IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received 28 March 2024, accepted 8 May 2024, date of publication 13 May 2024, date of current version 31 May 2024.

*Digital Object Identifier 10.1109/ACCESS.2024.3400211*

RESEARCH ARTICLE

# Maloid-DS: Labeled Dataset for Android Malware Forensics

**IMAN ALMOMANI[1,2], (Senior Member, IEEE), TALA ALMASHAT[2], AND WALID EL-SHAFAI[2,3], (Senior Member, IEEE)**

[1]Computer Science Department, King Abdullah II School of Information Technology, The University of Jordan, Amman 11942, Jordan
[2]Security Engineering Laboratory, Computer Science Department, Prince Sultan University, Riyadh 11586, Saudi Arabia
[3]Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

Corresponding authors: Iman Almomani (i.momani@ju.edu.jo; imomani@psu.edu.sa) and
Walid El-Shafai (eng.waled.elshafai@gmail.com)

**ABSTRACT** Billions of people globally use Android devices (https://backlinko.com/iphone-vs-android-statistics). As such, these devices are highly targeted by security attackers. One of the most threatening attacks is to infect devices with malicious software (malware). Fortunately, there are various ways to counteract these attacks and prevent them. One of these methods is developing a comprehensive malware dataset that researchers can utilize for malware analysis, detection, prediction, and prevention systems. This paper introduces a unique, up-to-date, labeled Android malware dataset (Maloid-DS) comprising a comprehensive set of malware families that reached 345 families with 47,971 malware samples. First, we intensely studied existing datasets utilized by previous research works. These datasets are limited in (a) the number of studied families, (b) the number of samples under each family, (c) the number of new malware samples, (d) the proper categorization of the malware families, (e) the accurate mapping of the sample with its corresponding malware family, (f) providing well structuring of the malware families and subfamilies, and (g) presenting a profound description of each family behavior. All these limitations were seriously tackled by introducing Maloid-DS. The process of creating Maloid is detailed in this paper. Moreover, several case studies are demonstrated in this paper to show the value of Maloid and how different types of analysis systems and AI-based detection and prediction solutions could utilize it. While the full potential of Maloid-DS in real-world scenarios is subject to ongoing research and practical application, it represents a substantial contribution to the cybersecurity community, offering a broad and detailed foundation for protecting Android devices against malware threats.

**INDEX TERMS** Android OS, malware forensics, labeled datasets, deep learning, malware analysis, detection and classification, cybersecurity applications.

## I. INTRODUCTION

The Android OS is the most popular operating system globally and dominates the global smartphone market with almost 71% of the market share.[1] Two of the main reasons for this popularity are the large number of diverse apps that can be found in the Android applications store and the customizability of the devices concerning both software and hardware. This is largely due to the open-source feature of Android OS, which allows the users as well as developers to customize the Android device to their liking. Specifically, users can root their devices to make custom changes that were previously blocked to them. Additionally, this open-source feature allows developers to easily develop different applications, which greatly increases the number of applications in the Google PlayStore. Users can even download apps from third-party app stores by downloading the Android Package Kit, or APK, of the desired application.

However, these Android characteristics can leave the user's device vulnerable to different attacks. Specifically, Android devices become a prime target of malicious

The associate editor coordinating the review of this manuscript and approving it for publication was Junho Hong.

[1] https://gs.statcounter.com/os-market-share/mobile/worldwide

software (malware), mainly due to the open-source nature of Android [1]. According to the Center for Internet Security malware report [2], Android malware has spiked in the first quarter of 2023 by 20% compared to the last quarter of 2022. Additionally, during the COVID-19 pandemic, as more and more people shifted to cyberspace to follow quarantine guidelines and work remotely, attackers took advantage and increased the frequency and sophistication of their malware attacks [3]. As a result, many users must take the necessary precautions to protect themselves from the increasing threat of malware attacks on their devices.

Fortunately, many experts are working towards ensuring users' safety from these malware attacks [4], [5], [6]. One of these important ways is to develop a dataset that contains samples of the new malware families. Android datasets can be used to help researchers train their developed AI (Artificial Intelligence) models. As a result, their models can be utilized in different tools that can detect existing malware families and predict the newly released ones [7]. Additionally, these datasets can help increase the accuracy of malware analysis tools and even detect unknown malware [8]. We will discuss these research works that developed malware datasets extensively in this paper.

However, there are limitations to these published datasets. One of the main limitations of the released datasets is that they provide samples as APK-based only. This can limit the applications of the dataset on different AI-based detection models and analysis tools. Additionally, many of the available datasets compose a limited number of samples, which can affect the diversity and accuracy of an AI model. Other published related papers also do not classify the collected families into different categories, and even the samples are not accurately mapped to these families. Another limitation of the current work is the restricted number of malware families the researchers collected. Moreover, most existing datasets don't provide profound descriptions of the malware families' behavior. Consequently, these limitations motivated us to introduce an up-to-date, labeled, well-structured, descriptive, and comprehensive dataset for Android Malware (Maloid-DS).

The main goals and contributions of this paper are summarized as follows:

1) Develop a substantial dataset with around 47,971 malware APK samples composed of more than 345 malware families. These malware samples ranged from well-known malware families in 2010 to recent ones found in 2024. This dataset accumulated malware samples from various sources, including official datasets and code repositories. We plan to release the constructed Maloid dataset through an official website.[2]
2) Provide a detailed and precise description of the collected malware families. From these descriptions, we created different categories based on the malicious behavior of the families. Specifically, we described each family's attack behavior and how the malware spreads. From these descriptions, we distributed the malware families into these categories.
3) Customize the dataset based on the user's needs. In other words, the interested party can use the malware samples as APK-based, image-based, or feature-based, where different types of malware analysis can be applied. This includes static, dynamic, vision-based, or even blended analysis. Consequently, this offers the users many options and flexibility in using the appropriate malware formats on their desired tools. The interested party can also choose which extracted features to use for the analysis process. As a result, this allows the users to customize the dataset as per their needs to increase the accuracy of their results. We have presented three case studies in this paper to stress this point.
4) Finally, Maloid offers a valuable educational source that could be heavily utilized in the academic context and continuous learning and training in the field of computer malware and analysis.

However, we faced some challenges during the creation of the Maloid dataset. Firstly, many of the official datasets where we collected the samples were either discontinued or prohibited from accessing their datasets. Additionally, the datasets we accessed and some of the papers we collected are considered outdated and published some years ago. Nonetheless, we were able to collect samples from more recent sources and collected other papers published more recently. Another challenge we faced was finding the correct description and category for the family since many anti-virus vendors name the same variants differently. This can affect the accuracy of our dataset [8]. However, we overcame this challenge by analyzing the collected samples of each categorized malware family using VirusTotal and getting the variant's name and the category it belonged to.

The rest of this paper is organized as follows: Section II provides a survey and comparison of related work. Section III describes how we collected the malware samples and produced the Maloid dataset in detail. In Section IV, we display the categories we created as well as describe the family in each category precisely. Section V provides recommendations on how best to utilize this dataset by presenting three different case studies. Section VI outlines the limitations and challenges associated with the development and compilation of the Maloid-DS dataset. Section VII details a comprehensive strategy suggested for the periodic updates to the Maloid-DS dataset. Finally, we summarize and conclude this paper in Section VIII, and offer some future research directions.

## II. RELATED WORK

This section highlights the different works that analyzed malware families from different datasets and those that

[2] https://sel.psu.edu.sa/research/datasets/datasets.php

created datasets by collecting different samples. Some papers used the samples collected for the datasets to train the tools proposed in their solutions [7], [9], [10]. Other papers did not collect malware samples but rather surveyed and analyzed other papers to provide a description for Android malware families [11], [12], [13]. However, most of the papers provide a description only for the family they used in their datasets as well as the source of the samples collected. Table 1 summarizes the comparison and analysis done on existing works that created datasets and described the malware families used in their datasets.

Many papers focused on creating datasets and then using them to train the tool proposed in their work. In [10], the authors collected many samples from different datasets, both from official and unofficial sources. This paper offered a diversity in the number of dataset sources. Furthermore, the authors provided a succinct and summarized description of the collected malware families. Similarly, [9] utilized their collected samples from different datasets to train their proposed tool and test its detection accuracy. Additionally, it provided a more diverse variety of malware families. Both papers analyzed a large number of samples as part of their dataset. However, there are limitations in both papers since they focused on the tool accuracy analysis. In [10], since their main goal was to train the proposed tool, the authors did not add the different families into categories, which can increase the dataset's accuracy.

On the other hand, one of the main focuses of [7] is to analyze their proposed system using their own created dataset. Therefore, the authors collected a substantial amount of Android APK samples, both malicious and benign. In addition to collecting multiple samples, the authors concisely described the behavior of the malware families collected. Moreover, the authors classified the malware families into different categories based on their attack behavior. However, although the authors described the families, they neglected to provide a comprehensive and detailed description of the utilized families. Additionally, the authors collected malware samples from a limited number of datasets and provided the malware and benign samples in the dataset as APK-based. The authors in [14] also collected malware APK samples to train their proposed detection system and test its accuracy. The authors classified the malware families into different categories to increase the system's ability to detect and identify the malware samples better. Additionally, they described the categories that detail the general behavior of the malware families. However, the paper does not provide a comprehensive description of each one of the malware families themselves. Additionally, the paper only used samples from a limited number of datasets. Consequently, the authors collected little malware samples for the training and testing experiments.

We also analyzed other papers that only studied articles that collected samples rather than creating the dataset themselves [11], [12], [13]. The authors of each paper do not introduce a new labeled dataset with collected samples. Specifically, they managed several papers and performed an in-depth analysis of them and the malware families specified in them. In [12], the authors analyzed 243 papers on malware families and their datasets. Moreover, the authors in [13] researched around 40 papers discussing malware families. However, they provided a detailed description of the malware families based on their behavior. In [11], the authors offer a precise, in-depth description of the behavior of malware families. However, as a result, they only described a limited number of malware families.

Similarly, in [12], the authors described the characteristics and behavior of the malware families thoroughly, including the malware's infection strategies and attack goals. Additionally, they offered the families into different categories through two different classifications. Specifically, the first classification was based on the characteristics and motivations of the malware families. The second classification was based on the behavior and methodology of the malware families.

Corresponding to the previous two works, the paper in [13] briefly described multiple malware families. The authors also discussed the limitations of the datasets collected by the articles that the authors analyzed. However, the main focus of these papers is exploring other articles that released malware family datasets and introduced malware analysis tools. As a result, these papers did not collect malware samples from official dataset sources and released newly labeled datasets. Additionally, in [11] and [13], the authors did not classify the families into different categories.

The remaining papers' main focus was developing and creating datasets with samples collected from various sources [15], [16], [17], [18], [19], [20], [21]. Regarding many of these papers, the authors focused on various factors such as the number of samples, different malware families, and the datasets they used. Many of these papers describe the malware families they collected. Specifically, the authors discussed the attack behavior of the malware families. However, in [16], the authors only describe malware families found in the adware category, which limits the diversity of the dataset. Although [21] described the malware families, the description provided is brief and only targeted a few numbers of the malware families. Similar to [16], this paper mainly focuses on malware families that affect the victims financially. Although the authors described the malware families in [15], the description is brief and focused on the technical details. The authors only provided specific details to a small number of malware families.

Furthermore, each paper developed its datasets by collecting malware samples from different datasets. This affected the number of samples collected by the authors for their datasets and the diversity of the malware families. For instance, since [21] focuses on financial malware, it collected a limited number of malware APK samples and a low number of diverse malware families. Equivalently, in [18], the authors collected samples from multiple datasets. However, the malware samples collected and their subsequent malware families were limited and low in diversity. The authors in [17]

**TABLE 1.** Summary and comparison among related works analysing Malware Families and Datasets.

| Related Work | Year | Samples Quantity | Datasets | Families | Advantages | Disadvantages |
|---|---|---|---|---|---|---|
| [15] | 2017 | 405 | AMD | 71 | - Provides detailed description on the malware samples including technical details | - Only focused on one dataset and its samples (AMD)<br>- Limited number of samples used<br>- Description provided is brief and limited |
| [16] | 2019 | 266 | - Drebian<br>- Others (Blog Posts) | 7 | - Provides a detailed description of the malware family described as Adware | - Limited number of samples<br>- Limited number of datasets<br>- Only collected and described malware families in the Adware category |
| [17] | 2020 | 15570 | - National Internet Emergency<br>- Drebin | 16 | - Provides a high number of samples<br>- Provides a detailed description of the families | - Limited number of datasets<br>- Limited number of families<br>- Does not categorize the families |
| [18] | 2013 | 1485 | - Dr. Web<br>- Kaspersky Mobile Security<br>- NQmobile<br>- Zoner Mobile Security | 58 | - Used samples from different multiple different datasets<br>- Provides a detailed description of the malware families | - Limited number of samples<br>- Does not categorize the family<br>- Limited number of families |
| [19] | 2012 | 1260 | Various Android Markets (Unspecified) | 49 | - Provides a detailed description of the families with screenshots<br>- Provides different classifications of the families | - Limited number of samples<br>- Did not use a specific or official dataset<br>- Low number of families |
| [11] | 2020 | — | — | 5 | - Gives in-depth description of malware families | - No Samples were analyzed and did not use any specific dataset |
| [9] | 2016 | 15,884 | Genome<br>Drebin<br>M0Droid<br>VirusTotal | 78 | - Provides a high number of samples<br>- Multiple different datasets<br>- Provides description of the families | - Does not classify the families into categories<br>- Only uses the sample to train proposed tool<br>- Limited number of families |
| [10] | 2019 | 17,016 | Drebin<br>AMD<br>GooglePlay | 232 | - Provides a high number of samples<br>- Multiple different datasets<br>- Provides a customized dataset | - Used the dataset to train their tool<br>- focuses on the accuracy of proposed tool<br>- No description of the families |
| [20] | 2017 | 40,000 | Google Play<br>SlideMe<br>GNOME | 10 | - Provides a high number of samples<br>- Multiple different datasets<br>- Provides detailed description of the family | - Does not categorize the families<br>- Limited number of families |
| [7] | 2020 | 400,000 | Canadian Center for Cyber Security<br>VirusTotal<br>AndroZoo | 191 | - Provides a high number of samples<br>- Creates own dataset<br>- Provides a brief description of the family<br>- Categorizes the family into different categories | - Focus of paper is on the malware analysis tool<br>- Only provides a breif description of the families.<br>- Samples provided are only APK-based<br>- Limited number of datasets |

**TABLE 1.** ***(Continued.)*** **Summary and comparison among related works analysing Malware Families and Datasets.**

| | | | | | | |
|---|---|---|---|---|---|---|
| [12] | 2021 | — | — | 41 | - Provides a detailed description of the families collected from the papers<br>- Discusses multiple characteristics of the malware families<br>- Categorizes the family into different categories based on multiple factors | - Does not collect malware samples, but analyzes papers that collected malware samples<br>- Does not provide a new dataset<br>- Describes and categorizes a limited number of families collected from the papers |
| [21] | 2018 | 1758 | - Android Genome Malware project<br>- Malware Security Blogs<br>- Anti-Malware Vendors<br>- Security Researchers | 32 | - Categorizes the families into the type of malware (Adware, Banking, etc.)<br>- Verified the categories of samples through VirusTotal<br>- Provides a brief description of the family | - Limited number of samples<br>- Low number of different families<br>- Description provided is brief and limited |
| [13] | 2020 | — | - Drebin<br>- Genome<br>- Collection<br>- Repository<br>- AMD<br>- UpDroid<br>- Contagio<br>- AndroZoo<br>- Marvin<br>- AndroMalShare | Multiple | - Provided an in-depth survey on the papers including malware anlysis methods and techniques, datasets, and the malware families<br>- Described the limitations of the papers and how they analyzed Android malware and its families | - Does not categorized the malware families<br>- Only surveys the papers and their limitations and not the malware families |
| [14] | 2016 | 2,784 | - Genome<br>- Contagio-Mobile<br>- VirusShare | 125 | - Classifies the malware families based on behavior | - Limited number of datasets<br>- Does not provide description of the family<br>- Only used samples to test detection tool |
| **Proposed Maloid** | **2024** | **47,971** | **Many Datasets (Drebian, AMD, VirusShare, etc.)** | **345** | **- Offers a diverse and large number of malware families and samples**<br>**- Classifies malware families into seven categories**<br>**- Collects Malware samples as recent as 2024**<br>**- Provides a detailed and precise description of the malware families**<br>**- Maps the malware sample to its family accurately**<br>**- Supports existing types of malware analysis** | **- Dedicated for Android operating system malware analysis** |

and [20] collected many malware samples to include in their datasets. Despite the large number of samples collected, the sources from which they collected them are considered limited. Consequently, the families the authors gathered are considered low. Finally, although the authors in [16], [19], and [15] provided a detailed and precise description of the families, the datasets they produced are limited. Specifically, the authors collected samples from a limited number of

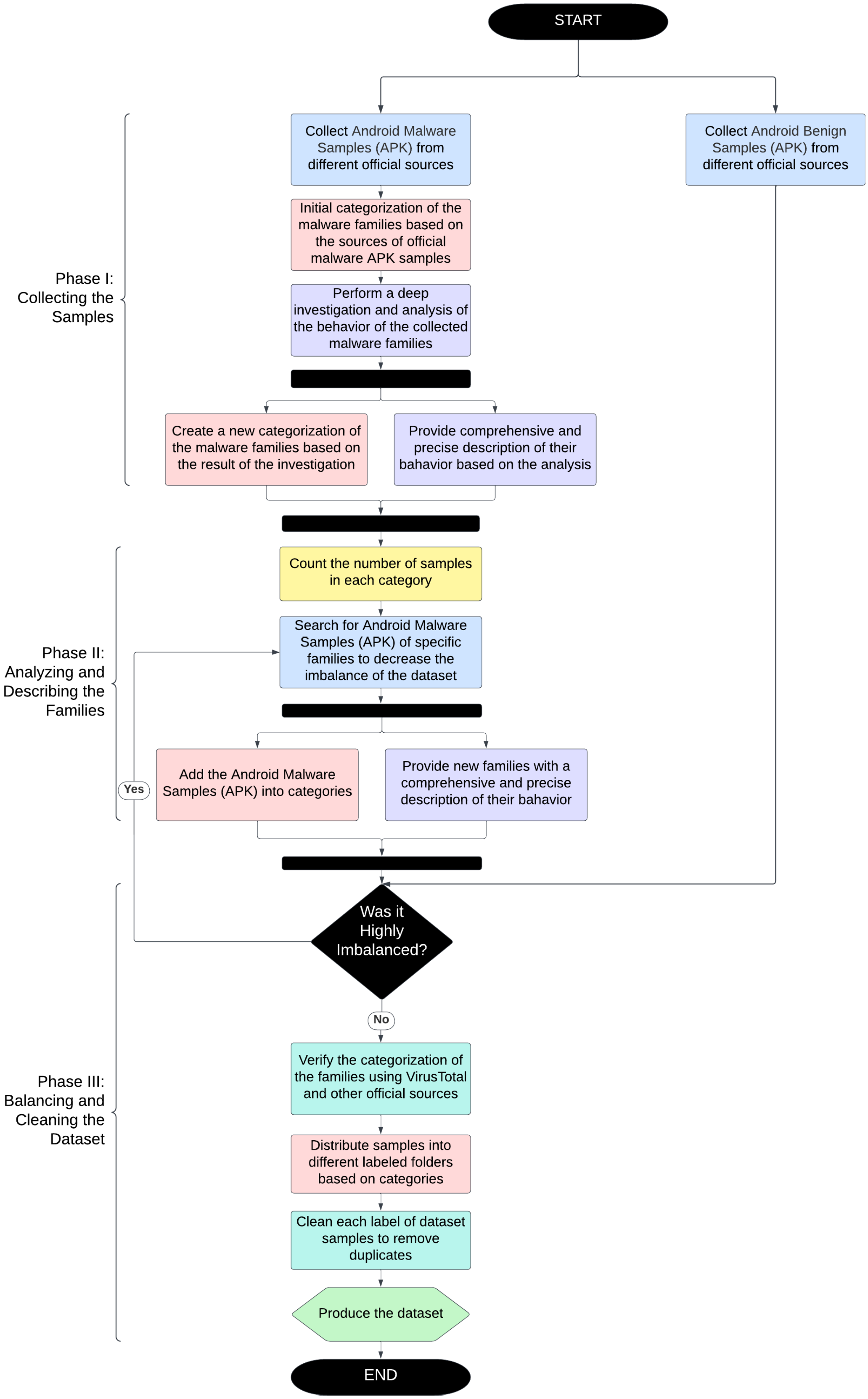

START
Collect Android Malware Samples (APK) from different official sources
Collect Android Benign Samples (APK) from different official sources
Phase I: Collecting the Samples
Initial categorization of the malware families based on the sources of official malware APK samples
Perform a deep investigation and analysis of the behavior of the collected malware families
Create a new categorization of the malware families based on the result of the investigation
Provide comprehensive and precise description of their bahavior based on the analysis
Phase II: Analyzing and Describing the Families
Count the number of samples in each category
Search for Android Malware Samples (APK) of specific families to decrease the imbalance of the dataset
Add the Android Malware Samples (APK) into categories
Provide new families with a comprehensive and precise description of their bahavior
Yes
Was it Highly Imbalanced?
No
Phase III: Balancing and Cleaning the Dataset
Verify the categorization of the families using VirusTotal and other official sources
Distribute samples into different labeled folders based on categories
Clean each label of dataset samples to remove duplicates
Produce the dataset
END

**FIGURE 1.** Flowchart on the creation process of the Maloid Dataset.

families and datasets, where [16], [19] do not specify the datasets they used. Moreover, the papers collected a small number of samples for their datasets.

Finally, we analyzed these articles based on the availability of malware family categorizations. Many papers, such as [15], [17], [18], and [20], only focused on collecting malware samples and describing the families. In other words, they did not distribute the families into different categories. On the other hand, the other articles provide a specific classification of the malware families collected. In [16], the paper focused on collecting malware families belonging to the Adware category. Additionally, in [19], the authors classify the malware families based on different characterizations, such as the installation method, activation method, and malicious behavior or payload. Similar to our work, the authors in [21] classify the malware families that they collected into categories based on the attack behavior of the malware families. Specifically, their categories are SMS-Malware, Ransomware, Scareware, Banking, and Adware.

