top-15 sensitive permissions used in these apps. It is surprising to see that, sensitive permissions like "Call Phone", "Read Contacts", "Access Fine Location", "Read SMS", and "Camera" are widely used in these apps. Some malicious apps even use the sensitive permissions that only available in the latest Android SDK versions. For example, ACCESS_BACKGROUND_LOCATION and ACTIVITY_RECOGNITION are introduced in API level 29 (Android 9.0), which allow an app to access location in the background and recognize physical activities, respectively. Remote control is the second largest behavior category. These malicious apps communicate with remote C&C servers and receive commands from the server to perform related malicious behavior and send the collected data to the attacker. We have identified 17 families receive commands from remote services. Rough 37.2% malware families have the behaviors of sending text messages or making phone calls. These malware send high-rate SMS message, call phones or subscribe to without user authorization to obtain financial benefits. Besides, 4 families steal users’ banking information. The Malicious developers carefully design a phishing page similar to the official bank login or payment interface to confuse the victim, or redirect to a third-party website when the user performs a bank operation. There are four families are indeed ransomware that asks for Bitcoins to
make a profit. Once launched, it will encrypt the victim’s mobile phone files or force a lock screen and extort a high ransom. Furthermore, we have identified three aggressive adware families exploited by COVID-19 themed malware.

5.3 Anti-analysis Techniques

Previous work suggested that sophisticated malicious apps have exploited a number of anti-analysis techniques to evade detection. Thus, we further seek to analyze whether the COVID-19 themed malicious apps have such behaviors. Here, we take advantage of APKid [1], a widely used tool for identifying the packers, obfuscators, and other anti-analysis techniques used by covid-19 themed malware. We use APKid tool to scan all the 277 malware samples (with AV-rank ≥ 1), rough 52% (143 apps) of them use at least one anti-analysis technique, as shown in Figure 8. We classify the anti-analysis techniques used by COVID-19 themed malware into the following five categories.

**Obfuscator.** Obfuscation is the process of modifying an executable APK file, it modifies actual method instructions or metadata, it does not alter the output of the program. Obfuscator includes rename string, variables and method name, encrypted data, etc. It makes the decompiled source code more difficult to understand, and makes it more difficult for security personnel to analyze malicious apps. These are 34 COVID-19 themed malware use obfuscation techniques for evading detection, including unreadable method names, unreadable field names, and unreadable method names.

**Packer.** In order to strengthen the protection strength of Android, the malware pack Dex files to prevent them from being cracked by static decompilation tools and leaking the source code. For example, the malware\(^2\) (app name: corona virus) use ApkProtect [2] tool to packer the Apk file.

**Anti Disassembly.** The Apk file is actually a zip package. We can disassemble the Apk files, and decompile them to obtain the resource files and source code. Anti disassembly technique is to prevent the Apk file from being disassembled. Anti-disassembly uses specially crafted code or data in a program to cause disassembly analysis tools to produce an incorrect program listing. For example, the malware\(^2\) (app name: Corona Updates) adds code segments with illegal class names, which invalidates the decompilation tools.

**Anti Debug.** Malicious apps can avoid some dynamic debugging techniques by listening to port 23,946 (default port of android_server) and debugging related processes such as android_server, gdb, gdbserver, etc. In our dataset, there 19 malware samples use the Debug.isDebuggerConnected() method to check whether they are in debugging.

**Anti Virtual Machine.** The malware check whether they are running on real devices by analyzing the environment in which the APK runs, checking device information, device serial numbers, sandbox processes, feature directories and files of the simulator, etc. Once it is detected that it is not running on a real device, some malicious behavior will not be triggered to avoid dynamic detection. Roughly 33.2% COVID-19 themed malware detect the running environment, sandbox processes, and device hardware serial numbers to avoid analysis.

\(\text{RQ} \#3: \text{ Trojan and Spyware are the two main categories for COVID-19 themed malware. Their purposes are either stealing users’ private information, or making profit by cheating users using tricks like phishing pages, sending premium SMS/Phone calls, stealing bank accounts, and locking the phones. Anti-analysis techniques have been used by roughly 52% of these apps.}\)

\(^2\)MD5:3c0b5bc0e6f0b143e51be77fc0d028994  
\(^2\)MD5: e521b0e519c0f08217e3e90c894f094
6 MALICIOUS CAMPAIGNS

Our aforementioned study indicates the prevalence of COVID-19 related Android malware. We next seek to understand the malicious campaigns behind them.

6.1 The Developers of COVID-19 Malware

We extract the developers certificates from 277 malware and we obtain 68 different developer signatures in total. We found that some malware developers may use the known common keys in the community to sign apps. The most famous keys are the publicly known private keys included in the AOSP project. The standard Android build uses four known keys, all of which can be found at build/target/product/security. For example, TestKey is the generic default key for packages that do not otherwise specify a key. Other publicly-known keys include Platform (key), Shared (key) and Media (key). Thus we collect these keys and compare them with the signatures we extracted, and two of them were identified. For other developer signatures, we further search them on Google to confirm they are not public known signatures. At last, we have 66 private signatures left.

Habitual Malicious Developers. We hypothesis that, these malicious apps are created by habitual malicious developers, and they just take advantage of coronavirus pandemic to lure unsuspicous users. To verify our hypothesis, we seek to collect more apps released by these developers. Thus, we take advantage of Koodous to crawl all the apps released by these 66 malicious developers. Finally, we harvest 125,395 apps in total. We further check all the detection result of these apps from VirusTotal.

As shown in Figure 9, 27 habitual malicious developers release at least one app before the COVID-19 outbreak. Table 5 shows the top-10 habitual developers ranked by the number of released apps. Some of them are popular since 2014. However, from another point of view, roughly 60% of the COVID-19 malware developers are new emerging developers that only targeting this pandemic, i.e., they only release COVID-19 themed malware. This observation contradicts our hypothesis.

Figure 9: The Cumulative Number of Malicious Developers.

We further investigate whether these developers are focused only on creating malware, by calculating the the proportion of malware samples among all the apps they developed (defined as Malware Rate). Here, we have adopted two thresholds to flag a malware, $AV - rank = 1$ and $AV - rank = 10$. As shown in Figure 10, under the threshold of $AV - rank = 1$, over 77% of the developers have Malware Rate higher than 90%, and 37 out of 66 developers only release malware. Under the threshold of $AV - rank = 10$, over 32% of the developer have Malware Rate higher than 90%, and all the apps released by 14 developers are malicious. For all the 125,395 apps we collected, more than 91% of them are flagged by at least one engine and rough 72% of them are flagged at least 10 engines. This result suggests that most of the apps released by these developers are malicious.

6.2 Origins and Targets

Developer Countries. We further want to know the countries of these malicious developers, to investigate whether these malicious attacks are performed by developers in a specific regions. However, it is non-trivial to known their real location. We only can extract their country information from the corresponding signature information. Note that, this information might not be precise, as developers can intentionally modify this information and provide a fake one, or just leave it empty. However, it is the only way for us to approximately investigate their countries. Finally, we have successfully identify the countries of 59 developers.

Figure 11 shows the distribution of the countries of malicious developers. Most of them (34 developers) were claimed to be located in US, and the rest of them were claimed to be located in India, China, Turkey, Indonesia, Russia, Italy, etc.

Target Regions. We further want to know the target regions of these malicious apps, however, it is hard to know
### Table 5: The Top 10 Habitual Malicious Developers.

| Developers Certificate (SHA1) | Earliest Active Time | Country Code | # COVID-19 Malware | # Released Apps | # Malware AV-Rank >=1 | AV-Rank >=10 |
|-------------------------------|----------------------|--------------|--------------------|----------------|-----------------------|--------------|
| ece521e385e9bca33559e3afe1a64dd204583fa | 2014-10 | ID (Indonesia) | 2 | 71899 | 99% | 93% |
| 6d2aa36c507d0db156d8a077989aa8c6c7226540 | 2015-10 | IN (India) | 1 | 11562 | 94% | 62% |
| cu9f4145a36a8685d90a6d2ca2f580725c6e69c1 | 2014-03 | CN (China) | 1 | 11282 | 97% | 62% |
| 925ca49940d7788aa86d9f97f4d7adaccd1d4f0 | 2016-02 | None | 4 | 8984 | 29% | 6% |
| b0c633ae1171953132547433e3bb90482076d | 2015-12 | US | 1 | 6348 | 96% | 75% |
| dd2b1fabe67577ce55712d9881deba7c76d7854f | 2016-10 | US | 1 | 4666 | 95% | 15% |
| 0f399e6b74bd7e963645687a1a3fedc156971 | 2015-08 | AU (Australia) | 1 | 4557 | 43% | 3% |
| 9a9372947674c89d1fdeee4e497df73e7537528c | 2017-09 | IQ (Iraq) | 1 | 3289 | 100% | 99% |
| 524272445e993de601bb3ca3eb3bae43e4588e | 2018-07 | None | 10 | 993 | 100% | 99% |
| 05dce7bb0891d2793336b431dd0f50ab6d6c95e | 2019-09 | IT (Italy) | 1 | 940 | 100% | 95% |