About the previous works, we can see that most papers contain several limitations, namely, the quantity and diversity of the dataset sources, samples, and even families. Another constraint is that many of the papers' focus is on the accuracy of their analysis tool rather than the dataset itself. We also found that most papers did not classify the families into different categories. Finally, the malware samples and families collected from many papers would be considered outdated and from an earlier period. In this paper, the malware families are classified into the categories we recommended after a thorough investigation. Additionally, we provide a comprehensive and detailed description to all the families of the samples we collected. To collect more recent samples, we explored other malware sample sources. Finally, we managed and structured a substantial number of samples for each category to balance out the dataset.

In other words, this paper does not only provide a unique, massive repository of Android malware families and samples with a complete and accurate description, but it also offers an essential guide to researchers and developers on how Maloid can be heavily utilized in their malware analysis systems to ensure the production of malware detection systems with high accuracy that would protect Android users' data and devices.

## III. MALOID DATASET CREATION METHODOLOGY

This section describes the methodology we followed to build the Maloid dataset. Figure 1 summarizes the main processes implemented through this methodology, which is divided into three phases: the first phase is collecting the samples, the second phase is analyzing and describing the families, and finally, the third phase is balancing and cleaning the dataset. The phases are described in more detail below.

### A. PHASE I: SAMPLE COLLECTION

The first phase of the dataset creation is collecting malicious and benign APK samples from multiple sources. For the benign samples, we collected the APKs from multiple sources, which include StormDroid-Kuafudet, CIC MalDroid 2020 Dataset [22], the CIC MalDroid 2017 Dataset [23], VirusTotal APK files, GitHub repositories, and Google Play Store. On the other hand, we collected the malicious APK samples from multiple sources, including both official sources and unofficial sources. These sources include malware APK samples from DREBIN Dataset [24], Leopard Mobile Dataset, AMD dataset [25], CIC MalDroid 2020 Dataset [22], and the CIC MalDroid 2017 Dataset [23] which we considered as official sources. Finally, we also collected Ransomware APK samples and benign samples from a dataset developed by the Security Engineering Lab [26].

After collecting the samples, we created an initial categorization for the malware families of the samples that we have collected so far. Specifically, we initially developed different malware categories similar to the official sources' categories, including the CIC MalDroid 2017 Dataset [23]. After creating this initial categorization, we performed a deep and thorough investigation of the malware families. In this step, we focused on the malware families' attack behavior and the effect of the attack on the victim. Based on this investigation, we finalized the categorization of the families and approved them for our dataset. Concurrently, we added a detailed and precise description of the malware families that we collected. Both the categorization and description can be found in section IV.

### B. PHASE II: ANALYSIS AND DESCRIPTION

Once Phase I was completed, we moved on to Phase II. This phase focuses on further analyzing the malware families, enhancing their description, and increasing the number of samples and families. The first step we took was to count the number of samples found in each category. This helped us analyze the categories, understand which of the categories needed improvement, and increase the number of their samples. As a result of this analysis, we decided to begin searching for additional malware APK samples. As previously mentioned in Phase I in III-A, we collected samples from official sources. However, to improve the accuracy of our dataset, we collected various APK samples from unofficial sources such as code repositories and VirusShare. Hence, the initial balance of the dataset was improved.

Since we searched different sources for APK samples, we also added multiple new malware families to our dataset. Therefore, the next step we took was investigating the behavior of these new families. Based on these investigations, we added these malware families into their respective categories. Additionally, we added precise and comprehensive descriptions to these new families. As mentioned before, the description and categories of these families can be found in section IV. Finally, we reached Phase III of the dataset creation.

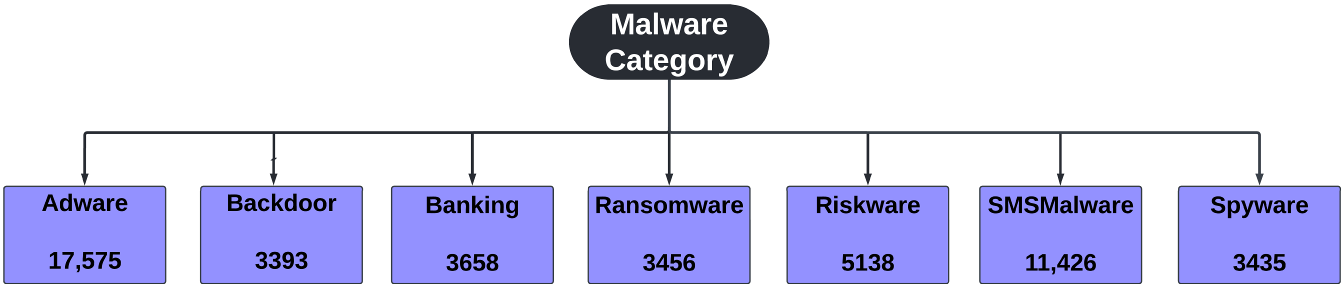


FIGURE 2. A high-level view of the 7 categories with the total number of families' samples in each.

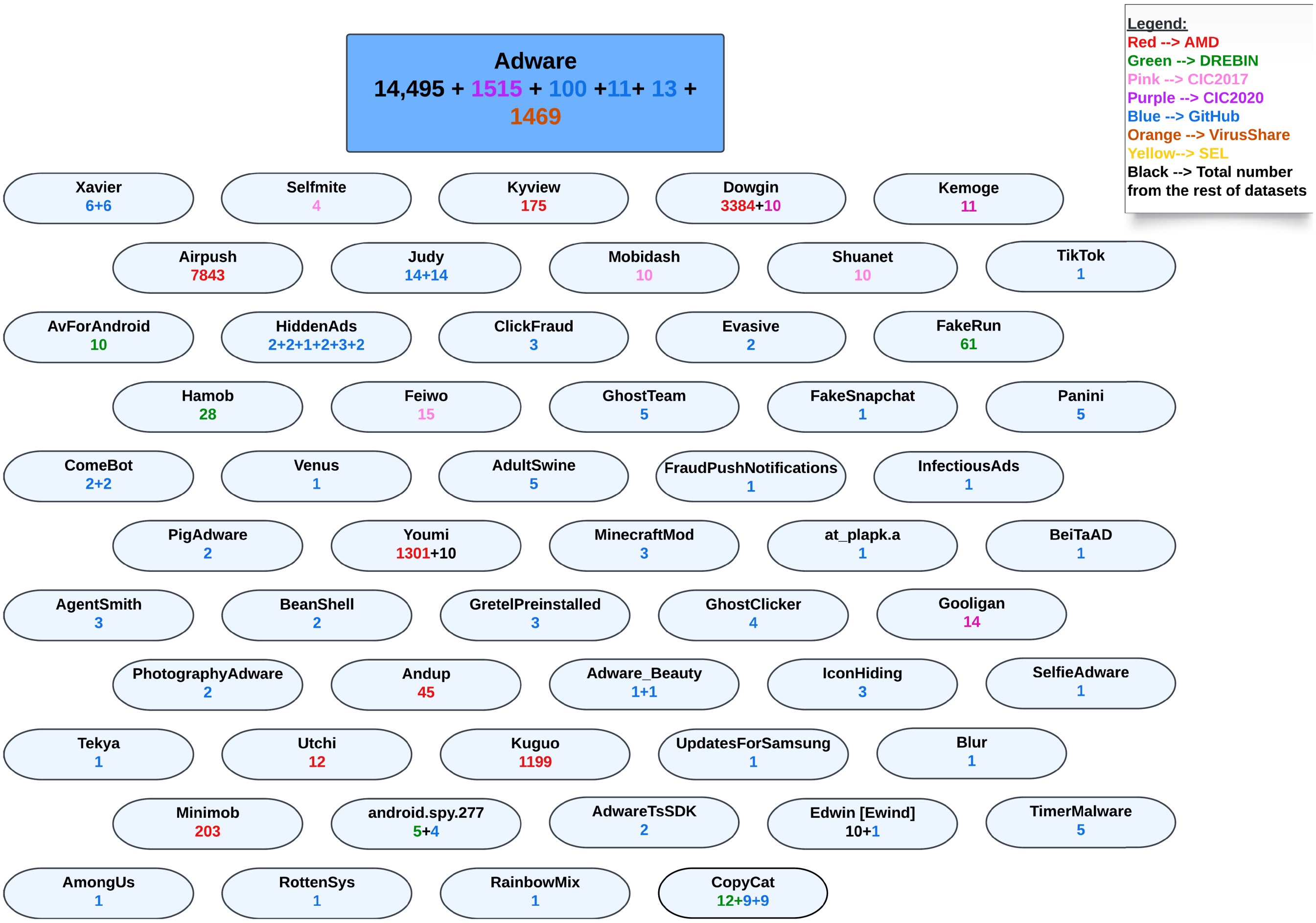


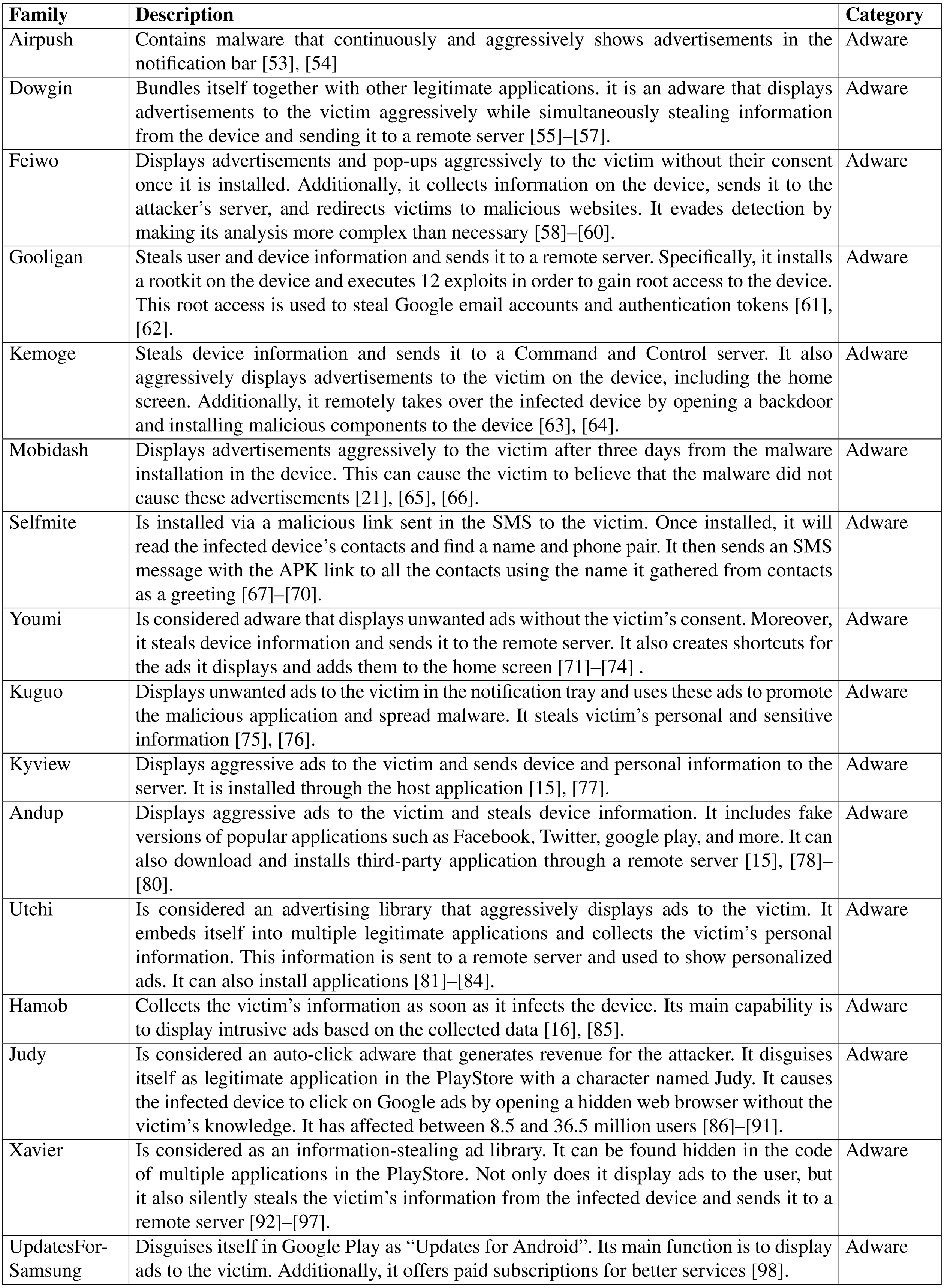
FIGURE 3. Adware Category with its families' names and their number of samples.

### C. PHASE III: DATASET BALANCING AND CLEANING

The third and final phase focused on balancing the dataset with the number of samples and cleaning the dataset from any duplicates of the APK samples. The first step in this phase is to check whether the dataset is highly imbalanced. If there is a high percentage of sample imbalance, we return to Phase II of the methodology. Specifically, we return to the second step of the phase, where we searched for different APK samples and families from different sources. On the other hand, if we find the dataset to be properly balanced, then we continue to the next step. In this next step, we verify the categorization of the families of the samples we collected. This ensures that the dataset can provide accurate and precise results when used to train AI models. We verified the families by uploading the APK samples to malware detection tools such as VirusTotal.

After verifying the categories of the families, we created multiple folders that were labeled with the seven malware categories. We then distributed the APK samples of the collected families to the corresponding folder. Then, we cleaned each folder of the dataset to remove any duplicate APK

**TABLE 2.** Adware Category and its families.



| Family | Description | Category |
|---|---|---|
| Airpush | Contains malware that continuously and aggressively shows advertisements in the notification bar [53], [54] | Adware |
| Dowgin | Bundles itself together with other legitimate applications. it is an adware that displays advertisements to the victim aggressively while simultaneously stealing information from the device and sending it to a remote server [55]–[57]. | Adware |
| Feiwo | Displays advertisements and pop-ups aggressively to the victim without their consent once it is installed. Additionally, it collects information on the device, sends it to the attacker's server, and redirects victims to malicious websites. It evades detection by making its analysis more complex than necessary [58]–[60]. | Adware |
| Gooligan | Steals user and device information and sends it to a remote server. Specifically, it installs a rootkit on the device and executes 12 exploits in order to gain root access to the device. This root access is used to steal Google email accounts and authentication tokens [61], [62]. | Adware |
| Kemoge | Steals device information and sends it to a Command and Control server. It also aggressively displays advertisements to the victim on the device, including the home screen. Additionally, it remotely takes over the infected device by opening a backdoor and installing malicious components to the device [63], [64]. | Adware |
| Mobidash | Displays advertisements aggressively to the victim after three days from the malware installation in the device. This can cause the victim to believe that the malware did not cause these advertisements [21], [65], [66]. | Adware |
| Selfmite | Is installed via a malicious link sent in the SMS to the victim. Once installed, it will read the infected device's contacts and find a name and phone pair. It then sends an SMS message with the APK link to all the contacts using the name it gathered from contacts as a greeting [67]–[70]. | Adware |
| Youmi | Is considered adware that displays unwanted ads without the victim's consent. Moreover, it steals device information and sends it to the remote server. It also creates shortcuts for the ads it displays and adds them to the home screen [71]–[74] . | Adware |
| Kuguo | Displays unwanted ads to the victim in the notification tray and uses these ads to promote the malicious application and spread malware. It steals victim's personal and sensitive information [75], [76]. | Adware |
| Kyview | Displays aggressive ads to the victim and sends device and personal information to the server. It is installed through the host application [15], [77]. | Adware |
| Andup | Displays aggressive ads to the victim and steals device information. It includes fake versions of popular applications such as Facebook, Twitter, google play, and more. It can also download and installs third-party application through a remote server [15], [78]–[80]. | Adware |
| Utchi | Is considered an advertising library that aggressively displays ads to the victim. It embeds itself into multiple legitimate applications and collects the victim's personal information. This information is sent to a remote server and used to show personalized ads. It can also install applications [81]–[84]. | Adware |
| Hamob | Collects the victim's information as soon as it infects the device. Its main capability is to display intrusive ads based on the collected data [16], [85]. | Adware |
| Judy | Is considered an auto-click adware that generates revenue for the attacker. It disguises itself as legitimate application in the PlayStore with a character named Judy. It causes the infected device to click on Google ads by opening a hidden web browser without the victim's knowledge. It has affected between 8.5 and 36.5 million users [86]–[91]. | Adware |
| Xavier | Is considered as an information-stealing ad library. It can be found hidden in the code of multiple applications in the PlayStore. Not only does it display ads to the user, but it also silently steals the victim's information from the infected device and sends it to a remote server [92]–[97]. | Adware |
| UpdatesFor-Samsung | Disguises itself in Google Play as "Updates for Android". Its main function is to display ads to the victim. Additionally, it offers paid subscriptions for better services [98]. | Adware |

**TABLE 2.** *(Continued.)* **Adware Category and its families.**

| | | |
|---|---|---|
| FakeSnapchat | Disguises itself as the legitimate social media application Snapchat. Once the victim installs and launches the application, it displays ads to them. When the victim tries to log in, it displays a connection error message. Additionally, the malware makes sure that the victim is connected to the Internet to display the ads [99]–[102]. | Adware |
| adware_beauty | Hides behind multiple beauty camera applications found in the Google Play store. These applications can display ads to the victim, redirect victims to phishing websites, and steal the infected device's information and send it to the attacker [103]–[105]. | Adware |
| tv_remote/ HiddenAds | Disguises itself as multiple simulator applications in the Google Play store. It displays intrusive ads aggressively to the victim. It avoids detection by hiding the application in the system folders. One of its most downloaded applications, "Easy Universal TV Remote", forces the victims to give five-star reviews to increase exposure and installations. Another of its application is a popular QR code scanner [106]–[111]. | Adware |
| Adultswine | Disguises itself as legitimate gaming applications that are aimed for children. Once installed, it begins to aggressively display inappropriate and adult-themed ads to the victim. In addition to displaying ad, it tries to trick the user into downloading and installing malware disguised as security applications. [112]–[115]. | Adware |
| ClickFraud | Mainly targets users in the US, Brazil, and Mexico. It is spread by disguising itself as legitimate applications in the Google Play store as well as injecting itself into the code of benign software. In addition to displaying ads to the user when installed, it also has the capability of crypto mining using the infected device, which can slow down the device's performance [116], [117]. | Adware |
| GhostTeam | Disguises itself as application found in the Google Play store. It ensures that it is installed on a physical device, not an emulator. It floods the infected device with unwanted pop-up ads. It can also take control of the infected device by installing a malicious payload and stealing the login credentials of the victim's FaceBook account [118]–[121]. | Adware |
| Panini | Hides behind multiple different names and icons that are generic. Once the malware is executed, it displays multiple ads on the infected device [122]. | Adware |
| RottenSys | Disguises itself as a WiFi management tool. It aggressively displays ads, both pop-up and full screen, to the victim in order to gain money. It also appears to be preinstalled on Android devices without any interference from the victim beforehand. The victims believe it is a pre-installed Wi-Fi service app [123]–[125]. | Adware |
| TimerMalware | Disguises itself as a legitimate application on the Google Play store. Each time it is reported and removed, it returns to the store with a different package name. It has a timer of four hours after installation to activate. After activation, it requests admin permission to be able to uninstall itself later and aggressively displays ads to the user to gain money [126]. | Adware |
| Adware TsSDK | Disguises itself as entertainment applications found in the Google Play store. It uses third-party Android libraries to persistently display full-screen ads on the device and tries to convince the victim to install additional applications. These libraries drain the device's batteries and slow down its performance [127]. | Adware |
| BeiTaAd | Injects itself into legitimate applications as an ad plugin. It aggressively and persistently displays ads on the infected device that hinders the victim's interaction with it. It displays full-screen ads on the lock screen, plays audio and video advertisements in sleep mode and active mode, and displays ads when the user is not using the application [128]. | Adware |
| ComeBot | Displays unwanted ads on the device. Another behavior of this malware is its ability to remain on the device by hiding its icons [129]. | Adware |
| Evasive | Disguises itself as gaming applications found in the Google Play store. It displays aggressive full-screen ads to the victim and uses evasive techniques to avoid detection and removal [130]. | Adware |
| FraudPush-Notifications | Disguises itself as applications found in the Google Play store. It uses Google Chrome to load compromised websites on the device. These websites subscribe the victim to notifications services which display persistent pop-up ads on the infected device [131]. | Adware |
| Gretel-Preinstalled | Is found already installed on specific Android devices, Gretel, in the system apps folder. It displays unwanted ads to the victim as well as downloading and installing other applications on the device [132]–[134]. | Adware |

**TABLE 2.** *(Continued.)* Adware Category and its families.

| | | |
|---|---|---|
| InfectiousAds | Takes advantage of the Android OS's vulnerabilities to perform various malicious activities. These activities include injecting malicious software on the infected device and displaying intrusive ads to the victim. It spreads by injecting itself into legitimate applications that appear harmless [135]. | Adware |
| Photography-Adware | Disguises itself as a variety of photography applications found on Google Play. It executes its malicious activities 30 minutes after the installation of the malware. This allows the malware to evade detection more easily. These activities mainly include displaying full-screen ads which interfere with the victim's activities [136]. | Adware |
| Venus | Disguises itself as a legitimate application in Google Play. When the user executes the application, it will subscribe the victim to ads and premium subscription services without them knowing [137], [138]. | Adware |
| AgentSmith | Disguises itself as a legitimate Android application. It can exploit Android vulnerabilities in order to replace benign applications on the device with malicious versions. Its main functionality is to show advertisements to the user, which uses the device's resources for financial gain [139]. | Adware |
| IconHiding | Disguises itself as a legitimate application in Google Play. It aggressively displays ads to the victim that interfere with them. It evades detection and removal by hiding its icon from the victim [140], [141]. | Adware |
| selfieAdware | Masquerades as applications that filter selfie photos. Its main activity is to aggressively display full-screen ads to the victim. It can also secretly record audio from the infected device [142], [143]. | Adware |
| Tekya | Disguises itself as a legitimate application in Google Play. Itperforms ad fraud by mimicking and stimulating the victim's clicks on ads from ad agencies for financial gain [144]–[146]. | Adware |
| AmongUs | Can be found disguised as a fake version of the mobile game, Among Us, in third-party stores. It turns the game into Adware that aggressively displays full-screen ads to the victim and can slow the device down [147]–[149]. | Adware |
| PigAdware | Displays aggressive ads to the victim that intrudes on the device's usability. A characteristic of this malware is that they inject itself into the System App directory. This makes the adware harder to remove without causing device failure [150], [151] | Adware |
| Blur | Disguises itself as photo applications in the Play store. The main function of this malware is aggressively displaying multiple ads to the victim. Additionally, to make it harder to uninstall, it hides its icon from the home screen of the device [152], [153]. | Adware |
| BeanShell (AKA Circle) | Disguises itself as various legitimate applications found on Google Play. It is a bot that receives commands from the server using BeanShell library scripts. Its main function is to display ads to the victim and simulate clicks on websites that the malware loads [154], [155]. | Adware |
| minecraftMod | Disguises itself as applications that provide mods to the popular game Minecraft. However, it only displays aggressive and intrusive ads to the victim without providing the promised service. It hides its icon and continues to display ads to the victim on the home screen [156]–[158]. | Adware |
| RainbowMix | Disguises itself as a retro gaming emulator in the Play Store, with around 240 applications. Its main job is to generate a profit for the attacker by displaying intrusive and aggressive out-of-context ads to the victim, which intrudes on their user experience [159]–[162]. | Adware |
| TikTok | Disguises itself as the video-sharing application TikTok. It mainly targets Jio users in India by luring them with a free Lenovo laptop or the application itself, which is banned in India. It prompts the victim to share the APK with their contacts. Additionally, it generates revenue by displaying ads to the victim [163], [164]. | Adware |
| FakeRun | Aggressively shows ads to the user in order to get a profit for the attacker. It also forces users to give the application a five-star rating on the Android Market and share the app's information on their Facebook accounts before the execution [165]–[167]. | Adware |

**TABLE 2.** *(Continued.)* **Adware Category and its families.**

| | | |
|---|---|---|
| Edwin [Ewind] | Is added to legitimate applications by recompiling these applications with the malware as part of its source code. It displays ads to the victim for the attacker's financial gain. It collects device information and forwards SMS messages to the attacker. It can also give the attacker full remote access to the infected device [168]–[171]. | Adware |
| Minimob | Is a repackaged version of a live wallpaper application, BlueArt. It spams the user with intrusive advertisements. It can be executed without hurting the device and steals the victim's personal information (GPS Location, Phone Number, google api) and device information to a remote server [42], [172], [173]. | Adware |
| Shuanet | Will attempt to root the device to bypass factory reset if discovered once installed. This malware displays ads to the victim aggressively [174], [175]. | Adware |
| android.spy.277 | Masquerades as a benign and legitimate application. However, it steals the victim's information from the device and sends it to a CC (command&control) remote server. It then uses the stolen information to show specialized ads to the victim [16], [176]. | Adware |
| AvForAndroid | Masquerades as antivirus software. Its main functions include: monitoring book readers' and pdf readers' activities, installing shortcuts on the device, stealing bookmark lists and user accounts, changing network status, and recording audio [177]–[179]. | Adware |
| GhostClicker | Is most prevalent in Southeast Asia. It is described as an auto-clicking adware that simulates a user's clicks on the ads in order to gain a profit for the attacker without the victim's knowledge. It finds advertisements by embedding itself in the Google-owned Admob. It evades detection in various ways, including stopping the auto-clicking routine [16], [180]–[182]. | Adware |
| CopyCat | Generates revenue and gains a profit by displaying pop-up ads to the victim. Additionally, it gains root privileges in order to control the infected device and install ads on the device [183]–[186]. | Adware |

files. This step further advances the accuracy and ensures the balance of the dataset. Finally, after cleaning the folders, we produced the Maloid dataset detailed in this paper. In the following section, we discuss each category that resulted from the dataset creation and provide an in-depth description of the malware families.

## IV. MALOID DATASET STRUCTURE AND DESCRIPTION

This section presents the distribution of malware families into seven different categories. These categories include Adware, Backdoor, Banking, Ransomware, Riskware, SMSMalware, and Spyware. Figure 2 lists the categorizations and the number of samples collected under families classified under this category. For example, the category with the largest number of families' samples is Adware, with 17,545. In contrast, the Backdoor category has the lowest number, with 3393 families' samples. The samples were collected from different sources, as detailed in the subsections below.

We also describe in detail the functions and main behavior of each family. Our Maloid Dataset collected samples from various resources, including AMD, DREBIN, AMD, CICAndMal-2017, CICAndMal-2020, SEL lab, VirusShare, GitHub, and others. Maloid dataset refers to the source from where each sample was collected. In the following subsections, for each category, the families classified under it will be listed with their precise descriptions. Also, the number and source of samples under this family will be shown.

### A. ADWARE

This section highlights the families that were classified as Adware. Adware is a type of malware that disruptively and aggressively displays ads to the victim. It also performs ad fraud on the advertising network for the attacker's financial gain [16]. This type of malware spreads using pop-up ads and, in some cases, with botnets. However, there are ways to mitigate and prevent the families in this category. For example, users can check their devices for unknown applications, stop them from running, clear their caches and data, and finally uninstall them. Other strategies they can use include clearing the cookies and caches from their browsers, installing ad blockers, and carefully clicking on website ads [16], [27].

Figure 3 below displays the families categorized as Adware and the corresponding number of APK samples found. The color coding illustrates the source from where the sample is collected. So, under the Adware category, 1515 samples were collected from CICAndMal-2020, 100&11&13 from Github,1469 from AMD, and 14,495 from the rest of the datasets. Within the same malware family, the source is also identified. For example, for the "Dowgin" family, 3384 samples were collected from the AMD dataset and 10 samples from the DREBIN dataset. For the "Xavier" family, GitHub is the source, but from two different repositories. Additionally, Table 2 displays each adware family and its description.

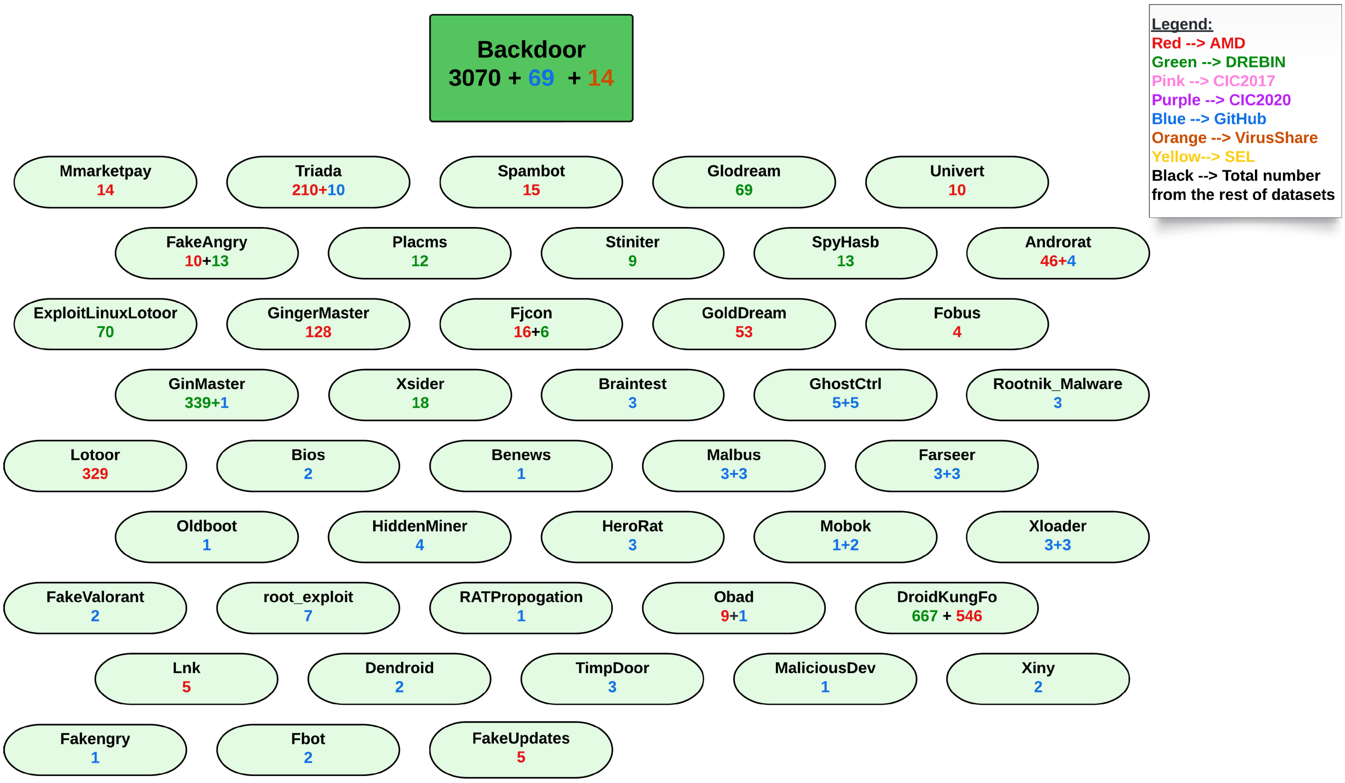


**FIGURE 4.** Backdoor Category with its families' names and their number of samples.

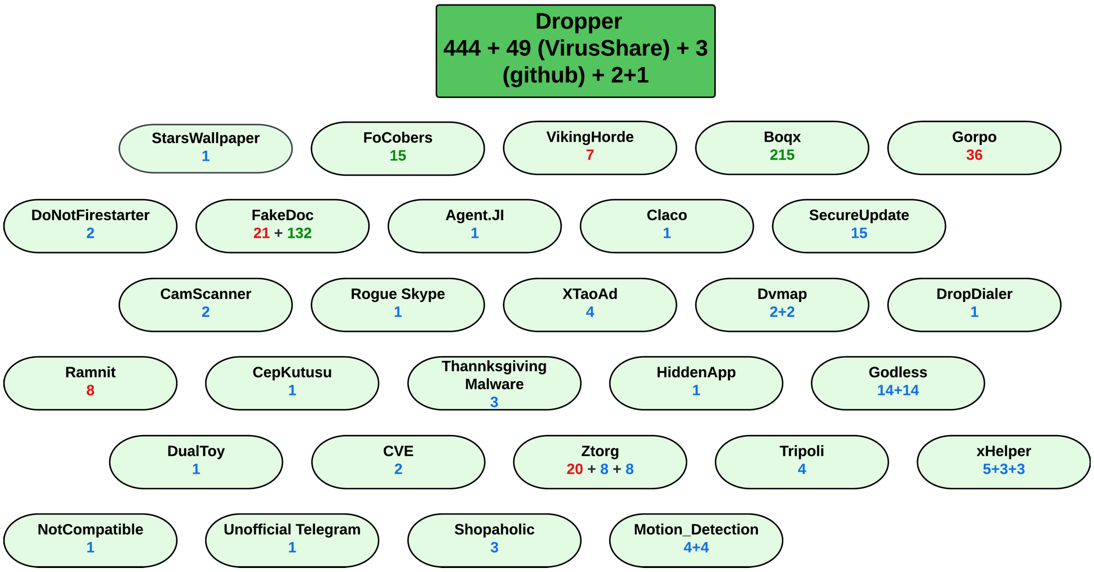


**FIGURE 5.** A sub-group of the Backdoor known as Dropper with families' names and number of samples.

## B. BACKDOOR

This section highlights the families that were classified as Backdoor, as shown in Figure 4. The Backdoor is a type of malware that allows the attacker a different, unauthorized entry point to access the device [28]. They spread through various means, which include SMS messages, calls, Android games and applications, URL links, plug-ins, and botnets [28]. We also added a subcategory to the Backdoor malware known as Trojan Droppers, or simply Droppers. Like the Backdoor, Droppers are malware the attackers use to inject other malicious programs [29]. Since they display similar behaviors, the Dropper malware has

**TABLE 3.** Backdoor Category and its families.

| Family | Description | Category |
|---|---|---|
| Glodream | Steals device information, incoming SMS messages, and call details. Then, it sends the captured information to a remote server. It also receives instructions from the server to perform multiple actions, such as sending SMS through the infected device and installing malicious applications [187], [188]. | Backdoor |
| Triada | Disguises itself as a Chinese application, Wandoujia. It steals the victim's information stealthily and sends them to a remote server. It can hide plugins that perform malicious activities. It can gain root access. It can modify the Zygote process to control the launch and usage of all applications on the device. It avoids detection by residing in the device's RAM [15], [189]–[194]. | Backdoor |
| Fjcon | Repackages itself in legitimate applications. It hides its domains and URLs using AES encryption. It affects devices with customized ROM. Its main function is to stealthily install and/or remove the software from the device. It also monitors SMS messages and blocks some messages from their inbox [195], [196]. | Backdoor |
| Spambot | Infects devices via different applications that the victims download. It uses the infected device as a bot to send spam SMS messages and adds it to a bot network controlled by a remote server. It also pays users to download an infected application [197], [198]. | Backdoor |
| FakeAngry | Silently collects the victim's personal information and sends it to a remote server by embedding it in URL links, HTTP Requests, and text messages. It spreads by recompiling with legitimate applications [199], [200]. | Backdoor |
| Univert | Collects device information, the victim's contacts, and SMS messages and sends them to a remote server. It also sends SMS to premium rate numbers [15], [201]. | Backdoor |
| Obad | Is distributed alongside Opfake. The infected device sends messages to all its contacts in the background with a malicious link that installs Obad. It also spreads via a fake Google Play store and third-party markets. It gains admin privileges by stealthily exploiting Android vulnerabilities. It performs malicious activities from a remote server's commands [202]–[206]. | Backdoor |
| DoNot-Firestarter | Spreads using Google's Firebase Cloud Messaging in addition to a CC server. The attacker can use Firebase to direct it even if the server is taken down. It can collect device information and send it to the server. Based on the collected data, it is capable of delivering a malicious payload to infected devices [207]–[209]. | Backdoor (Dropper) |
| Godless | Takes advantage of the PingPongRoot exploit (CVE-2015-3636) and the Towelroot exploits (CVE-2014-3153). It disguises itself as a legitimate application on the PlayStore, where it roots the infected device. It downloads malicious applications that can be used for different attacks. It affected around 90% of Android devices in Indonesia, India, and Thailand [210]–[213]. | Backdoor (exploit) |
| Rouge _skype | Is a rogue plug-in that disguises itself as Skype in the background when the plugin is loaded and run. Additionally, it requests superuser permissions from the victim when it is run. Its main function is to change the infected device's startup script. This allows the malware to install applications on the infected device's system directory [214], [215]. | Backdoor |
| motion _detection | Disguises itself as two applications found in the Google Play store: Currency Converter and BatterySaverMobi. Once installed, it uses the infected device's motion sensors to avoid detection in sandboxing environments since there are no motion sensors. If the device moves, it runs the malicious code and attempts to download Anubis with a fake system update [216]–[219]. | Backdoor (Dropper) |
| Fobus (AKA Podec) | Pretends to be an ad blocker but collects personal information and browser history. It sends SMS to premium rate numbers and receives them. It also makes calls and collects phone history. It tries to gain admin privileges and will lock the screen if revoked. If the victim persists, it will warn them to reset the device to factory settings [15], [7]–[222] | Backdoor |
| Stiniter | Can gain root privileges of the device and install other malware on the infected device [223], [224]. | Backdoor |
| Placms | Is capable of gaining root privileges of the infected devices. This allows the malware to perform various malicious activities on the device, including installing and deleting files and performing DoS attacks [186]. | Backdoor |

**TABLE 3.** ***(Continued.)*** **Backdoor Category and its families.**

| | | |
|---|---|---|
| SpyHasb | Is a monitoring tool that spies on the victim's phone calls, SMS messages, and GPS Location [14], [82], [225]. | Backdoor |
| Fakengry | Gains root access to the infected device. This allows the attacker to collect information on the device and download other software [226]. | Backdoor |
| Xsider | Gains root privileges to the infected device. This allows it to create a backdoor for the attacker and steal information stored in the device. It then sends the information to the server via a specified URL [186], [227]. | Backdoor |
| Ghostctrl | Is an evolved form of the OmniRAT tool that spreads by disguising itself as legitimate applications (WhatsApp, Pokemon GO). It controls many of the functions of the infected device stealthily. It persistently asks the user to install a malicious app. Once installed, it connects to a C&C server. It receives instructions to perform various malicious actions and has ransomware capabilities. It targeted Israeli healthcare organizations [228]–[230]. | Backdoor |
| Dendroid | Is an HTTP remote access trojan (RAT) that has a PHP panel. It automates the creation of Android Trojans and makes them easier to make. [231]–[234]. | Backdoor |
| Benews | Disguises itself as a news application. It uses the name of a fake news website to make it seem more legitimate. It is capable of bypassing the security mechanisms set in place in Google Play. Its main function is to dynamically load and install additional malware on the infected device once the victim opens the infected application [235]–[237]. | Backdoor |
| Braintest (Ghostpush) | Disguises itself as an application that can calculate the user's IQ. It is able to bypass the security of the Play store. Once installed and launched, it takes advantage of four known root exploits to gain the root privilege of the device. This allows it to install other malware and malicious components. [238]–[242] | Backdoor |
| Farseer | Uses DLL side loading in order to inject malicious payload and code into devices. It targets Windows users. It shares ties and characteristics with the Android malware HenBox [243]–[246]. | Backdoor |
| Malbus | Disguises itself as a plugin used for a series of applications in the Google Play store that provide useful information on public transportation in South Korea. It steals the Google account credentials of the victim by displaying a fake login page from Google. It mainly targets government officials, but other Android users can fall victim to it [247]–[249]. | Backdoor |
| rootnik _malware | Exploits a Chinese commercial rooting tool called "Root Assistance" and an MTK root scheme. It reverses engineers to steal five exploits to root the infected device. It masquerades as a file manager and embeds its code on legitimate applications. It infected Android users globally, including in the United States, Malaysia, Thailand, Lebanon, and Taiwan [250]–[252]. | Backdoor |
| HeroRat | Spreads as legitimate applications found in third-party markets and messaging applications. When the user opens the application, a message explaining that the applications will be uninstalled is displayed. However, the malware is still in the infected device. It abuses the Telegram-bot functionality to take control and perform various malicious activities [253]–[256]. | Backdoor |
| HiddenMiner | Abuses the performance and capability of the infected device to mine the cryptocurrency, Monero, from the infected device until its resources are exhausted. It avoids detection by hiding itself from the victim. It spreads by disguising itself as an update for the Google Play application found in third-party markets [257]–[260]. | Backdoor |
| MaliciousDev | Disguises itself as driving gaming applications in the Google Play store. Every time the victim tries to open the application, the game crashes. In reality, It is installing and downloading malware in the background without the victim's knowledge [261], [262]. | Backdoor |
| TimpDoor | Disguises itself as a voice messaging application that spreads via malicious links sent by SMS. Once the victim installs it, it turns the infected device into a hidden Socks proxy that redirects traffic to a third-party server. This allows the attacker to use the mobile device as a backdoor into corporate or home networks [263]–[266]. | Backdoor |
| Xloader | Disguises itself as a security application on Android devices. It uses DNS spoofing in order to infect devices with malicious payloads. It can also steal information stored in the infected device [267]–[269]. | Backdoor |

**TABLE 3.** *(Continued.)* Backdoor Category and its families.

| | | |
|---|---|---|
| FakeValorant | Disguises itself as a fake version of the anticipated game, Valorant. When visiting the compromised website, it prompts the victim to install the malware. Once the application launches, it pushes the victim to install other risky applications. The victim is tricked into installing these apps to play the game, but they will not be able to play the game [270]–[274]. | Backdoor |
| Xiny | Injects its malicious code into gaming applications. It can gain root access on the infected device, which allows it to steal sensitive information and delete and install applications on the device. It is also able to display ads to the victim [275]–[277]. | Backdoor |
| Mobok | Disguises itself as a photo editing tool on the Play store. Its main capability is stealing the victim's sensitive information and using the collected data to subscribe them to a premium service. It acts as a backdoor for the attacker to fully control the infected device [278], [279]. | Backdoor |
| RAT-Propagation | Describes RAT malware's propagation techniques. These include spreading the malware via emails claiming to request a resume submission or other phishing tactics. Another propagation technique is the malware disguising itself as legitimate applications [253], [280]. | Backdoor |
| Mmarketpay | Disguises itself as a weather application and affected more than 100,000 Chinese devices. It downloads paid content without the victim's knowledge from the Chinese online market, Mobile Market, by simulating clicks. It intercepts the SMS with the verification code and enters it on the Mobile Market website, which also causes high phone bills [281]–[285]. | Backdoor |
| Lnk | Exploits the CVE vulnerability (CVE-2010-2568). LNK is an extension for shortcuts. The malware hides itself in LNK files and sends them to victims. It points to a specific URL or code to be executed and downloads other malware. It also attempts to gain privilege over the device [15], [286]–[288]. | Backdoor |
| GoldDream | Targets Chinese-speaking users. Popular game apps are repackaged with it, which silently monitors the device's SMS messages and phone calls. It sends information to a remote server and executes malicious commands from the server. It can dynamically send premium rate numbers via the server for profit [17]–[291]. | Backdoor |
| AndroRAT | Is a remote access Trojan embedded in a carrier application. It allows an attacker to control an infected device remotely and steals device information and user information. It was first developed as a proof of concept [292]–[295]. | Backdoor |
| ExploitLinux-Lotoor | Exploits a specific vulnerability in the system (CVE-2009-1185) that grants the attacker root privileges [296]. | Backdoor |
| Lotoor | Targets Android users and looks for vulnerabilities in the device silently. It exploits the vulnerabilities to gain root privileges. After getting admin privileges, it collects sensitive info, monitors application installation, disables device security, and changes device settings. It must be downloaded manually [11], [297]. | Backdoor |
| GingerMaster | Repackages itself in legitimate applications and takes advantage of the GingerBreak root exploit to get root access. It connects to a C&C and downloads a malicious app from it into the device. It collects data about the infected device and sends it to the server. It targets users of android devices with the Gingerbread OS. [186], [298]. | Backdoor |
| Agent.JI | Disguises itself as an update for Flash Player. It is distributed through social media and certain adult-themed websites. Its main function is to monitor the infected device's activities as well as download other malware on the infected device [299]–[302]. | Backdoor (Backdoor (Dropper)) |
| VikingHorde | Creates a botnet that disguises ad clicks as proxied IP addresses to make money for the attacker. It spreads by disguising itself as games in the Google Play store. It connects with a remote server to receive and execute commands and sends device information to them. If the infected device is rooted, the malware can update and install malicious programs [15], [303]–[305]. | Backdoor (Dropper) |
| Boqx (AKA Boxer) | Is a repackaged version of a popular gaming application. It downloads malicious software and other contents from a remote server, specifically the malicious payload from xbox.ooqqxx.com [303], [306], [307]. | Backdoor (Dropper) |