![Figure 11: The Distribution of the Countries of Malicious Developers. Most of them were claimed to be located in US.](image)

Based on the distribution of malicious developers, we can see that most countries are located in the US. The distribution is based only on the Android binary. Here, we use an alternative approach. The Android APK file stores some resource files under the res/values directory, such as string.xml and arrays.xml. After the app is launched, these resource files will be read and displayed on the UI. In order to display different languages texts on UIs in different countries or regions, Android app developers add different suffix strings to the Values file names to distinguish languages they supported and dynamically load these resource files when the app runs. These string names follow the ISO 639-3 encoding rules. ISO 639-3 is an international language code standard, which contains 136 two-letter codes, used to mark the world’s major languages. These codes are used as a shorthand for language in many places, such as English is represented by en, German is represented by de, Chinese is represented by zh.

We extract the names of all the values files under the /res folder, and compare these languages to check which countries or regions the apps can display. Note that, developers not only use the region as a suffix, but also use the device screen resolution (such as values-hdpi, values-mdpi, etc), and Android version (such as values-v19, values-v21, etc) to display matching text information on different devices. Thus We filter out this kinds of files. Besides, this naming method also allows the area code to be added after the language to distinguish that multiple countries will use the same language, such as values-pt-rBR.

![Figure 12: Top 20 languages and their representative countries targeted by COVID-19 malware developers.](image)

Finally, we find that these 277 malicious apps contain 81 kinds of different language resource files, of which 219 apps contain at least 2 different languages. As shown in Figure 12, We list the top 20 languages and regions. This data may indicate the countries and regions targeted by these malicious apps. English countries is no doubt the primary target of the malware, roughly 94% of apps support English. Besides, languages such as Arabic, Spanish, Russian, Turkish and Chinese are widely supported by these malicious apps.
Coronavirus is used as a lure to attack unsuspicious users. Most of the apps released by these developers are malicious. Based on the information collected, these developers are mainly located in US, with rest of them are located in India, Turkey, etc. Besides English countries, Arabic countries, Europe, and China are also the main targets of them.

7 RELATED WORK
To the best of our knowledge, the coronavirus-themed mobile apps have not yet been systematically studied. Nevertheless, various studies have explored the security and privacy aspects of mobile apps, as well as the studies of coronavirus pandemic from other domains.

7.1 Security Analysis of Mobile Apps
A large mount of studies have analyzed mobile apps from security and privacy aspects, including malware detection, permission and privacy analysis, repackaging and fake app detection, privacy leakage identification, and identifying and analyzing third-party libraries, etc. Besides, some researchers in our community have analyzed specific types of mobile apps. For example, Hu et al. [31] analyzed the ecosystem of fraudulent dating apps, i.e., the sole purpose of these apps is to lure users into purchasing premium/VIP services to start conversations with other (likely fake female) accounts in the app. Ikram et al. [32] measured 283 Android VPN apps to understand security and privacy issues. Mobile health apps have been studied by previous work [40], [41] and [29].

A number of existing tools and techniques can be adopted/integrated to analyze the issues in coronavirus-themed mobile apps. Thus, we decide to release the dataset to the community to boost the research on COVID-19 themed apps.