**TABLE 3.** *(Continued.)* **Backdoor Category and its families.**

| | | |
|---|---|---|
| Ztorg | Is under the umbrella of Triada and works with two other families (Leech, Gorpo). It gains the root privilege of the device. It is embedded in legitimate applications. It only communicates with a remote server to download and install the malicious application. It uses a protection technique to completely hide from static analysis [15], [308], [309]. | Backdoor (Dropper) |
| Gorpo | Is under the umbrella of Triada with two other families (Ztorg, Leech). It gains root privilege of the device and installs the malware family, Fadeb [15], [308], [310]. | Backdoor (Dropper) |
| FakeDoc | Disguises itself as the legitimate "Android Battery Doctor", a battery booster application on the Android Market. It steals information from the victim and sends it to a remote server. It also aggressively displays ad pop-ups on the device. It can also download and install applications on the device [289], [18]–[314]. | Backdoor (Dropper) |
| Ramnit | Searches for files with specific extensions to infect them with malicious code. This makes it harder to remove it without erasing all the files. It spreads via an infected development environment. It is part of a botnet. It evolved from the source code of the Zeus Trojan. It steals financial information and banking credentials. It sends information to a remote server [315]–[319]. | Backdoor (Dropper) |
| DualToy | Infects Windows PC. It drops and installs malware on Android and iOS devices through side-loading. On the Android devices it infects, it contacts the C2C server and installs multiple Chinese applications. It mainly targets Chinese users, but it was found in devices in the United States, United Kingdom, Thailand, Spain, and Ireland [320]–[323]. | Backdoor (Dropper) |
| SecureUpdate | Targets Android users found in Middle Eastern countries. It disguises itself as security updates for the infected devices and spreads through malicious links in spear phishing campaigns and fake news websites by the Two-Tailed Scorpions. It downloads malicious payloads and exploits the Calendar function of Android to install the payloads at specific dates [324]–[327]. | Backdoor (Dropper) |
| xHelper | Disguises itself as a legitimate application by stealing package names of benign applications. Its main function is to download malicious applications. It remains on the device, persistently awaiting commands from a remote server. It is highly resistant to detection and deletion. It remains on the device even after a factory reset [328]–[331]. | Backdoor (Dropper) (Backdoor) |
| Claco | Disguises itself as a legitimate application. It infects Windows devices by injecting the Android devices with the malicious PE file into the SD card and connecting it via USB to the Windows device. The infected PE file will automatically run and inject the malware, Ssucl, which steals text messages, contacts, pictures, and all SD Card files [332]–[336]. | Backdoor (Dropper) |
| DropDialer | Disguises itself as a legitimate application that sets wallpapers found in the Google Play store. In reality, it downloads another malicious file in the background and tricks the user into installing this file on the infected device [332]. | Backdoor (Dropper) (Backdoor) |
| NotCompatible | Infects Android devices using a drive-by technique where the user visits a compromised website. Once it infects a device, it begins downloading the malware, update.apk, on the device. It then tricks the user into installing the downloaded malware [337]–[339]. | Backdoor (Dropper) |
| FoCobers | Spreads by injecting malicious code into applications and file types. It also injects malicious software into the device to spread malware [340]. | Backdoor (Dropper) |
| CepKutusu | Is a Turkish site that masquerades as an Android app store. All the applications this site offers contain infectious malware. When victims click on the Download Now button for an application, it installs banking malware on the device. It is capable of intercepting and sending SMS messages, displaying fake activity, and downloading other apps [341]–[344]. | Backdoor (Dropper) |
| FakeUpdates | Starts a service in the background that retrieves APKs from a remote server. It shows a dialogue box for an update to download the files into the SD card. It gathers device information, including International Mobile Equipment Identity (IMEI) number and International Mobile Subscriber Identity (IMSI) number, and sends them to a remote server [15], [310], [345], [346]. | Backdoor |
| DroidKungFu | Mainly targets Chinese users. It can root Android phones that are vulnerable and steal confidential information. It can do this by installing a backdoor on the device. It then sends the stolen information to a remote server [289], [347]. | Backdoor |

**TABLE 3.** *(Continued.)* **Backdoor Category and its families.**

| | | |
|---|---|---|
| GinMaster | Takes advantage of GingerBreak, a root exploit, and steals a device's confidential information. Then, it sends it to a remote website [289]–[291]. | Backdoor |
| XTaoAd | It's dex file contains no malicious code. However, it contacts its remote server and downloads and installs multiple arbitrary malicious JAR files on the device. It then loads and runs these files. Additionally, it auto-downloads applications and tricks the victim into installing them by appearing on the home screen of the infected device [332]. | Backdoor (Dropper) |
| CamScanner | Is injected in the code of the legitimate app, CamScanner. The application began as a legitimate application with no malware. However, recent versions have become infected with a trojan Dropper. Itdownloads malicious modules that perform other activities [348]. | Backdoor (Dropper) |
| Thanksgiving-Malware | Takes advantage of the shopping season before Christmas to trick users into downloading malware. They masquerade as shopping deal applications in order to trick users into installing them. Once installed, it will redirect the victim to a compromised website that injects malware into the device [349]. | Backdoor (Dropper) |
| HiddenApp | Disguises itself as a legitimate application in Google Play. Its main function is to download malware that displays ads [350]. | Backdoor (Dropper) |
| Tripoli | Describes an operation to target Libya and its cities. It spreads the malware through Facebook pages containing a malicious link. Its main objective is to spread the malware and infect as many devices with it as well as steal sensitive information [351], [352]. | Backdoor (Dropper) |
| unofficial Telegram | Claims to be an unofficial Telegram application that provides more features than the official application. In reality, the attackers inject malicious code into the open-source Telegram code. Its main activities include running services without the victim's consent and loading malicious websites [353]. | Backdoor (Dropper) |
| Shopaholic | Is also called Shopper. It disguises itself as an accessibility application found in third-party stores and the Play store. It can take control of the victim's Google, and Facebook accounts to register for shopping and entertainment applications. It can also leave five-star reviews on applications in the Play store [354], [355]. | Backdoor (Dropper) |
| starsWallpaper | Is similar to Agent. It disguises itself as wallpaper applications found in Google Play. It simulated the victim's clicks on ads to create revenue for the attacker [356], [357]. | Backdoor (Dropper) |
| Bios | Injects malicious dex code to ELF SO as well as other malware from the server [332]. | Backdoor |
| Oldboot | Infects devices using boot partitions and booting script files to inject malware on the device before the booting process. It downloads multiple applications on the device, which consumes its battery and bandwidth. Additionally, it steals and sends SMS messages [332], [358], [359]. | Backdoor |
| Fbot | Is a variant of Mirai. It spreads by searching for devices that have enabled ADB which is hosted on port 5555 open. Its main function is to search for the crypto-miner malware, Trinity, and remove it. This malware receives instruction from a remote server that uses blockchain to communicate with the malware [360]–[363]. | Backdoor |
| Dvmap | Is a rooting malware like Ztorg that injects malicious code into system libraries, allowing it to take control of the infected device and gain root access. It is distributed as a gaming application in Google Play Store. It bypassed the security measures by uploading a clean version of the app and then updating the application with the malware [92], [364]–[367]. | Backdoor (Dropper) |

been added as a subcategory of Backdoor, as shown in Figure 5. Users can mitigate and prevent these malware attacks in different ways. For example, they can enforce a network monitoring policy, install and download antivirus solutions, implement a network monitoring tool, and ensure their devices are protected with firewalls [28], [30]. The descriptions are shown in Table 3.

### C. BANKING

This section highlights the families that were classified as Banking, shown in Figure 6. Banking is a type of malware that imitates different banking application websites. This tricks the user into entering their banking credentials and private information, allowing the attacker to steal their financial assets [31]. These malware families can spread through Backdoor Trojans and spoof bank login pages. To avoid this malware infection, users can apply multi-factor authentication on their bank accounts, use a password manager for different accounts, and avoid installing software from unofficial websites or suspicious links. Organizations can also train their employees on cyber security awareness techniques and offer tips to prevent infection risks [31],

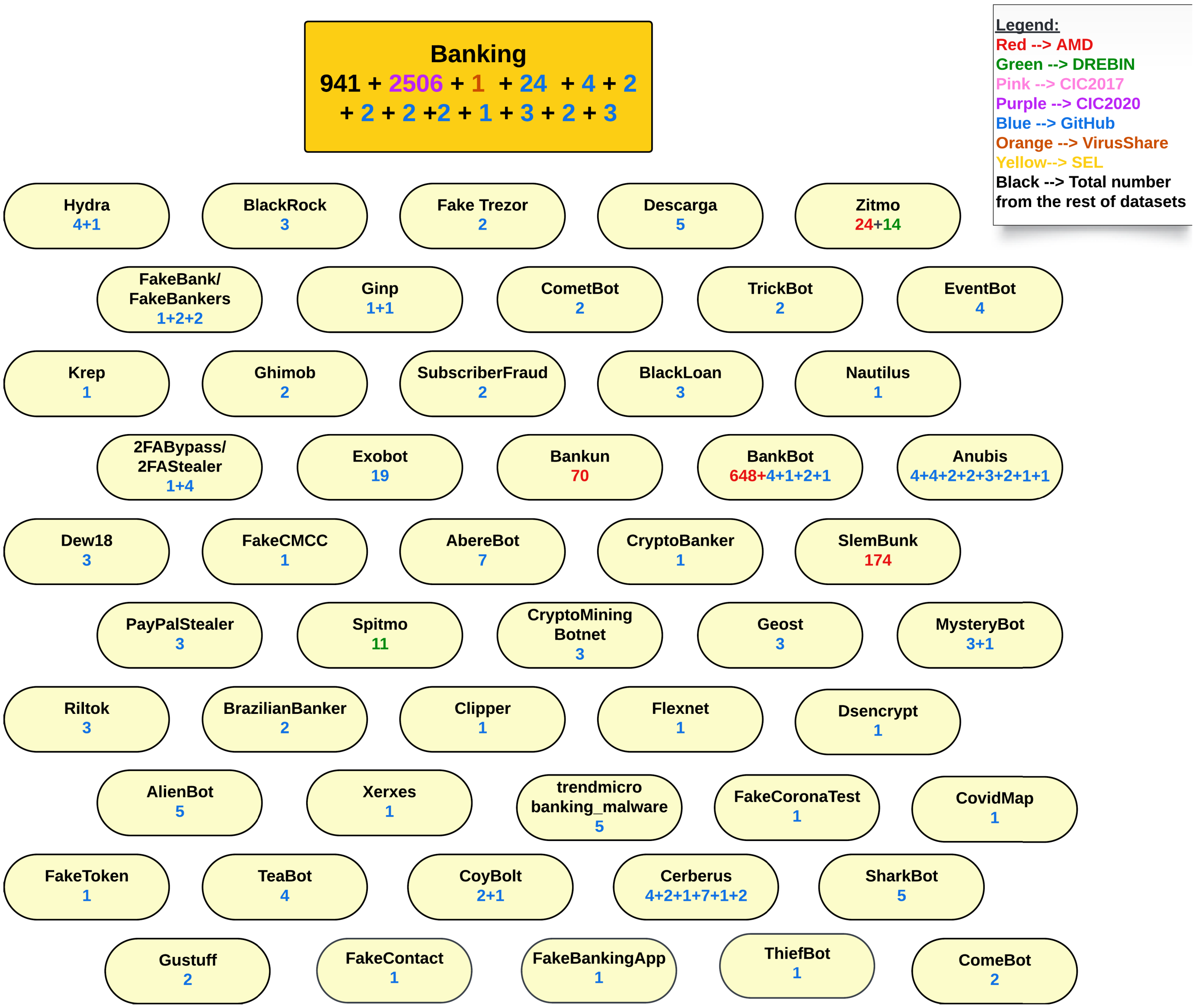


**FIGURE 6.** Banking Category with its families' names and their number of samples.

[32]. Table 4 specifies the description of the Banking families.

### D. RANSOMWARE

This section highlights the families that were classified as Ransomware. Ransomware, displayed in Figure 7, is a type of malware that prevents the victims from accessing or using their devices in different ways. It might lock the devices or encrypt the users' data. It then demands a ransom to be paid to the attacker for the users to regain access to their devices or data [33].The malware families in this category have several methods of spreading and infecting devices. These methods include network propagation, email attachments, removable media, malicious advertising or malvertising, social media, and SMS messages. Recently, Ransomware can be sold as a product or as a subscription in a business model known as Ransomware as a Service (RaaS). However, some techniques can be implemented to mitigate this type of attack. A number of these methods include keeping an offline backup of your data, recovering the data using reverse engineering if the attacker wiped the data, using IDS applications, avoiding interactions with suspicious links and email attachments [34], [35], [36]. The descriptions of the families are shown in Table 5.

### E. RISKWARE

This section highlights the families that were classified as Riskware, as shown in Figure 8. Riskware is legitimate software with no malicious intentions for the user. However, it has the high potential of evolving into a malware attack as the Android permissions of the software can be considered risky [37], [38]. Since Riskware is legitimate software, it can take many forms. These forms include applications, IRC

**TABLE 4.** Banking Category and its families.

| Family | Description | Category |
|---|---|---|
| FakeToken | Spreads through downloadable image links on SMS messages. It monitors the device's activities and calls. It records the conversation when the victim receives or calls a certain number. It performs an overlay attack on financial applications to steal the victim's login credentials and credit card information for monetary gain. It steals the one-time mTAN codes via SMS [368]–[372]. | Banking |
| BankBot | Steals the victim's confidential information, banking credentials, and credit card information. It displays a fake overlay window to mimic banking sites and applications to steal victim's information. These banking applications include CitiBank, WellsFargo, etc. It can send and intercept SMS messages, make calls, track infected devices, and steal contacts [92], [373]–[376]. | Banking |
| MysteryBot | Is similar to LokiBot but includes improved functionalities. It performs overlay attacks on different banking applications. It contains keylogging capabilities that record touch gestures and sends them to a remote server. The ransomware component is in development. It will lock the infected device's files in a password-protected ZIP file [377]–[380]. | Banking |
| SlemBunk | Is installed when users visit an adult website where a message prompts the user to upgrade flash. It disguises itself as a popular application. It checks if the victim opened a banking application. It overlays a phishing window on the application to steal user credentials and finances. It can forward SMS and calls from bank numbers [15], [381]. | Banking |
| Bankun | Pretends to be a legitimate Korean banking app. It gets root access to the infected device and replaces the legitimate banking application. It steals the victim's sensitive information when the victim enters their data in the UI of the "bank". It steals victim's contact information to send malicious links from the infected device [15], [382], [383]. | Banking |
| Zitmo (Zeus-in-the-mobile) | Spreads through infected security update links in SMS messages. It is cross-platform, affecting Blackberry, Android, and Windows Mobile. It is designed to intercept SMS from banks and steal mTAN (Mobile transaction authentication number)codes. It forwards the codes to a remote server and steals the personal information of the user to perform an unauthorized bank transaction and steal money [384]–[386]. | Banking |
| Spitmo | Intercepts SMS messages from banks and financial applications and sends them to a remote server. It then uses this code to validate bank transactions. It is also capable of stealing information [186], [387]. | Banking |
| AbereBot (Escobar) | Contains multiple new features. It disguises itself as a McAfee application in third-party markets. It steals the sensitive information of over 140 banks' customers through phishing overlays. It has gained more malicious features after rebranding into Escobar, including controlling a device remotely, removing itself from the device, and other malicious activities [388]–[391]. | Banking |
| AlienBot | Can be found in 9 different applications in the Google Play Store by using a new Backdoor, Clast82. It is a Malware-as-a-Service that allows a remote attacker to inject malicious code into financial and banking applications to steal the victim's credentials and account details. It allows the attacker to take full control of the infected device [392]–[394]. | Banking |
| Anubis | Disguises itself as the French telecom company Orange S.A application. Once downloaded, it steals the login credentials of the user. It uses stolen information to steal the victim's money from banks, financial institutions, cryptocurrency wallets, and virtual payment platforms. It has affected over 400 financial institutes [395], [396]. | Banking |
| Cerberus | Is distributed as MaaS in underground forums. It disguises itself as a Flash Player application and escalates privileges. It connects to a remote server to perform multiple malicious actions. It performs overlay attacks on various banking apps to steal login credentials, credit card details, and 2FA codes. It avoids detection by taking advantage of the device's step-counting features [397]–[402]. | Banking |
| Hydra | Uses an overlay attack to steal the login credentials, similar to Anubis, of the victim's bank account, specifically in the German bank Commerzbank. It hijacks the bank's login page and overlays a fake page to steal the victim's credentials. It is injected into banking applications that claim to be legitimate. It is distributed to the PlayStore using a Backdoor [399], [403]–[407]. | Banking |

**TABLE 4.** *(Continued.)* **Banking Category and its families.**

| | | |
|---|---|---|
| trendmicro<br>_banking<br>_malware | Describes different families of banking malware that steal the victim's banking credentials through phishing techniques and lock them out of their devices. (Fanta, CRYPICH, Ramnit, Cridex, Yuyapa, Malphishing) [408]. | Banking |
| Sharkbot | Is distributed in legitimate-looking antivirus applications in Google PlayStore that claims to clean the system. In reality, it targets Automatic Transfer Systems (ATS) to initiate money transfers stealthily by bypassing 2FA techniques. It performs overlay attacks to steal banking login credentials. This malware is mostly active in the UK, Italy, and the US [409]–[413]. | Banking |
| TeaBot | Steals a victim's bank account credentials and any information related to online banking. It also acts as a remote access trojan (RAT) that can take control of the infected device from a remote location. It masquerades as an application that can scan barcodes in the Google PlayStore [414]–[417]. | Banking |
| Exobot<br>(Marcher) | Spreads by sending malicious download links through SMS. It then downloads an application that appears legitimate where it requests various permissions. It performs two different attacks: an overlay attack to trick the victim into giving the attacker their banking login credentials and an interception of SMS messages to compromise the bank's 2FA mechanism [418]–[420]. | Banking |
| Comebot | Is similar to Anubis [421], [422]. | Banking |
| Descarga | Tricks the victim into downloading legitimate-looking messaging applications. It displays icons for different MMS applications when the victim installs them. Once launched, it persistently requests admin privileges until accepted. It displays a Google Play pop-up that asks for credit card information. It sends device information to the attacker's C2C server [423], [424]. | Banking |
| Dsencrypt | Disguises itself as the Google Play store app that requests admin privileges. Once granted, a pop-up alert is displayed with the messages "Program Error" and "It's Deleted!". It then disappears from the home screen but still performs malicious activities on the device. This includes stealing text messages, signature certificates, and bank passwords and sending them to the attacker [425], [426]. | Banking |
| FakeBankers/<br>FakeBank | Can be found in 22 apps distributed in third-party stores and social media sites. It mainly targets banks in Korea. It intercepts a victim's phone calls targeted to their banks and redirects them to the attacker impersonating a bank representative to steal banking details. It collects bank SMS messages, records bank calls, and displays a fake bank login UI [332], [427]–[430]. | Banking |
| Krep | Targets the largest bank in Russia and Eastern Europe, Sberbank. It disguises itself as the bank's application with a login page very similar to the legitimate application to steal the victim's credentials. It also targets WhatsApp users by deceiving them with a paid encryption service. It overlays a screen on the legitimate application asking for payment details [431]. | Banking |
| FakeCMCC | Targets users in China that spread by sending an SMS message with a link claiming they won 100 Yuan. The link redirects them to a malicious website where a login button is shown. Once clicked, it directs them to enter their banking credentials to receive the bonus. It also asks the victim to install a fake China Mobile app to get the bonus [332]. | Banking |
| Dew18 | Disguises itself as a well-known banking application found in Korea. It executes when the victim adds their information to the loan application page. Clicking the "Apply" button sends a confirmation message. It begins with the victim's banking details. It blocks the victim's calls to the bank support by monitoring their calls and playing a pre-recorded audio file [432]. | Banking |
| PayPalStealer | Disguises itself as a battery optimizer application found in third-party markets. It steals money from the victim's PayPal account by mimicking the victim's clicks. It then transfers the victim's money to the attacker's account. It can also perform an overlay attack over the screens of targeted legitimate applications [433]–[436]. | Banking |
| 2FABypass/<br>2FAStealer | Is able to bypass Google's 2019 restrictions on SMS and Call Log Permissions. It steals OTP codes without asking for SMS Permissions. It disguises itself as BtcTurk, a Turkish cryptocurrency exchange. It steals the OTP from the notification display on the device and dismisses the notification. This allows it to avoid the detection of fraudulent actions [437]. | Banking |

**TABLE 4.** *(Continued.)* Banking Category and its families.

| | | |
|---|---|---|
| CoyBolt (BasBanke) | Targets Brazilian Android users by sending malware advertisements on Facebook and WhatsApp. The link redirects them to the application stores that host the malware, where it disguises itself as a utility application (CleanDroid). It steals the victim's financial information. It also has spyware capabilities such as keylogging [438]–[440]. | Banking |
| Crypto-Mining-Botnet | Infects Android devices through open ports in the ADB. Its main function is to use the infected device's resources for crypto-mining [441]. | Banking |
| FakeBanking-App | Disguises itself as the Ziraat Bank mobile application. Its main function is to steal the victim's banking credentials. It also downloads payload to intercept the bank's OTP message [442]. | Banking |
| Gustuff | Spreads by its download links sent through SMS messaging. Its main functionality is to steal and phish the victim's credentials from banking and financial applications as well as from Android payment and messaging applications [443]–[445]. | Banking |
| Riltok | Targets users in Europe and Russia. It infects devices by disguising itself as legitimate free ad services and spreading via SMS messages. The main function of the malware is to perform overlay attacks on the financial application that the user opens in order to steal their banking and financial credentials [446]. | Banking |
| Clipper | Exploits the tendency of users to copy the addresses of cryptocurrency wallets into clipboards. Specifically, it intercepts the copied address and changes it to whatever the attacker wants it to be. The attacker could change the address to their wallet in order to take the money [447]. | Banking |
| FakeTrezor | Disguises itself as Trezor, the cryptocurrency wallet. Itdisplays a login page where the victim enters their credentials and sends them to the attacker [448]. | Banking |
| Geost | Disguises itself as a legitimate application. Its main function is to steal banking and financial information through the victim's SMS [449]. | Banking |
| Ginp | Targets banks in Spain and the UK. It disguises itself as an Adobe Flash player. It performs overlay attacks to steal the victim's login credentials and credit card information [368], [442], [450], [451]. | Banking |
| CometBot | Targets banks in Germany. It is also based on the banking trojan, BankBot. It steals the banking credentials of the victims and is able to intercept the mTAN (Mobile transaction authentication number) to avoid detection [442], [452]. | Banking |
| Covid _CovidMap | Is infected with CERBERUS via VirusTotal reports. The malware disguises itself as a covid19 map website but in reality it infects the victim with the malware [453], [454]. | Banking |
| EventBot | Disguises itself as legitimate applications with very similar icons, which can confuse the victim. Its main function is to steal the financial and banking information of the victim in their banking applications by intercepting and reading SMS and bank pins. It can also log in to the victim's banking accounts [455]–[457]. | Banking |
| Xerxes | Used to be a private hacking tool used exclusively by a hacking group. Then, its source code became public, and its popularity increased with cyber-criminals. It not only steals the banking credentials of the victim, but it also encrypts the device's files and data. The malware then demands a ransom to decrypt the files [458]–[460]. | Banking |
| BlackLoan | Targets VISA customers in China, Vietnam, Malaysia, and other countries. It disguises itself as a Visa website that tricks users into entering their banking and personal information [461], [462]. | Banking |
| Nautilus | Disguises itself as a covid-related application, specifically a COVID-19 alert application. When the victim turns on the alerts, it begins to silently collect and send sensitive information from the device to the attacker [380], [442], [463], [464]. | Banking |
| covi-FakeCorona-Test | Is a banking trojan that steals the victim's banking information via VirusTotal report. It uses Covid19 to trick users into downloading and installing the app [465]. | Banking |
| FakeContact | Masquerades as applications that can trace contacts from third-party stores. The main function of the malware is to steal sensitive data from the victim, including banking and financial credentials [466]–[468]. | Banking |

**TABLE 4.** ***(Continued.)*** **Banking Category and its families.**

| | | |
|---|---|---|
| Flexnet | Is based on GM Bot Trojan. It spreads via links sent by SMS messages. Once installed, it shows an error to the victim and hides its icon to avoid removal. Then, it steals the victim's banking information and mobile phone accounts to steal their money. The attacker uses that money to pay for multiple services [442], [469]. | Banking |
| Brazilian-Banker (BrazKing) | Disguised itself as legitimate applications for Brazilian banks. It displays the login page of the banks in order to steal the banking credentials of the victim [470]–[472]. | Banking |
| BlackRock | Targets different, popular applications installed on the device, including banking, shopping, and entertainment apps. It spreads through third-party stores. Its main capability is performing overlay attacks on the targeted applications to steal the victim's credentials. It performs several other activities, including intercepting SMS and keylogging the device [473]–[476]. | Banking |
| Ghimob | Spreads by sending phishing emails claiming to be creditors containing the malicious link. It can steal sensitive information from 153 banking, financial, cryptocurrency, and exchange applications. It allows the attacker to control the device remotely to make transactions using the victim's account [477]–[480]. | Banking |
| ThiefBot | Targets clients belonging to Turkish banks. It steals the banking and finances of the victim [481]–[483]. | Banking |
| TrickBot | Targets both organizations and individuals for their banking information, account credentials, and bitcoins. It spreads via spam email campaigns and infected website URLs. Additionally, it is able to intercept SMS messages to get the banking OTP [484]–[486]. | Banking |
| Subscriber-Fraud | Disguises itself as a photo editing tool. When the user installs the tool, It begins to steal information from the device and send it to a remote server. While the victim uses the limited functions of the application, the malware begins to subscribe the user to a paid service by opening the compromised web pages [487]. | Banking |
| Crypto-Banker | Aims to steal the victim's PayPal credentials in the infected device. Once it steals the credentials, it encrypts the device's files and locks the infected device [442]. | Banking |

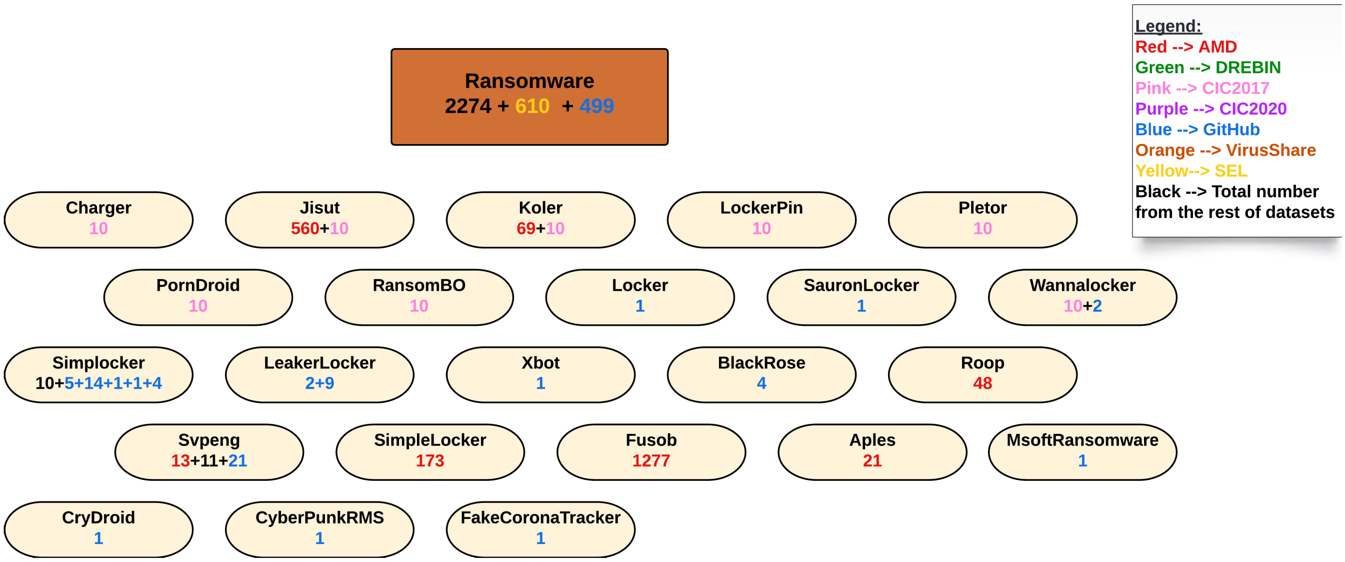


**FIGURE 7.** Ransomware Category with its families' names and their number of samples.

(Internet Relay Chat) clients, dialer programs, file downloaders, monitoring software, password management, and Internet server services. To avoid making it malicious, users must install antivirus solutions, implement risk management plans in organizations, and use detection tools to identify the risk. They must also uninstall the software if it has become

**TABLE 5. Ransomware Category and its families.**

| Family | Description | Category |
|---|---|---|
| Charger | Embeds itself in legitimate applications. It steals contacts and SMS messages from the infected device. It asks the victim to allow it to gain admin permissions. If granted, the malware locks the victim out of the device and displays a message with a payment demand of 0.2 bitcoin, or $180. It avoids detection by encoding its string into binary arrays [488]–[490]. | Ransomware |
| Jisut | Mainly targets Chinese users. It was initially created as a malicious prank, then later used for financial gain as well. It locks users out of their devices and delivers a random message via a female voice. It resets the PIN code so the user can't restart it and displays a ransom of 40 Yuan. To prevent installation, the malware preserves the admin privileges it obtained [491]–[493]. | Ransomware |
| Koler | Is packaged as an adult-themed application. It displays an FBI warning as a scare tactic to trick the victim into paying the ransom. If the ransom is not paid, the FBI warning will be displayed repeatedly and persistently on the device screen, effectively locking the device [494], [495]. | Ransomware |
| LockerPin | Was one of the first true examples of ransomware permanently locking a device from the victim. It makes the device very difficult to unlock without losing all the victim's data. A ransom of $500 is demanded with a message that this is a fine for viewing illegal adult material. It prevents uninstallation by obtaining and preserving admin permissions [496]–[498]. | Ransomware |
| Pletor | Searches for files in the connected SD card and encrypts them using AES encryption. It specifically targets media files and documents. It then sends a threatening ransom message demanding payment to decrypt the file [499], [500]. | Ransomware |
| PornDroid | Hides behind a fake application. Once downloaded, the malware also downloads LockerPin, which locks the device by changing its PIN. Masquerading as the FBI, it sends the victim a message accusing them of having illegal materials on their devices (child pornography). The victim must pay a fine of $500 in order to use the infected device again [501]–[504]. | Ransomware |
| Simplocker (SLocker) | Targets users in Ukraine. It disguises itself as a law enforcement application. Once installed, it steals device information and sends it to a remote server (CC). It also encrypts files on the local drive using AES encryption. To decrypt the files, the victim must pay the ransom request of 260 UAH (16 EUR) through the MoneyXy service [500], [505]–[508]. | Ransomware |
| Svpeng | Was originally created to steal credit card information. It was then converted into a ransomware that locks users out of their devices. It displays a message that accuses the victim of downloading child pornography. To unlock the devices, the victims must pay the attacker a fine. It also scans the device for banking applications to compromise them in the future [509], [510]. | Ransomware |
| Wannalocker | Is a variant of WannaCry. It encrypts files in the external storage disk of the device using AES, similar to SimpLocker. It displays a ransom demand window similar to WannaCry's display. It also shows two different timers: one to countdown the time left to double the ransom money and another timer to countdown until all the files will be deleted and lost [511], [512]. | Ransomware |
| Fusob | Targets users in Germany, US, and UK for state-sponsored attacks and espionage. It is used as a RAT to remotely access the device. It accuses the victim of a misdemeanor and changes the device's PIN. It then demands a ransom in the form of a fine to unlock it. It does not activate for devices set with post-Soviet countries' languages. It survives factory resets [12 ]–[515]. | Ransomware |
| RansomBO | Causes many changes to the device, such as data encryption once downloaded. To reverse these changes, it "advises" the victim to pay the ransom to the attacker [21], [494], [516], [517]. | Ransomware |
| SimpleLocker | Encrypts the victim's data in external storage using AES with a unique key and demands payment. It changes the name and extensions of the files as well. A more advanced version uses a key per device rather than a single unique key [15], [518], [519]. | Ransomware |

**TABLE 5.** *(Continued.)* **Ransomware Category and its families.**

| | | |
|---|---|---|
| Roop | Hides in malicious programs. It attempts to gain admin privileges. It locks the user out of the device and demands a ransom. It is executed every time the device is booted [15], [520], [521]. | Ransomware |
| Locker | Tricks users into thinking it is a system update application. Once launched, it sends a confirmation message to the attacker. It locks the device after updates are installed and displays a ransom demand. It will turn the infected device off if the victim attempts to remove it and warns them that the device's data will be removed. Once the victim clicks on an option, a screen with a password shows up to leave standby mode [522]–[524]. | Ransomware |
| Aples | Disguises itself as an antivirus scanner. It locks the device when the user launches the application. When the victim reboots the device, an FBI warning screen is displayed with a demand for payment [15], [525]. | Ransomware |
| LeakerLocker | Claims it made a backup of a victim's sensitive information unlike many ransomware that encrypts a victim's file for ransom. It then threatens to leak the information if the victim does not pay the ransom. It spreads through two applications found in the Google PlayStore, "Wallpapers Blur HD" and "Booster Cleaner Pro" [526]–[529]. | Ransomware |
| xbot | Mainly targets users in Russia and Australia. It disguises itself as a banking application and the Google Pay interface. This allows the attacker to steal the victim's banking credentials and credit card information. The attacker sends a command to it to encrypt the device's contents and external storage. It displays a message for a ransom payment of $100 [530]–[533]. | Ransomware |
| BlackRose | Is considered as MaaS that can be sold to interested buyers. It disguises itself as a video player application and requests Accessibility Services. It then begins to encrypt the files from the system's directories. It then shows the victim a message that demands $500 as payment for inappropriate materials from the FBI to decrypt their files [534]–[538]. | Ransomware |
| SauronLocker | Disguises itself as a legitimate application. Once launched, it encrypts the device's files and replaces the home screen wallpaper with the ransom note. Additionally, it abuses the device's resources to mine cryptocurrency [442], [539], [540]. | Ransomware |
| CryDroid | Disguises itself as a COVID-19 tracing application. In reality, it encrypts common file types in the system directory. It displays a notification for the user to open the ransom note. Encrypted files have the .enc file extension [541]. | Ransomware |
| Cyberpunkrms | Disguises itself as a fake mobile version of the popular PC and console game, Cyberpunk 2077. Once it gains access to the device's files, it encrypts them and sends a ransom note to the victim with instructions to pay $500 to decrypt them. If the victim fails to pay the ransom, all the files will be deleted [542]–[544]. | Ransomware |
| FakeCorona-Tracker | Disguises itself as a COVID-19 tracker application, "COVID-19 Tracker". When it is installed and executed, it locks the infected device and encrypts the device's files. It displays a ransom that demands a payment of $100 in Bitcoins in 48 hours to unlock the device and decrypt the files. Otherwise, it will delete the files on the device [545]–[547]. | Ransomware |
| Msoft-Ransomware | Spreads through online forums and different websites by masquerading as different applications. It blocks access to the device by displaying the ransom note on every window. It abuses system alert windows, accessibility features, and notification services. It uses machine learning to continuously evolve and change [548], [549]. | Ransomware |

infected [39], [40]. Table 6 displays the description of each family.

### F. SMSMALWARE

This section highlights the families that were classified as SMSMalware, displayed in Figure 9. SMSMalware is a type of malware that is spread by sending malicious links through SMS messaging texts as well as malicious websites [41], [42]. Additionally, once installed, this malware misuses the messaging feature by sending and receiving messages using the device, which can financially drain the victim [41], [42]. Users can protect themselves from this malware through different mitigation techniques, such as avoiding opening suspicious links, using malware detection applications, being cautious of senders and unusual messages, and reviewing their transactions and bills for suspicious activities [43], [44]. Table 7 describes the families collected in detail.

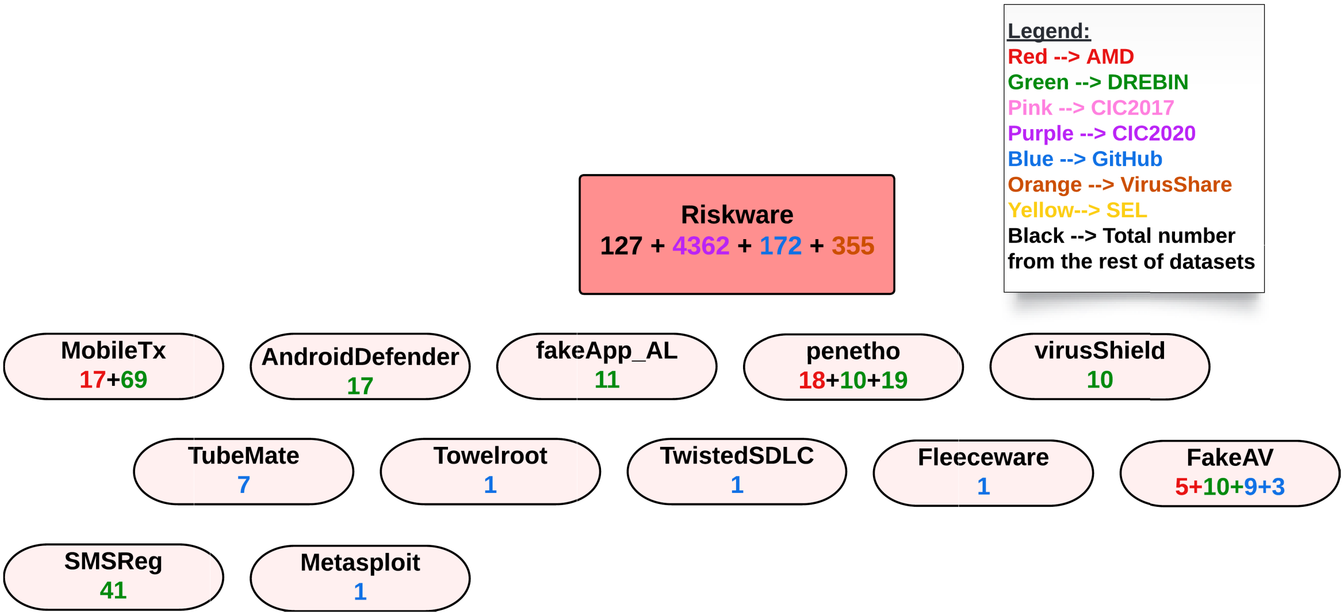


**FIGURE 8.** Riskware Category with its families' names and their number of samples.

### G. SPYWARE

This section highlights the families classified as Spyware, shown in Figure 10. Spyware is a type of malware that hides in a victim's device and begins stealthily monitoring them and their activities. It collects valuable information and sends them to the attacker without the victim's knowledge [45]. The families in the Spyware category can spread through multiple means. These methods include SMS texts, calls, malicious websites and applications, malicious files, email attachments, media devices, and fake login screens [46], [47]. The Trojan-Clicker is considered a subcategory of Spyware based on its behavior, as shown in Figure 11. The Clicker remains hidden in the victim's device and simulates their clicks to provide revenue for the attacker [48]. However, users can mitigate the malware families in this category through careful techniques. These techniques include using antivirus and anti-spyware software, not interacting with suspicious links, using malware detection applications, and being cautious of senders, unusual messages, and free application links [46], [47]. Table 8 describes the families of the Spyware category in detail.

## V. HOW TO UTILIZE THE MALOID DATASET

As elaborated before, the Maloid dataset is distinguished in collecting a massive number of different malware families with proper categorization, a large number of samples, and a detailed description of malware families all in one source. This section focuses on how researchers and developers can heavily utilize Maloid to build security and smart solutions to throttle, predict, detect, and prevent Android malware, as the impact of malware on Android devices and data might be severe.

Figure 12 provides an overview of how Maloid can benefit the malware forensics field. For example, the executable malware samples (APK files) can be taken as is and run as part of the dynamic analysis that studies the behavior of the malware during the execution time, whether in a real environment or a virtual one. On the other hand, reverse engineering could be applied to the APK files to recover the original code and then run different types of analysis on the source code, including parsing, feature extraction, and static analysis. Additionally, malware itself in its executable form, can be converted to images, whether gray or colored, to run different types of analysis called vision-based.

This paper highlights four cases in which different analysis systems can effectively utilize Maloid to detect Android Malware with high accuracy.

### A. CASE STUDY I. VISION-BASED ANALYSIS

We conducted this case study where we utilized the Maloid dataset to build an accurate AI-based predictive model integrated with our ongoing, in-development malware detection tool. This case study follows a similar process in a previous work [49]. We first converted the malware and benign APK samples in the Maloid dataset into images to do this. More accurately, we converted the APKs to grayscale images and RGB images. After converting the images, they were divided into three subsets: testing, validation, and training. Specifically, the training subset is used to train the model and learn the features of the samples. The validation subset ensures that the model is not overfitted and performs well. Finally, the testing subset calculates the model's performance in the form of different detection metrics.

**TABLE 6.** Riskware Category and its families.

| Family | Description | Category |
|---|---|---|
| MobileTx | Steals the International Mobile Subscriber Identity (IMSI) number and other information and sends it to a remote server. It also sends the IMSI number as an SMS message to a specific number [550]. | Riskware |
| SMSreg | Disguises itself as a legitimate application called "Battery Improve" that claims to maximize a device's battery usage. In actuality, it silently collects data without the victim's knowledge or consent. In malicious hands, it could damage the device and perform other malicious activities [17], [551]. | Riskware |
| TubeMate | Is originally legitimate and causes no harm to the device. It is a popular application found in third-party markets. It downloads videos from social media applications. Malicious attackers exploit its poor security and perform attacks on the device that downloaded TubeMate. Many attackers disguise their malware as TubeMate. It also displays multiple pop-up ads [324], [552]–[554]. | Riskware |
| fakeAV (Fake Anti-Virus) | Disguises itself as a legitimate antivirus application. It performs a fake scan for free and claims to find viruses and malware on the device. The victim must register to the application service and pay a fee to remove them. Even if the user rejects the service and payment, it installs other malicious programs without the victim's knowledge [555], [556]. | Riskware |
| Twisted-SDLC | Infects Google apps with malicious Windows executable files. This doesn't harm the Android devices, but it shows that the applications were developed in infected Windows machines. This could have negative impacts on the software development life cycle [557]. | Riskware |
| Fleeceware | Is found in legitimate applications. It allows the user to download them for free for a short period of time. If the user hasn't uninstalled the application, it will charge hundreds of dollars from the user. There is no malicious code in the applications, but they abuse the business model in the Play store [558]. | Riskware |
| virusShield | Claims to be an antivirus solution. However, users have to pay $3.99 to download the application on their android device. It does not actually scan for malware and is a scam [559]. | Riskware |
| Android-Defender | Impersonates antivirus software. Specifically, it scans the infected device for any virus. It then suggests to the victims to buy a clean-up service after finding non-existent viruses in the device [560]–[562]. | Riskware |
| fakeApp_AL | Is found in the market, hiding as Minecraft cheat applications. When the user opens the application and interacts with the interface, the application warns that a dangerous virus is infecting their device. The victim must subscribe to a premium-rate SMS service and activate it to remove the virus [563], [564]. | Riskware |
| Towelroot | Is a rooting tool developed by famous white hat hacker, George Hotz. It allows Android users to root their own devices with a simple one-click interface by exploiting the Android kernel's vulnerability (CVE-2014-3153). Attackers can repackage it as a legitimate application. They are then able to root the Android device and perform malicious activities [565]–[568]. | Riskware |

After dividing the dataset into subsets, 22 different models were built. These models are CNN-based algorithms include our developed Scratch model [49],VGG16, ResNet50, VGG19, DenseNet121, DenseNet169, DenseNet201, EfficientNetB0 to EfficientNetB7, InceptionResNetV2, InceptionV3, MobileNet, MobileNetV2, MobileNetV3Large, MobileNetV3Small, and Xception models [50], [51], [52]. A complete list of all the models used can be found in Figure 13. After creating the models, they were then loaded to begin the training phase. The model was trained using the images saved in the training subset and then using the validation subset. After training the models with a satisfying number of trials, the best parameters produced were saved for the evaluation of the models. These parameters include the learning rate, the security analysis, and other important CNN parameters.