7.2 Coronavirus-related Studies
Since its outbreak, Coronavirus has attracted great attentions from the research community. A large number of studies were focused on the medical domain. Many medical scientists have made outstanding contributions to the virus structure, pathological analysis, detection methods and treatment methods [26, 27, 42, 46] of COVID-19. Besides, a number of computer scientists have adopted machine learning techniques to identify and classify COVID-19 CT images. For example, Butt et al. [25] designed multiple convolutional neural network (CNN) models to classify CT samples with COVID-19. Wang et al. [45] used deep learning models to identify CT images of COVID-19 patients for fast judgment. In the field of social science, Kim [33] collected the comments made by the Korean people on social media to analyze the negative emotions and social problems during COVID-19 outbreak. Lin et al. [36] used Google keyword search frequency to predict the speed of the spread of the COVID-19 outbreak in 21 countries/regions. Schild et al. [38] collected comments from social media to analyze sinophobic behavior during the outbreak. Malavolta [22] developed an automatic web scraper to crawl app from Google Play and perform some basic analysis. However, only a few official apps were included and none of them is malware. Although a number reports have revealed the existence of COVID-19 themed Android malware, to the best of our knowledge, our study is the first to characterize them in a systematic way.

8 CONCLUSION
In this paper, we present the first measurement study of COVID-19 themed mobile malware. We first make effort to create and maintain a repository of COVID-19 themed apps, by collecting samples from a number of sources, including app markets, well-known app repository and the COVID-19 related domains. We then present comprehensive analysis of these apps from the perspectives of popularity and trends, distribution and installation, malicious behaviors, and the attackers and malicious campaigns behind them. Our research can help boost the research on coronavirus-themed cyber security threats.