Subsequently, the collected CNN models were then tested. The tests were conducted using the best parameters saved during the training. The results of this testing are then evaluated using specific metrics. These metrics were chosen

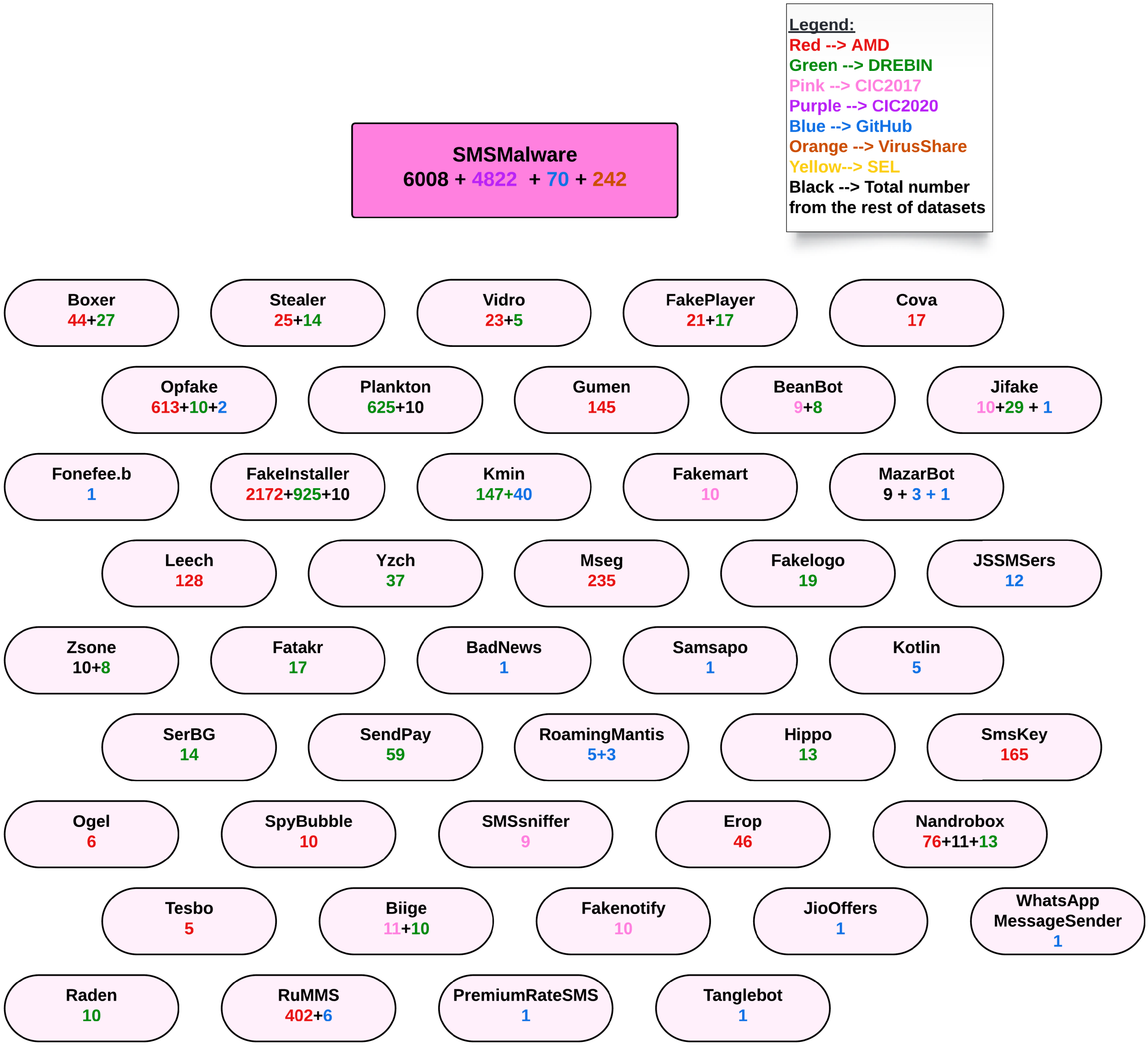


FIGURE 9. SMSMalware Category with its families' names and their number of samples.

based on the models' needs, available resources, and the created dataset's effectiveness. These metrics include the F1 score, precision, and recall of the models. RGB and grayscale vision samples were used during this experiment. The summary of the performance results is shown in Table 9. From this table, it can be concluded that the Scratch CNN model [49] achieves superior detection efficiency for the color & grayscale formats of the Maloid dataset compared to other models.

Finally, after acquiring the results of the models and gauging their accuracy, we started integrating the model with our malware detection tool. Currently, we are in the process of testing our tool and its accuracy with the AI model integration. The results of this integration and further details will be specified in future work. This case study is one of the many methods of using our extensive dataset in the malware detection field. The summary of this case study steps can be found in Figure 13.

### B. CASE STUDY II. CATEGORY-BASED ANALYSIS

To evaluate the credibility and precision of our extensive dataset, an additional case study was conducted specifically focusing on a particular category within the collected dataset, namely the Ransomware category. The primary aim of this case study was to conduct a static-based analysis of both the ransomware and benign samples to gain valuable insights.

To facilitate the analysis, we randomly selected a subset consisting of 500 ransomware APKs and 500 benign APKs.

**TABLE 7.** SMSMalware Category and its families.

| Family | Description | Category |
|---|---|---|
| FakeInstaller | Disguises itself as an installer for other applications. When the malware is executed, it sends SMS messages to premium rate numbers belonging to the attacker to steal money from the victims [17]. | SMSMalware |
| Plankton | Steals device information and silently sends them to a remote server when installed on the device. Additionally, it downloads files onto the device that could be malicious [569]–[571]. | SMSMalware |
| Opfake | Sends SMS messages to premium-rate numbers which charge the victim [572], [573]. | SMSMalware |
| BeanBot | Sends out premium-rate SMS messages from the infected device. It forwards the device's data to a remote server and takes control of the device using the remote server to create a bot network [20], [575]. | SMSMalware |
| Biige | Records SMS messages, calls, locations, and others and uploads them to a remote server. It performs root exploitation to escalate privileges. It downloads software on the device. It also sends spam and SMS to the victim contact list [186], [374]. | SMSMalware |
| Fakemart | Targets android users in France. It masquerades as a front-end application to access the Black Market. It sends premium SMS to short numbers without the victim's knowledge. It updates the configuration and makes silent calls in the background. It removes the SMS responses and notifies a remote server when a specific SMS response is received [186], [374], [576], [577]. | SMSMalware |
| Fakenotify | Pretends to be an update notifier application. It sends SMS messages to premium rate numbers and downloads malicious software. It redirects users to malicious websites. It avoids detection from antivirus by using obfuscation techniques [186], [374], [578], [579]. | SMSMalware |
| Jifake | Disguises itself as a messaging application, Jimm, that is popular in Russian-speaking countries. It mainly silently sends SMS messages to premium-rate numbers (5537). It also downloads other malicious software [374], [580]. | SMSMalware |
| MazarBot | Spreads by sending malicious APK links in SMS messages. It gains the device's admin privileges and erases any stored data on the infected device. It turns the device into a hacker's network of the botnet. It targets specific locations via geographical location attack and avoids installation on devices set to the Russian language [374], [581]. | SMSMalware |
| Nandrobox | Steals data from the infected device and sends them out using SMS messages to a specific number (1065800815747). It then intercepts incoming messages from that number and deletes them to avoid detection [186], [374], [582]. | SMSMalware |
| SMSsniffer | Steals information on the device and sends SMS messages to other devices [186], [374]. | SMSMalware |
| Zsone | Is found in third-party markets. It is mostly targeted at users in mainland China. It sends SMS messages to premium-rate phone numbers and registers users to a paid service. It removes all SMS messages from specific originating numbers [186], [374], [19], [584]. | SMSMalware |
| RuMMS | Targets users in Russia. It sends fake SMS messages with links infected with the malware to victims. It requests admin privileges that allow the malware to hide itself and avoid detection. It sends SMS to banks and victim's contacts, uploads SMS to servers, and forwards incoming calls. It is named as RuMMS because its URLs are all in the same format: (-).ru/mms.apk [585]–[587]. | SMSMalware |
| SmsKey | Sends SMS to premium rate numbers. It spreads by embedding itself into a host app that a victim downloads [15], [588]. | SMSMalware |
| Gumen | Sends SMS to premium rate numbers and subscription services. It sends device information to attackers [15]. | SMSMalware |
| Leech | Is under the umbrella of Triada and works with two other families (Ztorg, Gorpo) to take over the Zygote process. It gains the root privilege of the infected device. It installs the malicious app to the system folder [15], [308], [589]. | SMSMalware |
| Erop | Sends SMS to premium rate numbers. It intercepts messages from infected devices and steals personal information. It disguises itself as the application EroPlayer app [590]–[593]. | SMSMalware |

**TABLE 7.** *(Continued.)* **SMSMalware Category and its families.**

| | | |
|---|---|---|
| Boxer | Differs from Boqx. It silently sends SMS to premium rate numbers via commands. It receives SMS messages and makes phone calls. It has affected a total of 63 countries. It spreads through infected applications in the Google Play Store. It also poses as fake downloaders and installers. It sends sensitive information to the server [15], [594]–[598]. | SMSMalware |
| Stealer | Sends SMS messages to premium-rate short numbers without the victim's knowledge. It encrypts data with BASE64 and GZip. It receives commands from a remote server and sends the results back to the server [15], [599]–[601]. | SMSMalware |
| Vidro | Connects to a remote site and updates itself. It sends SMS messages to premium rate numbers without the victim's consent. It connects to another remote server and downloads content from the server. It spreads when the victim visits an adult website and installs the adult application [591], [602], [603]. | SMSMalware |
| FakePlayer | Disguises itself as a legitimate media player. It sends SMS messages to Russian premium rate numbers and charges the victims money for sending these SMS [583], [604], [605]. | SMSMalware |
| Cova | Enrolls users in premium SMS services. It secretly installs apps and prompts users to download them. It loads web pages on the infected device that sends SMS messages to different numbers when the victim interacts with them [15], [71]. | SMSMalware |
| Ogel | Gathers SMS and device information and sends them to a remote server. It hides the remote server's URL using Java native code to hide their malicious intent and avoid detection. It also sends SMS to specific targets [15], [606]. | SMSMalware |
| Tesbo | Connects to multiple remote servers and receives commands from them in XML. It gathers device information such as International Mobile Subscriber Identity (IMSI) number and application package name. It sends out SMS messages to a specific remote server with the message "[IMSI]@[random from 1-10]" [15], [607] | SMSMalware |
| Raden | Sends SMS messages to a Chinese premium number [186]. | SMSMalware |
| Hippo | Sends SMS messages to premium rate numbers which charge the victim. Additionally, it intercepts the received SMS message to avoid detection [14], [186]. | SMSMalware |
| SerBG | Is also known as Launcher. It disguises itself as the utility application, Android Market Security Tool. It collects contact and device information on the device, such as IMEI, SMS sender number, and phone number. It also blocks SMS messages from certain phone numbers [14], [608]. | SMSMalware |
| Fatakr | Disguises itself as an income solution application found on the Play Store. It steals user information and sends it to the attacker through SMS messaging, which charges the user [186], [609]. | SMSMalware |
| Fakelogo | Uses the infected device to send SMS messages in a specific format to multiple, specific numbers. It also verifies that the message is delivered using the standard SMS verification function [14], [610], [611]. | SMSMalware |
| Yzhc | Sends SMS messages to multiple premium rate numbers, which can charge the victim of the infected device. The contents of the message include a text with the letters "YZHC", the IMEI number of the device, and user value., which increases the charge for the victim. It disguises itself as PPXIU, a Chinese social network [14], [609], [612]. | SMSMalware |
| Covid (TangleBot) | Targets Android users in the US and Canada. It takes advantage of the COVID-19 pandemic and sends SMS messages claiming to have information on Covid and vaccinations with a link. Once the link is clicked, it will download the malware on the device. It can perform multiple tasks, such as stealing the victim's banking credentials through overlay attacks [613]–[615]. | SMSMalware |
| Android.-Troj.at-fonefee.-b | Sends premium SMS messages from the infected device [186], [616]. | SMSMalware |
| JSSMSers | Disguises itself as applications found in the Google Play store. It subscribes the victim to premium SMS numbers. It bypasses the user's notice by intercepting the welcome message from the subscriptions service and marking it as read [12 ], [618]. | SMSMalware |
| BadNews | Disguises itself as advertising libraries in legitimate applications. In reality, it displays advertisements and fake news articles that link to SMS fraud malware [332]. | SMSMalware |

**TABLE 7.** ***(Continued.)*** **SMSMalware Category and its families.**

| | | |
|---|---|---|
| Samsapo | Sends SMS messages to infected Android devices with a Russian message, “Is this your photo?” and a malicious link. Like PC worms, it spreads by sending messages and links to saved contacts. It downloads additional malicious files, steals and sends information to a remote server, and registers the device to a premium-rate service [332], [619], [620]. | SMSMalware |
| Kotlin | Describes the first malware that was written in the Google programming language, Kotlin. It disguises itself as an Android device optimizer, “Swift Cleaner”, found in the Google Play Store. It performs various actions, including stealing device information, performing ad click fraud, and subscribing the victim to a premium-rate SMS service [621]–[624]. | SMSMalware |
| Roaming-Mantis | Spreads to Android devices using SMS phishing messages. It sends links to the victims that install a fake Google Chrome (Android 9 and below) or fake Google Play application (Android 10 and above). Its main function is to steal SMS messages and personal information from the infected device [625]–[628]. | SMSMalware |
| JioOffers | Targets Android users in India with the Jio network. It infects devices by sending SMS and Whatsapp messages with the app link claiming to offer 25GB. It also uses the contact list of the infected device to spread the malware to contacts with the Jio numbers [442]. | SMSMalware |
| WhatsApp-Message-Sender | Uses the infected device’s Whatsapp to send messages with the APK link to spread to other devices [442]. | SMSMalware |
| Premium-RateSMS | Contains FakePlayer malware [629]. | SMSMalware |
| Mseg | Sends SMS messages to premium rate numbers silently. It steals device information such as phone number and sends it to a remote server [15], [82], [630]. | SMSMalware |
| SendPay | Steals information on the device and sends it to a remote server over the internet. Additionally, it monitors incoming SMS messages and subscribes the victim to a paid mobile service that charges the victim without their consent [631], [632]. | SMSMalware |
| Kmin | Displays a fake prompt message that asks the users for certain permissions to execute malicious activities. It remains active and persistent even if the permissions are rejected. It sends SMS messages to premium-rate numbers, downloads additional applications to the device, and steals and sends user data to a remote server [17], [633] . | SMSMalware |
| SpyBubble | Is a monitoring tool. It embeds and encodes the information gathered in XML format. It collects the user’s GPS location and sends it to a remote server. It collects the victim’s personal information, phone logs, and SMS messages and sends them to the server [199], [634]–[636]. | SMSMalware |

The static-based analysis for the ransomware category involved a systematic approach.

Initially, we performed the decompilation of binary portable APK files to extract the AndroidManifest.xml binary file, which contains crucial metadata and well-defined permissions associated with the Android APKs. We employed APKtool, a widely recognized industry-standard tool [847], for decompilation. This tool enabled us to efficiently deconstruct the zipped Android apps into their respective manifest and SMALI files.

This case study serves as a testament to our unwavering commitment to rigorously evaluate the accuracy and comprehensiveness of our extensive dataset, thereby establishing a solid and dependable foundation for our research. The methodologies employed in this analysis significantly contribute to the field of forensics, enabling a profound understanding of the characteristics and behavior of malware in Android applications.

The static-based analysis leverages a feature set consisting of 389 distinct features, 228 API packages, and 161 permissions. These features are extracted from the manifest and SMALI files of the assembled APKs. The parsing process involves a two-stage approach, wherein each Android APK is scanned separately. Initially, the manifest file of each APK is parsed to quantify specific features, including permissions. Subsequently, in the second stage, the SMALI files of each APK are parsed to determine the usage of API packages. The extracted features are then stored in a database.

Furthermore, we employed pre-processing, preparation, and cleaning mechanisms on the extracted features in the static-based analysis case study context. This step aims to eliminate zero-values or null attributes and represent the features in an appropriate format before feeding them into

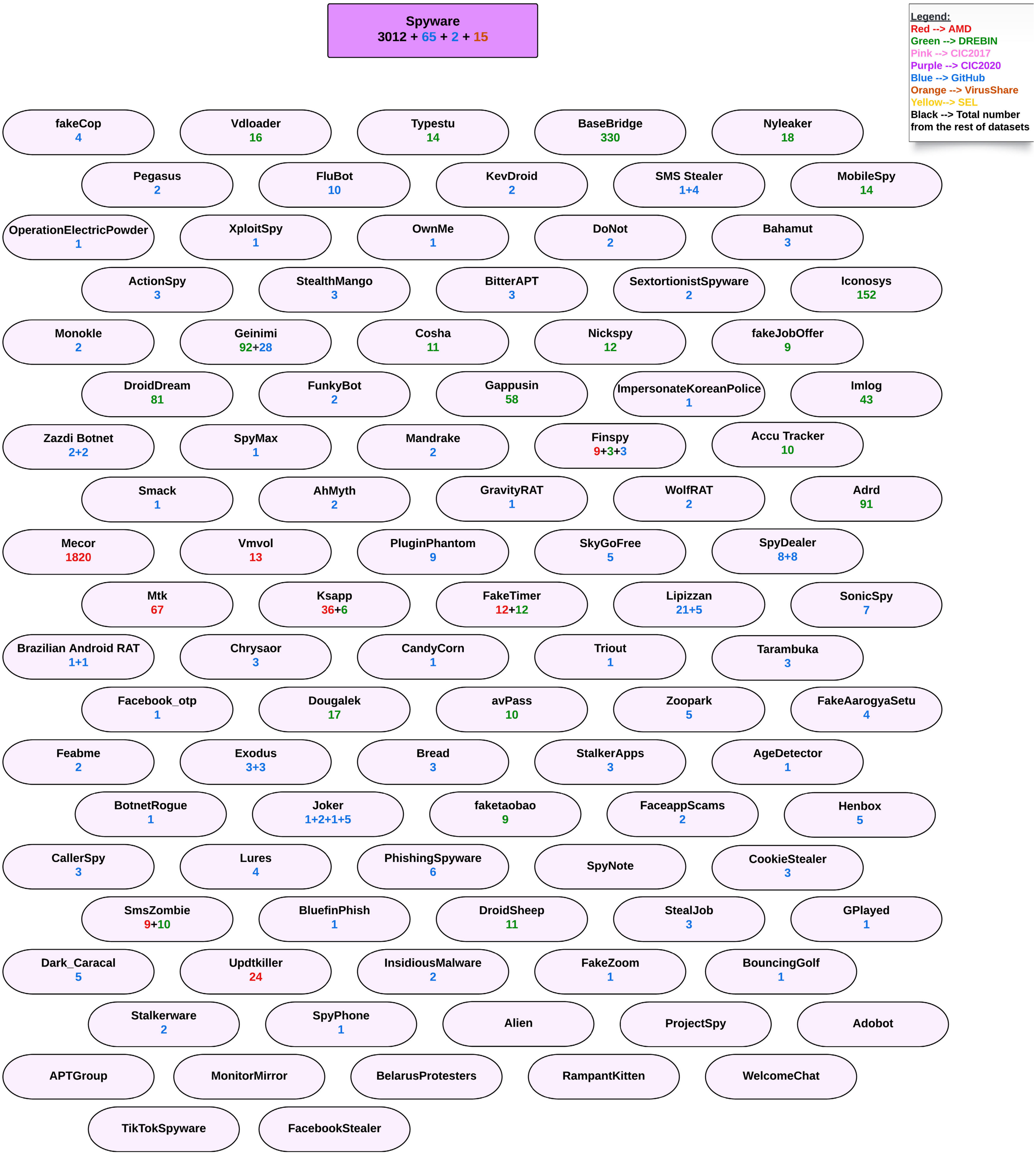


**FIGURE 10.** Spyware Category with its family names and their number of samples.

the machine learning (ML) classifiers being investigated. Specifically, we utilized eight distinct ML models, namely Logistic Regression (LR), Linear Discriminant Analysis (LDA), Naive Bayes (NB), k-nearest neighbor (KNN), Decision Tree (CART), Ada Boost (AB), Random Forest (RF), and Support Vector Machine (SVM) [848], [849].

Subsequently, the ML classifiers were trained and tested using the extracted features from the APK files. Various

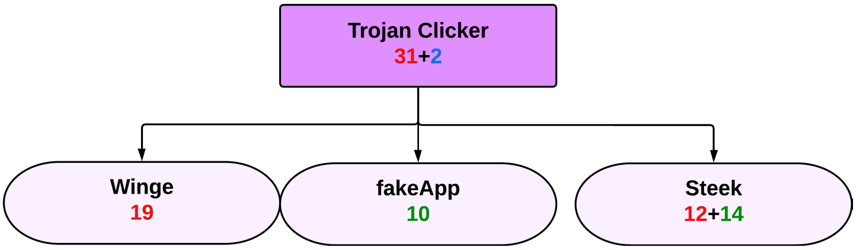


**FIGURE 11.** A sub-group of the Spyware family known as Clicker with the family and number of samples.

evaluation metrics such as accuracy, F1-score, recall, and precision were employed to assess the used classifiers' efficacy. These measures facilitate a comprehensive evaluation of the classifiers' performance in detecting and classifying the analyzed Android APKs. Utilizing multiple evaluation metrics ensures a robust and thorough assessment of the classifiers' abilities to accurately identify potential threats, such as Ransomware, within the APKs.

The dataset is partitioned into separate training and testing subsets to ensure a robust evaluation. Precisely, 80% of the benign and ransomware samples were allocated for training the layers of the ML classifiers. In contrast, the remaining 20% of samples were reserved for testing the performance of the ML classifiers.

The results of the detection analysis, presented in Table 10, reveal that the tested ML models exhibit favorable and satisfactory detection capabilities. This is evident from their high precision, recall, F1-Score, and accuracy values. Notably, the AB model is the most successful among the examined ML classifiers, achieving a high detection accuracy that reached more than 97%. Conversely, the LR model demonstrates relatively lower detection performance when compared to the other ML models.

The results of the detection analysis, presented in Table 10, reveal that the tested ML models exhibit favorable and satisfactory detection capabilities. This is evident from their high precision, recall, F1-Score, and accuracy values. Notably, the AB model is the most successful among the examined ML classifiers, achieving a high detection accuracy that reached more than 97%. Conversely, the LR model demonstrates relatively lower detection performance when compared to the other ML models. The obtained results reaffirm the viability and efficacy of the static-based analysis case study in accurately distinguishing between ransomware and benign APKs. These findings hold significant implications for our comprehensive dataset, as they contribute substantially to enhancing the security and dependability of Android applications.

By effectively identifying potential threats posed by ransomware attacks, our research endeavors to fortify the protection of users and their sensitive data. The successful application of the static-based analysis approach further solidifies the foundation of our dataset, amplifying its potential applications in diverse domains concerning cybersecurity and malware detection.

### C. CASE STUDY III. FEATURES-BASED ANALYSIS

To thoroughly investigate the importance and the impact of our distinguished Maloid dataset, we conducted an additional case study (Case Study III) that focused on specific features extracted from the APK files of Android malware samples. In this case study, we meticulously selected subcategories of malware apps and subjected them to a decompilation process to extract the Android Manifest (AM) files. Subsequently, we transformed these AM features into 2D grayscale images. The malware classes randomly chosen for this case study analysis include Jisut, BankBot, Kuguo, Fusob, Youmi, Mecor, FakeInst, and Dowgin malware families.

The fundamental aim of this case study was to employ both static-based and vision-based approaches to extract one of the primary features of Android malware APKs (AM files) and convert them into visual images. This transformation enabled us to explore the applications of visual detection and classification techniques for these malware samples. By integrating static and vision-based analyses, we sought to gain valuable insights into the distinctive characteristics and behavior of the selected malware classes, contributing to a comprehensive understanding of the Android malware landscape.

The AM files were extracted from the chosen Malware APKs using the APKtool, previously employed in case study II for decompilation. Subsequently, these extracted AM files were converted into images, facilitating their utilization in evaluating the examined CNN models for detection analysis. In this context, we employed the identical set of 22 CNN models previously utilized in the case study I for detection and classification. Furthermore, adhering to the approach established in Case Study I, we maintained consistency in the evaluation process, employing the identical partitioning ratio for malware images into three distinct subsets: testing, validation, and training. This methodology ensures uniformity and comparability in our evaluation procedures, enabling a robust assessment of the Maloid dataset and the examined model's performance across different experiments. The outcomes of this case study concerning the scrutinized evaluation metrics are demonstrated in Table 11.

**TABLE 8.** Spyware Category and its families.

| Family | Description | Category |
|---|---|---|
| BotnetRogue (Dark Shades) | Is a remote access Trojan (RAT). It attempts to gain full control of the device in order to steal sensitive information and perform other various activities [637]. | Spyware |
| Mtk | Steals device information and sends it to a remote server. It is distributed in third-party applications in China. It downloads and installs applications without user interaction. It can also delete applications [15], [638]. | Spyware |
| avPass | Distributes itself as a clock application. In reality, it steals information from the infected device. It also attempts to uninstall or bypass security applications that are installed on the device to avoid detection [639], [640]. | Spyware |
| fakeJobOffer | Disguises Android apps that offer fake jobs prevalent in India. It allows users to submit their CVs but asks for a fee to proceed. It shows a message, “Important incoming email from HR, do the needful”, from HR when the device is booted up. It redirects the user to a fake website with a fake job offer as an image. The victim must pay a fee to secure their offer [641]–[643]. | Spyware |
| faketaoBao | Is an update for a popular Chinese shopping application, Taobao. It works like a real application with a functional shopping feature. It steals the victim’s TaoBao account credentials. It downloads other apps on the victim’s device without their knowledge as they use the malware [644], [645]. | Spyware |
| Mecor | Steals device information, including GPS location and phone number [15], [646]. | Spyware |
| Vmvol | Collects sensitive information and sends it to the attacker. It shows victims a message to download a critical update to trick them into downloading the malware payload [15], [647]. | Spyware |
| Finspy (FinFisher) | Was developed and sold legally by an IT firm. Governments can customize it to use for espionage purposes and steal the victim’s personal information, such as location, messages, recordings, and other data, and send it to a remote server. It infects devices when the user clicks on malicious links in SMS and emails. It gains root privilege by exploiting DirtyCow exploit [648]–[651]. | Spyware |
| SmsZombie | Exploits a vulnerability in the China Mobile SMS Payment System. It piggybacks a wallpaper application in the Chinese android market, GFan. It has affected 500,000 devices in China. It persistently requests permissions to elevate privileges. It collects the victim’s personal information and banking details and sends them to a remote server via SMS message [652]–[656]. | Spyware |
| DroidSheep | Is able to hijack a victim’s session on websites which allows it to perform Man-in-the-Middle attacks [186], [657]. | Spyware |
| Accu Tracker | Is considered a monitoring tool that converts the infected device into a GPS tracker [186], [658]. | Spyware |
| Cosha | Steals personal information from the infected device and sends it to a remote server [186], [659]. | Spyware |
| Nickspy | Steals information from the infected device and sends it to a remote server. It is also able to extract the GPS location of the device and record phone calls from the device [186], [660]–[662]. | Spyware |
| MobileSpy | Is also known as Godwon. It steals personal information from the device and sends it to the attacker. This includes information from social media as well as call logs [14], [186]. | Spyware |
| Typstu | Steals the victim’s personal information found on the device. It then sends the information to a remote server [14], [186]. | Spyware |
| Vdloader | Steals device information, such as the IMEI and IMSI number of the device, and sends it to a remote server [14], [186], [663]. | Spyware |
| Dougalek | Steals the victim’s personal information including the contact list and sends it to a remote server [14], [186], [664]. | Spyware |
| Nyleaker | Steals the victim’s information and SMS messages and sends them to a remote server [665]. | Spyware |
| Facebook-Stealer (FaceStealer) | Hides behind an application that claims to be a photo editor. Once launched, it shows the user the login page for Facebook and asks the user to login to use the application. It steals the victim’s credentials and sends them to a C2C server. The attacker uses the stolen credentials to steal the victim’s personal information and account details [666]–[668]. | Spyware |

**TABLE 8.** ***(Continued.)*** **Spyware Category and its families.**

| | | |
|---|---|---|
| FakeCop | Mainly targets Japanese users. It is found in applications that imitate popular Japanese security solutions. Specifically, the application is an information stealer that steals the victim's personal information, such as contacts, SMS messages, and app lists. It sends this information to a CC server. It also performs various tasks given to it by the server [669]–[672]. | Spyware |
| FluBot | Spreads through links sent by SMS messaging. It steals the victim's personal information and data, such as passwords and online banking details. It was able to spread worldwide, with a high concentration in Spain and Finland. Since it spreads via SMS, it steals the contacts of the infected device and sends the SMS messages to the contacts [673]–[676]. | Spyware |
| Pegasus | Is sold for millions to different governments by the Israeli company, NSO. It infects iOS and Android devices by exploiting zero-day vulnerabilities to perform a zero-clicks attack. It turns the device into a surveillance monitor to spy on the victim. It steals messages from messaging applications and locations, records phone calls, uses the camera and microphone for recording [677]–[681]. | Spyware |
| SMS Stealer | Steals any sent and received SMS messages from the infected device. It then sends it to a remote server. It also sends International Mobile Equipment Identity (IMEI) number and device ID, and operator to the server [682], [683]. | Spyware |
| SpyDealer | Can spread to devices remotely through UDP, TCP, and SMS channels. It steals sensitive information from the device. Specifically, it stealthily steals messages and information from multiple applications such as WhatsApp and Facebook. It is able to root the infected device using rooting exploits to gain full control of the device [684]–[686]. | Spyware |
| Chrysaor | Is a more evolved version of the NSO spyware, Pegasus. It mainly targets Android devices via SMS messages and masquerades as a legitimate application. It gains root privileges using framaroot exploits or using the superuser binary. It then starts monitoring the victim's activities and installs a keylogger. It avoids detection by uninstalling itself [687]–[690]. | Spyware |
| Lipizzan | Is allegedly created by Equus Technologies. It spreads by disguising itself as a legitimate Cleaner and Backup application in the Google Play store. It downloads a malicious component that monitors the device and validates certain abort criteria to gain root privilege. It monitors and steals device information and sends them to the CC server [691]–[694]. | Spyware |
| SonicSpy | Spreads through SMishing and third-party markets. It spreads as a messaging app, Soniac, by injecting malicious code into the open-source code of Telegram. It silently records audio, takes photos, makes outbound calls, sends text messages to specific numbers, and steals information such as Wi-Fi access points. It also attempts to gain control over the infected device [324], [695]–[698]. | Spyware |
| Brazilian Android RAT (BRATA) | Is a remote access trojan that mainly targets users in Brazil. It spreads through messaging applications, compromised websites, and injections in legitimate applications. It is used to mainly spy on its victims through various means, such as keylogging the infected device. It avoids detection by performing a factory reset on the infected device [699]–[702]. | Spyware |
| CandyCorn (PowerOffHijack) | Is able to spy on the victim's infected device even when the device is turned off. It can also control the device and perform multiple tasks, such as recording phone calls, sending text messages, making phone calls, and other activities without the victim's knowledge, even when the device is turned off. It spreads in Chinese application stores [703]–[705]. | Spyware |
| Feabme | Steals the sensitive information on the infected device, including passwords. It sends this stolen information to a remote server. It targets the victim's Facebook credentials. It disguises itself as applications found in the Google Play store called "Cowboy Adventure" and "Jump Chess" [513], [706], [707]. | Spyware |
| Smack | Is based on XMPP Smack Openfire, which is an open-source client connection library. It abuses the API functions of Smack to steal information from the infected device, such as the victim's contact information, short messages, phone records, GPS location, and date. It sends it to a remote server. It hides its icons and intercepts short messages [708]. | Spyware |

**TABLE 8.** *(Continued.)* **Spyware Category and its families.**

| | | |
|---|---|---|
| Dark_caracal | Is a group of hackers who develop malware to steal data and information from Android users. They mainly targeted government institutions, manufacturing companies, and defense contractors. It infected users in around 21 countries via spear phishing emails. The malware, Pallas, disguises itself as secure messaging app. It steals different multimedia files [709]–[711]. | Spyware |
| GPlayed | Disguises itself as the Google Play store named “Google Play Marketplace”. It steals the victim’s information and continues to spy on them. Uniquely, it adapts and changes to the attacker’s desires after deployment by remotely uploading plugins. This adds more functions to it, such as locking the infected device and demanding a ransom from the victim [712]–[715]. | Spyware |
| Henbox | Mainly targets users of the minority group, Uyghur, in China. It disguises itself as multiple legitimate applications in the Google Play Store. It spies on victims and steals information such as their devices and personal information, messages, social media accounts, and content. It is also able to access the device’s microphone, camera, and call logs [716]–[718]. | Spyware |
| KevDroid | Disguises itself as an anti-virus application, Naver Defender. It spreads through phishing emails to scare the targets into downloading the malware on their devices. Its main function is to steal personal and device information, including the victim’s contacts, call log, and text messages [719]–[721]. | Spyware |
| OwnMe | Mainly steals a victim’s personal information. It mainly targets the victim’s WhatsApp application. It steals their chat messages and media files from WhatsApp as well as the victim’s call history and internet browsing history [722]–[725]. | Spyware |
| SkyGoFree | Spreads by disguising itself as a legitimate cell network provider’s website. It claims to update its network and speeds up the service. It gains remote control of the device and spies on the victim. It steals the device’s stored information, text, and WhatsApp messages, connects the device to a compromised Wi-Fi network, and records audio at a specific location [726]–[728]. | Spyware |
| StealthMango (iOS: Tangelo) | Is disguised as applications in third-party markets. It also spreads through physical access to the device. It is supposedly part of an espionage campaign by the Pakistani military. It targeted government and military officials in the Middle East, Afghanistan, and India. It records audio and device screen, steals device information, tracks the device’s location, and more [729]–[732]. | Spyware |
| Tarambuka | Disguises itself as the Google Play store application with the old logo. It prompts the victim to enter their email address to identify the device and begin spying. It moves its files to the System Application directory to avoid removal. It steals the infected device’s information, browser history, and databases of social media apps [733]. | Spyware |
| Triout | Masquerades as legitimate benign applications found in third-party stores. It keeps its source code unobfuscated to act as a framework for editing its capabilities. Its capabilities include stealing information and data, such as messages, calls, videos, pictures, and GPS location, and sending all of them to a remote server [734]–[736]. | Spyware |
| Zoopark | Mainly targets Android users in the Middle East. It disguises itself as a news application popular among Middle Eastern users. It steals the victim’s information, such as messages, calls, multimedia, GPS location, and others, and sends them to a remote server. It also has backdoor capabilities. It targets databases of messaging applications such as Whatsapp and Telegram [737]–[739]. | Spyware |
| Exodus | Disguises itself as legitimate applications found in the Google Play store. It is believed to be developed by the Italian commercial company, eSurv, and sold to the Italian government. It has two components: One acts as a Backdoor, and the other acts as spyware. The second component steals the infected device’s data, records audio, and takes pictures [740]–[742]. | Spyware |
| AhMyth | Is built on top of the foundations of the remote access spyware AhMyth. It disguises itself as a radio music application that functions normally in the Google Play store. In the background, it steals the victim’s personal information and sends it to a remote server [743]. | Spyware |

**TABLE 8.** *(Continued.)* **Spyware Category and its families.**

| | | |
|---|---|---|
| Bouncing-Golf | Is also known as GolfSpy. It is a cyberespionage campaign targeted at Middle Eastern Android users. It disguises itself as legitimate applications hosted on certain websites of the attackers. Its main functionality is stealing the victim's information found on the device. It also executes commands from a remote server [744]. | Spyware |
| CallerSpy | Disguises itself as a messaging app that is hosted on a compromised website. The user can download the app by clicking on the download button. It steals information from the infected device and sends it to a remote server [745]. | Spyware |
| Faceapp-Scams | Describes the scams used by attackers to attract victims by disguising themselves as the popular game, FaceApp. These scams are mainly used to steal the victim's information from the devices [746]. | Spyware |
| Monokle | Spreads by disguising itself as a legitimate application. One of its unique behaviors is its ability to download malicious certificates in the infected device's trusted certificate in order to perform Man-in-the-Middle attacks. It is also able to extract information from the infected device as well as RAT functionality [747]. | Spyware |
| FunkyBot | Disguises itself as a legitimate application and spreads via SMS messaging. It steals device information, including IMEI, IMSI (International Mobile Subscriber Identity), and phone number. It also steals the victim's contact list. It sends this information to a remote server [748], [749]. | Spyware |
| impersonate-Korean-Police | Impersonates the application for the Korean Police Agency. Its main function is to steal the victim's information [750]. | Spyware |
| Joker (Bread) | Is part of the Bread malware family. It disguises itself as a legitimate application in Google Play. It steals information on the victim's device and sends it to a remote server. The data it steals, including SMS messages, contact list, and device information, helps the malware to interact with ads and to subscribe the victim to premium services for financial gain [751]–[754]. | Spyware |
| phishing-Spyware (Whistle-blower Spyware) | Spreads by impersonating a website, specifically, The Guardian's Secure Drop In, where whistleblowers can submit their information. On the compromised website, there is a link to download the malware. Its main function is to steal sensitive data and send it to a remote server [755]. | Spyware |
| stalkerApps | Can be found in monitoring applications in Google Play. It is able to monitor the activities of the victim and others that the victim added. It can also extract information from social media accounts [756]. | Spyware |
| Stalkerware | Disguises itself as an application that can monitor spouses, children, and employees. It steals information from the infected device and sends it to a remote server [757]. | Spyware |
| Covid-AgeDetector | Is spyware that steals the victim's sensitive information according to the VirusTotal report. It uses COVID-19 to trick users into downloading and installing the app [758]. | Spyware |
| Covid_Lures | Is spyware that steals the victim's sensitive information according to the VirusTotal report. It uses COVID-19 to trick users into downloading and installing the app [759]. | Spyware |
| Covid-SpyMax (CovidCom-mercial-Surveillance) | Disguises itself as legitimate applications, including a coronavirus live updates tracker. It spreads via a pharmacy website called "COVIDTZ". It gathers information on the device and records audio and videos to send it to the attacker. It changes system settings and applications' appearance. It was developed by the same group that developed SpyNote [760]–[762]. | Spyware |
| Covid _SpyPhone | Spreads by injecting its malicious code into other benign and legitimate software. Once installed, the attacker can monitor and spy on all the device activities, such as calls, SMS and MMS messaging, and track the physical location of the device [763], [764]. | Spyware |
| FakeZoom | Disguises itself as the popular video-calling application, Zoom. It displays the zoom login page where the malware steals the login credentials of the victim's account. Additionally, it is able to display ads to the victim [765]–[767]. | Spyware |
| XploitSpy | Is a spying tool for Android devices developed by a cyber security company in India. It uses the PaaS, Heroku, as a control panel to perform various monitoring and spyware activities [768], [769]. | Spyware |

TABLE 8. *(Continued.)* Spyware Category and its families.

| | | |
|---|---|---|
| ActionSpy | Was developed by the threat group Earth Empusa to monitor targeted groups in Tibet, Turkey, and Taiwan. It spreads through fake website pages and compromised news websites. It is capable of collecting information from the infected device. It also monitors messaging applications and collects chat logs from them [770]–[772]. | Spyware |
| DoNot | Is a Hacker Organization with malware that mostly concentrates on espionage and developing spyware [773]. | Spyware |
| Bahamut | Is a Hacker group that develops mostly spyware. They target Middle Eastern and South Asian countries. One of their spyware includes a phishing website and application called Jamaat that poses as a religious application. In reality, it steals information found on the device [774], [775]. | Spyware |
| BitterAPT | Spreads by masquerading as legitimate applications in Google Play. The Advanced Persistent Threat group developed it, which targeted users in Pakistan and other countries. It is mainly an espionage tool that has RAT capabilities and takes instructions from remote servers [776]. | Spyware |
| sextortionist-Spyware (Goontact) | Mainly targets users in Chinese-speaking countries, Japan, and Korea. Additionally, it targets users who visit adult websites that provide escort services and applications. Once the victim downloads the application, it steals the victim's sensitive information in order to blackmail them. This is known as sextortionism [777]–[779]. | Spyware |
| fakeAarogya-Setu | Injects itself into the Indian government's corona tracker application, Aarogya Setu. The victim installs the legitimate application while it simultaneously performs malicious activities in the background. It behaves similarly to SpyNote. It is able to record audio, take videos and pictures, steal SMS messages, and other actions [780], [781]. | Spyware |
| GravityRAT | Is a RAT espionage tool that disguises itself as a legitimate application. It mostly targets users in India. Its main function is to steal information and data from the infected device, which includes taking screenshots and recording audio and video. It then sends the stolen information to the remote server [782]–[785]. | Spyware |
| Insidious-Malware | Is called Banbra from VirusTotal scan. This malware's main functionality is to steal the device and personal information from the device it infected [786], [787]. | Spyware |
| WelcomChat | Contains BadPatch malware. It disguises itself as the Welcome Chat application that claims to be secure. In reality, it is a cyber-espionage campaign that targets Middle Eastern Android users. It provides the chatting functionality it promised. However, it spies on the chat communication. It steals SMS messages and records video, phone calls, and audio [788], [789]. | Spyware |
| Mandrake | Attempts to remain undetected by targeting specific devices and locations. It allows the attacker to gain complete control over the infected device. Its main function, however, is to spy on and steal the infected device's information [790]–[792]. | Spyware |
| CookieStealer (CookieThief) | Gains root access to the infected device. From there, the malware steals the cookies used by the device's browsers and Facebook app and sends them to the attacker. This allows the attacker to steal the login credentials of the victim and impersonate the victim themselves [793]–[795]. | Spyware |
| SpyNote | Mainly steals the victim's personal information and the device's information. It can access the microphone and camera of the infected device to record audio and video for spying purposes. It is considered a RAT since it can remotely infect devices and perform actions remotely [796]–[798]. | Spyware |
| Monitor-Mirror | Disguises itself as a parent monitoring tool. It can steal confidential and sensitive information from the infected device. Its other capabilities include allowing the attacker to remotely control the device and record audio and video [799], [800]. | Spyware |
| ProjectSpy | Disguises itself as a Coronavirus Update application to trick users. It mainly acts as spyware. Specifically, the malware steals information from the device and sends it to the user. Additionally, it is capable of stealing messages from messaging applications and saving them in a database [801]–[803]. | Spyware |