REFERENCES
[1] Apkid. https://github.com/rednaga/APKiD, 2020.
[2] Apkp. https://apkp.baidu.com/, 2020.
[3] Apkk. https://apkk.baidu.com, 2020.
[4] Appchina. http://www.appchina.com, 2020.
[5] Covid-19: Cloud threat landscape. https://unit42.paloaltonetworks.com/covid-19-cloud-threat-landscape/, 2020.
[6] Covid-19 exploited by malicious cyber actors. https://www.us-cert.gov/ncas/alerts/aa20-099a, 2020.
[7] Covid-19 goes mobile: Coronavirus malicious applications discovered. https://research.checkpoint.com/2020/covid-19-goes-mobile-coronavirus-malicious-applications-discovered/, 2020.
[8] Covid-19-themed malware goes mobile. https://www.bankinfosecurity.com/covid-19-themed-malware-goes-mobile-a-13981, 2020.
[9] Developing story: Covid-19 used in malicious campaigns. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains, 2020.
[10] Findings on covid-19 and online security threats. https://www.technology.safety-security/threat-analysis-group/findings-covid-19-and-online-security-threats/, 2020.
[11] Fresh covid-19 phishing scams try to spread malware: Report. https://www.bankinfosecurity.com/fresh-covid-19-phishing-scams-try-to-spread-malware-report-a-14131, 2020.
[12] Google play. https://play.google.com, 2020.
[13] Huawei market. http://app.hicloud.com, 2020.
[14] Koodous. https://koodous.com/, 2020.
[15] Myapp market. https://android.myapp.com, 2020.
[16] New android coronavirus malware threat exposed. Here’s what you must not do. https://www.forbes.com/sites/zakdoffman/2020/04/09/why-android-users-must-now-dodge-this-simple-15-minute-coronavirus-malware-threat/#6b020abc4c1d, 2020.
[17] Pearson correlation coefficient. https://en.wikipedia.org/wiki/Pearson_correlation_coefficient, 2020.
[18] Uptodown. https://en.uptodown.com, 2020.
[19] Virustotal. https://www.virustotal.com/, 2020.
[20] Vietnamese threat actors apt32 targeting wuhan government and chinese ministry of emergency management in latest example of covid-19 related espionage. https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html, 2020.
[21] Virustotal. https://www.virustotal.com/, 2020.
[22] Web scraper and analyzer of covid-related android apps. https://github.com/iivanoo/covid-apps-observer, 2020.
[23] Who director-general’s remarks at the media briefing on 2019-ncov on 11 february 2020. https://www.who.int/dg/speeches/detail/who-director-general-s-remarks-at-the-media-briefing-on-2019-ncov-on-11-february-2020, 2020.
[24] Steven Arzt, Siegfried Rasthofer, Christian Fritz, Eric Bodden, Alexander Bartel, Jacques Klein, Yves Le Traon, Damien Octeau, and Patrick McDaniel. Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps. Acm Sigplan Notices, 49(6):259–269, 2014.
[25] Charmaine Butt, Jaggpal Gill, David Chun, and Benson A Babu. Deep learning system to screen coronavirus disease 2019 pneumonia. Applied Intelligence, page 1, 2020.
[26] Yu Chen and Lanjuan Li. Sars-cov-2: virus dynamics and host response. The Lancet Infectious Diseases, 20(5):515–516, 2020.
[27] Victor M Corman, Olfert Landt, Marco Kaiser, Richard Molenkamp, Adam Meijer, Daniel KW Chu, Tobias Bleicker, Sebastian Brünink, Julia Schneider, Marie Luisa Schmidt, et al. Detection of 2019 novel coronavirus (2019-ncov) by real-time rt-pcr. The Lancet Infectious Diseases, 20(5):515–516, 2020.
[28] Leonard Schild, Chen Ling, Jeremy Blackburn, Gianluca Stringhini, Yang Zhang, and Savvas Zannettou. “ go eat a bat, chang!”: An early look on the emergence of sinophobic behavior on web communities in the face of covid-19. arXiv preprint arXiv:2004.04946, 2020.
[29] Marcos Sebastián, Richard Rivera, Platon Kotzias, and Juan Caballero. Avclass: A tool for massive malware labeling. In International Symposium on Research in Attacks, Intrusions, and Defenses, pages 230–253. Springer, 2016.
[30] Ali Sunyaev, Tobias Dehling, Patrick I. Taylor, and Kenneth D Mandl. Availability and quality of mobile health app privacy policies. Journal of the American Medical Informatics Association, 22(6):e28–e33, 2015.
[31] Lex van Velsen, Desirée JMA Beaujean, and Julia EWC van Gemert-Pijnen. Why mobile health app overload drives us crazy, and how to restore the sanity. BMC medical informatics and decision making, 13(1):23, 2013.
[32] Dawei Wang, Bo Hu, Chang Hu, Fangfang Zhu, Xing Liu, Jing Zhang, Binbin Wang, Hui Xiang, Zhenshun Cheng, Yong Xiong, et al. Clinical characteristics of 138 hospitalized patients with 2019 novel coronavirus–infected pneumonia in wuhan, china. Jama, 323(11):1061–1069, 2020.
[33] Haoyu Wang, Hae Li, and Yao Guo. Understanding the evolution of mobile app ecosystems: A longitudinal measurement study of google play. In The World Wide Web Conference, pages 1988–1999, 2019.
[34] Haoyu Wang, Zhe Liao, Jingye Liang, Narseo Vallina-Rodriguez, Yao Guo, Li Li, Juan Tapiador, Jieun Cao, and Guoai Xu. Beyond google play: A large-scale comparative study of chinese android app markets. In Proceedings of the Internet Measurement Conference 2018, pages 293–307, 2018.
[35] Shuai Wang, Bo Kang, Jinlu Ma, Xianjun Zeng, Mingming Xiao, Jia Guo, Mengjiao Cai, Jingyi Yang, Yaodong Li, Xiangfei Meng, et al. A deep learning algorithm using ct images to screen for coronavirus–infected pneumonia (covid-19). MedRxiv, 2020.
[36] Daniel Wrapp, Nianshuang Wang, Kizzmekia S Corbett, Jory A Goldsmith, Ching-Lin Hsieh, Olubukola Abiona, Barney S Graham, and Jason S McLellan. Cryo-em structure of the 2019-ncov spike in the prefusion conformation. Science, 367(6483):1260–1263, 2020.
[37] Yu Zhou, Yajin Zhou, Xuxian Jiang, and Peng Ning. Detecting repackaged smartphone applications in third-party android marketplaces. In Proceedings of the second ACM conference on Data and Application Security and Privacy, pages 317–326, 2012.
[38] Yajin Zhou and Xuxian Jiang. Dissecting android malware: Characterization and evolution. In 2012 IEEE symposium on security and privacy, pages 95–109. IEEE, 2012.