**TABLE 8.** ***(Continued.)*** **Spyware Category and its families.**

| | | |
|---|---|---|
| Adobot | Disguises itself as an application for the Saudi Health Council that tracks Coronavirus updates. It is considered an open-source malware with spyware capabilities. It is distributed by attackers impersonating Saudi Twitter accounts. Their modus operandi is tweeting breaking news from the health council with a malicious link to download the malware [442]. | Spyware |
| Alien | Is offered and sold to underground hacking forums as a MaaS. It can collect the victim's personal and device information and sends it to the attacker. It performs overlay attacks on multiple applications, including banking, to steal the victim's login credentials. It can load the spyware, Predator onto the infected device [804]–[806]. | Spyware |
| APTGroup | Is developed by the APT group known as StrongPity. The malware was distributed via a Syrian e-Gov website. Specifically, this malware replaced the government's official application with a version injected with the malware. Its main function is to steal contacts and files with specific extensions from the infected device [807], [808]. | Spyware |
| belarus-Protesters | Masquerades as anti-government news applications that, in reality, spy on Belarusian protesters and collect sensitive information on them. Specifically, it collected the victim's personal details and physical location [809], [810]. | Spyware |
| Rampant-Kitten | Is a hacking group that develops malware that spies on political opponents in Iran. They are focusing on malware that steals multi-factor authentication codes of multiple popular applications. It can steal the victim's login credentials and intercept the SMS message with the codes. It steals the victim's information stored on the infected device [811]–[813]. | Spyware |
| TikTok-Spyware | Disguises itself as a pro version of TikTok called TikTok Pro. In reality, users are downloading premium spyware that steals the victim's information stored in the infected device and FaceBook credentials. When the victim opens the applications, a fake notification is shown then the malware hides its icon [814]. | Spyware |
| WolfRAT | Is an espionage campaign that targets messaging applications such as WhatsApp and FaceBook Messengers. It is developed by the German organization Wolf Research crew for governments. Its main capability is stealing the victim's photos, videos, and audio files [815]–[817]. | Spyware |
| Ksapp | Steals sensitive information and sends them to a remote server. It disguises itself as the "Flow Free" application. It downloads and installs application package files. It is used as a botnet to launch a DDOS attack from Android devices. It is an interpreter with Lexer and Parser [15], [818], [819]. | Spyware |
| UpdtKiller | Convinces victims that they are providing security services. It connects to a C&C server to execute commands. It steals user information and sends it to the server. It avoids detection by killing anti-virus processes. It adds fake SMS messages to inbox and intercepts, replies, and blocks messages without the user's consent [15], [606], [820]. | Spyware |
| BaseBridge | Steals sensitive information and sends it to a remote server through SMS messaging. It is activated once the victim upgrades the malware and restarts the device. Additionally, the infected application may terminate other applications once it is upgraded [17], [583], [821]–[823]. | Spyware |
| Iconosys | Spoofs a registration page for the infected application the victim downloaded. It steals the information that the victim submits and may leak them to other recipients [824]–[826]. | Spyware |
| Geinimi | Steals device information and sends it to a remote server. It also executes remote commands from the server on the infected device, such as sending SMS messages and making phone calls [17], [827]–[829]. | Spyware |
| DroidDream | Got its name because it executes between 11 pm and 8 am when most victims are likely to sleep and use their phones less. It is considered a botnet that steals information from the infected device and sends it to a remote server. It also downloads suspicious applications to the device [17], [830]–[833]. | Spyware |
| Gappusin | Steals sensitive information on the device and sends it to a remote server. It also downloads suspicious applications [17], [834], [835]. | Spyware |

**TABLE 8.** *(Continued.)* Spyware Category and its families.

| | | |
|---|---|---|
| Imlog | Is distributed as a wallpaper application. It steals user information and sends it to a remote server [836], [837]. | Spyware |
| FakeTimer | Opens websites with adult content on the page when executed. It steals device information and sends it to remote server [82], [838], [839]. | Spyware |
| Zazdi Botnet | Is part of an information-stealing botnet network. It communicates with the bots and executes commands using Firebase Cloud Messaging (FCM). It infects devices through website links on a Facebook page. This link directs the victim to the application download link [840]. | Spyware |
| Winge | Activates during certain event calls (BOOT, GPS, TIME, SYS). It steals personal and device information and sends them to a remote server. It sends SMS to premium rate numbers and executes any commands sent from the server. It redirects the infected device to one of the URLs saved in the server [15], [841]. | Spyware (Trojan Clicker) |
| fakeApp | Masquerades as legitimate antivirus software. It sends SMS messages and makes calls to premium-rate numbers that the attacker controls. It also displays advertisements to the users and redirects them to malicious websites as well as directs them to install other applications when they click on the ads [842], [843]. | Spyware (Trojan Clicker) |
| Steek | Disguises itself as legitimate popular games. Once the victim downloads the game, it prompts them to enter their private information to complete the installation. It sends SMS messages and redirects users to websites advertising fake money schemes and lottery tickets [15], [82], [844], [845]. | Spyware (Trojan Clicker) |
| Facebook_otp | Is a spy trojan according to the VirusTotal reports and results [846]. | Spyware |
| Plugin-Phantom | Avoids static analysis detection by abusing the Android plug-in framework, DroidPlugin, to launch plugins without installing them. It steals files and information from the device, takes photos and screenshots, records videos, and logs keystrokes. It is divided into the host application and the malicious plugins. The nine plugins the malware abuses are Online, Task, Update, File, Location, Contact, Camera, Radio, and WIFI [324]–[851]. | Spyware |
| StealJob | Is developed and spread by the hacker group DoNot. It mainly targets users in Pakistan. It disguises itself as the Pakistani news application, KashmirVoice. Its main function is to steal sensitive information from the device [852]. | Spyware |
| bluefinPhish | Disguises itself as the BlueWin application. It steals the victim's email credentials and sends them to a remote server [853]. | Spyware |
| Adrd | Is bundled with legitimate Android applications. It changes the mobile device settings, steals device information and sends it to a remote server, and downloads other packages on the infected device [17], [854], [855]. | Spyware |
| Operation-Electric-Powder | Got its name from its role in the attack against the Israel Electric Company (IEC). This operation targets multiple domains, including malware targeting Android devices. It disguises itself as the legitimate application, Pokemon GO (pokemon.apk). This package impersonates IEC in some characteristics. Once installed, it installs the spyware on the device [324], [856]. | Spyware |

The analysis of the obtained results in Table 11 substantiates that the scratch CNN algorithm outperforms the other tested CNN algorithms regarding the lowest detection loss and the highest detection accuracy. Moreover, it is noteworthy that all examined CNN models have demonstrated favorable and satisfactory detection capabilities. These capabilities are evident from the high values of precision, recall, F1-Score, and accuracy achieved by each of the CNN classifiers. The robust performance of all CNN models underscores their efficacy in accurately detecting and classifying the malware families in our Maloid dataset, presenting promising implications for their practical applications in malware forensics.

The above three case studies are just examples. There is an unlimited number of scenarios where the Maloid dataset could be effectively utilized by all types of existing analysis systems that might consider all malware categories in their analysis, or only the families of one category, or even specific features of one malware family. Consequently, the result is achieving one main goal of preventing and predicting threatening malware before causing any harm to individuals and organizations.

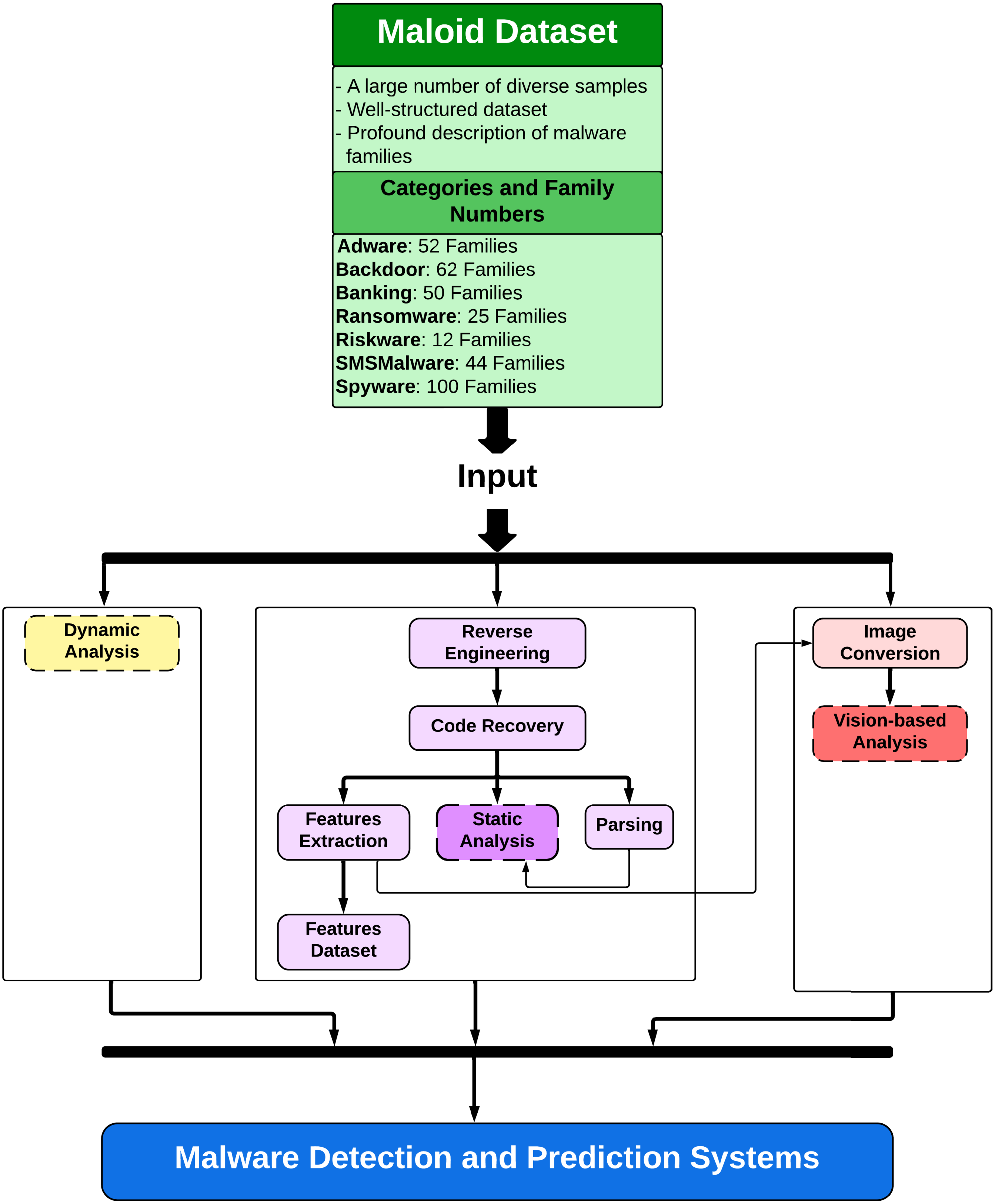


**FIGURE 12.** Maloid dataset utilization overview.

**TABLE 9.** Performance analysis of case study I.

| | | Metric | | | |
|---|---|---|---|---|---|
| **Model** | **Format** | **Accuracy(%)** | **F1-Score(%)** | **Precision(%)** | **Recall(%)** |
| **Scratch** | Color | 84.96 | 84.92 | 85.17 | 84.96 |
| | Gray | 84.83 | 84.83 | 85.13 | 84.83 |
| **VGG16** | Color | 78.02 | 77.92 | 78.65 | 78.02 |
| | Gray | 78.72 | 78.63 | 79.59 | 78.72 |
| **ResNet50** | Color | 80.5 | 80.42 | 80.94 | 80.5 |
| | Gray | 80.2 | 80.23 | 80.72 | 80.2 |
| **VGG19** | Color | 77.89 | 77.7 | 78.37 | 77.89 |
| | Gray | 78.85 | 78.75 | 79.05 | 78.85 |
| **DenseNet121** | Color | 77.33 | 77.33 | 78.0 | 77.33 |
| | Gray | 75.96 | 76.06 | 76.73 | 75.96 |
| **DenseNet169** | Color | 74.91 | 75.13 | 75.77 | 74.91 |
| | Gray | 76.47 | 75.97 | 78.01 | 76.47 |
| **DenseNet201** | Color | 77.06 | 76.89 | 77.0 | 77.06 |
| | Gray | 77.91 | 77.71 | 78.45 | 77.91 |
| **EfficientNetB0** | Color | 79.82 | 79.74 | 80.47 | 79.82 |
| | Gray | 79.89 | 79.92 | 80.74 | 79.89 |
| **EfficientNetB1** | Color | 80.34 | 80.17 | 80.79 | 80.34 |
| | Gray | 80.69 | 80.64 | 81.52 | 80.69 |
| **EfficientNetB2** | Color | 79.95 | 79.95 | 80.34 | 79.95 |
| | Gray | 80.25 | 80.44 | 81.33 | 80.25 |
| **EfficientNetB3** | Color | 80.27 | 80.09 | 80.98 | 80.27 |
| | Gray | 80.79 | 80.68 | 81.6 | 80.79 |
| **EfficientNetB4** | Color | 81.05 | 80.89 | 81.59 | 81.05 |
| | Gray | 80.85 | 80.78 | 81.43 | 80.85 |
| **EfficientNetB5** | Color | 79.98 | 79.88 | 80.71 | 79.98 |
| | Gray | 80.34 | 80.39 | 81.21 | 80.34 |
| **EfficientNetB6** | Color | 79.4 | 79.59 | 80.13 | 79.4 |
| | Gray | 78.21 | 78.58 | 79.34 | 78.21 |
| **EfficientNetB7** | Color | 80.09 | 79.94 | 80.29 | 80.09 |
| | Gray | 78.94 | 78.78 | 79.73 | 78.94 |
| **InceptionResNetV2** | Color | 45.83 | 36.71 | 36.49 | 45.83 |
| | Gray | 41.15 | 28.54 | 40.17 | 41.15 |
| **InceptionV3** | Color | 67.7 | 67.09 | 69.44 | 67.7 |
| | Gray | 69.23 | 68.62 | 72.52 | 69.23 |
| **MobileNet** | Color | 68.6 | 67.89 | 69.57 | 68.6 |
| | Gray | 73.11 | 72.61 | 74.35 | 73.11 |
| **MobileNetV2** | Color | 68.73 | 68.14 | 69.77 | 68.73 |
| | Gray | 72.66 | 71.97 | 73.5 | 72.66 |
| **MobileNetV3Large** | Color | 79.46 | 79.45 | 80.05 | 79.46 |
| | Gray | 78.63 | 78.6 | 79.18 | 78.63 |
| **MobileNetV3Small** | Color | 78.05 | 78.0 | 78.68 | 78.05 |
| | Gray | 77.24 | 77.04 | 78.01 | 77.24 |
| **Xception** | Color | 70.14 | 69.65 | 71.1 | 70.14 |
| | Gray | 72.03 | 71.68 | 73.61 | 72.03 |

### D. CASE STUDY IV. EDUCATIONAL RESOURCES AND TRAINING OPPORTUNITIES

Maloid offers a rich resource of malware samples from different categories and families, which academics can use heavily in teaching malware analysis courses at the undergraduate and postgraduate levels. Additionally, trainers who organize professional training and workshops in malware analysis can use Maloid samples to conduct a training series for different purposes while utilizing various analysis models.

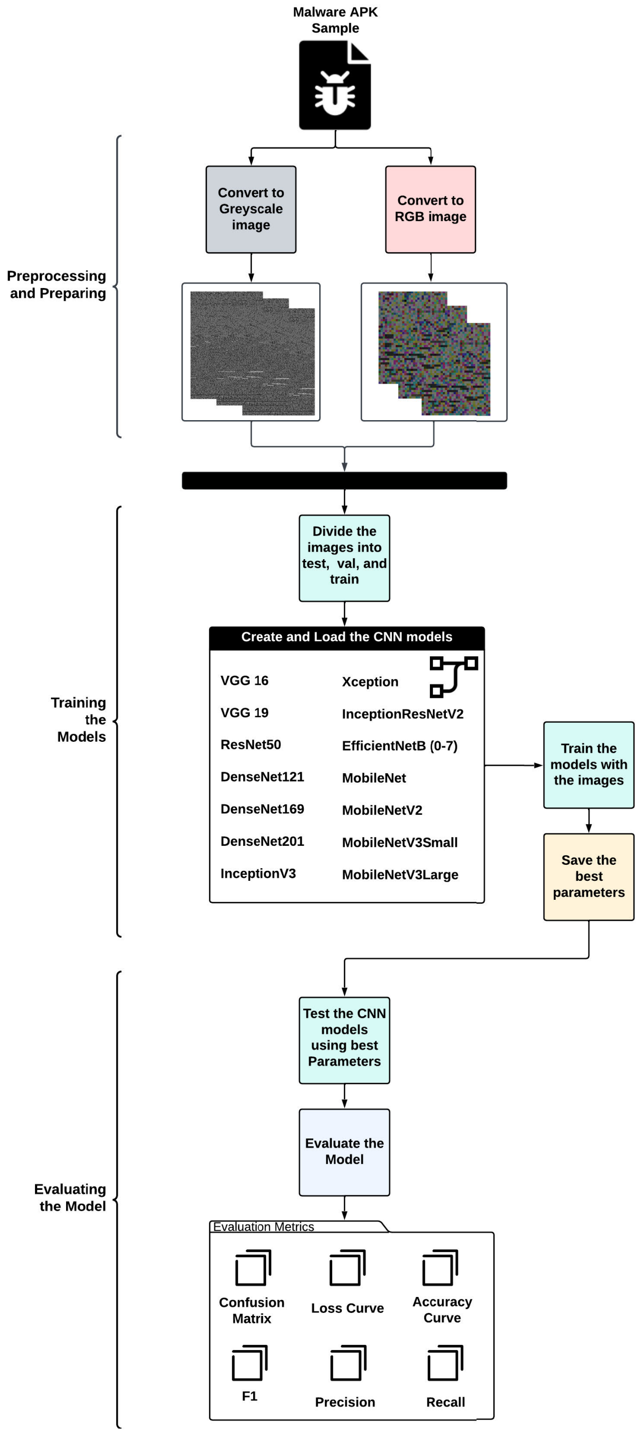


**FIGURE 13.** Steps of the conducting case study I (vision-based analysis).

## VI. LIMITATIONS AND CHALLENGES OF THE MALOID DATASET

While the Maloid dataset represents a significant step forward in the resources available for Android malware analysis, it has limitations and faces several challenges in its development and utilization. Below, we outline some of these limitations and challenges.

**TABLE 10.** Evaluation metrics for ML classifiers used in case study II.

| Classifier | F1-score | Precision | Recall | Accuracy |
|---|---|---|---|---|
| LR | 0.8401 | 0.8401 | 0.8401 | 0.8401 |
| LDA | 0.9021 | 0.9021 | 0.9021 | 0.9021 |
| NB | 0.8891 | 0.8893 | 0.8891 | 0.8891 |
| KNN | 0.9304 | 0.9304 | 0.9291 | 0.9304 |
| CART | 0.9413 | 0.9413 | 0.9413 | 0.9413 |
| AB | 0.9702 | 0.9702 | 0.9702 | 0.9702 |
| RF | 0.9442 | 0.9451 | 0.9451 | 0.9451 |
| SVM | 0.9246 | 0.9246 | 0.9246 | 0.9246 |

### A. LIMITATIONS

- **Android Specific:** Building a comprehensive dataset for OS-specific malware requires a deep specialty and much effort and time. This research focuses on Android OS and will consider other types of OS in future studies.
- **Coverage Gaps:** Despite our efforts to compile a comprehensive dataset, coverage gaps may exist due to the ever-evolving nature of malware. Certain emerging malware types or variants may be underrepresented as the landscape of threats expands.
- **Sample Collection Bias:** The dataset's composition is influenced by the availability of malware samples and the sources from which they are collected. This may introduce a bias toward more readily available or well-known malware families, which may affect the dataset's diversity.

### B. CHALLENGES

- **Sourcing Diverse Samples:** Continuously sourcing a diverse range of malware samples poses a logistical challenge, requiring extensive collaboration with security communities, researchers, and industry practitioners.
- **Maintaining Dataset Integrity:** Ensuring the accuracy and integrity of dataset entries as they scale, especially with community contributions, demands rigorous validation processes, which can be resource-intensive.
- **Adapting to Technological Advances:** The rapid pace of technological advancement in malware development and cybersecurity measures necessitates ongoing updates to the dataset. This process requires sustained effort and resources to maintain relevance.
- **Ethical and Legal Considerations:** Collecting and distributing malware samples should be executed carefully to adhere to ethical guidelines and legal restrictions, presenting a complex regulatory landscape.

Recognizing these limitations and challenges, our future work will focus on addressing these areas through targeted efforts aimed at expanding the dataset's coverage, enhancing its diversity, and refining its structure to better capture malware dynamics. We will explore innovative methodologies for sample collection and validation, advancements in malware analysis technologies, and engagement in active

**TABLE 11.** Performance analysis of case study III.

| | Metric | | | |
|---|---|---|---|---|
| **Model** | **Accuracy (%)** | **F1-Score (%)** | **Precision (%)** | **Recall (%)** |
| **Scratch** | 97.49 | 97.48 | 97.51 | 97.49 |
| **VGG16** | 91.02 | 90.93 | 91.14 | 91.02 |
| **ResNet50** | 93.77 | 93.61 | 93.77 | 93.77 |
| **VGG19** | 90.21 | 90.12 | 90.14 | 90.21 |
| **DenseNet121** | 91.59 | 91.4 | 91.37 | 91.59 |
| **DenseNet169** | 90.53 | 90.27 | 90.25 | 90.53 |
| **DenseNet201** | 90.78 | 90.6 | 90.58 | 90.78 |
| **EfficientNetB0** | 87.86 | 86.74 | 88.24 | 87.86 |
| **EfficientNetB1** | 89.16 | 88.51 | 88.97 | 89.16 |
| **EfficientNetB2** | 91.1 | 90.7 | 90.88 | 91.1 |
| **EfficientNetB3** | 91.83 | 91.61 | 91.64 | 91.83 |
| **EfficientNetB4** | 91.02 | 90.62 | 90.75 | 91.02 |
| **EfficientNetB5** | 90.13 | 89.89 | 89.94 | 90.13 |
| **EfficientNetB6** | 91.18 | 91.22 | 91.33 | 91.18 |
| **EfficientNetB7** | 91.75 | 91.46 | 91.67 | 91.75 |
| **InceptionResNetV2** | 47.09 | 40.7 | 50.22 | 47.09 |
| **InceptionV3** | 89.08 | 88.59 | 88.55 | 89.08 |
| **MobileNet** | 88.92 | 88.17 | 88.71 | 88.92 |
| **MobileNetV2** | 89.16 | 88.81 | 88.78 | 89.16 |
| **MobileNetV3Large** | 92.72 | 92.44 | 92.74 | 92.72 |
| **MobileNetV3Small** | 91.67 | 91.61 | 91.59 | 91.67 |
| **Xception** | 90.29 | 90.04 | 89.95 | 90.29 |

dialogue with the cybersecurity community to overcome these challenges. Through these efforts, we aim to evolve the Maloid dataset continually, ensuring it remains a valuable and relevant resource for the fight against malware.

## VII. HOW TO UPDATE THE MALOID DATASET

Due to Android malware's dynamic nature and ever-changing landscape, it is essential to introduce a detailed plan and strategy for keeping the Maloid dataset comprehensive and up-to-date. Thus, recognizing the critical need for having dynamic datasets in cybersecurity research, our update methodology is designed to incorporate new malware samples systematically, ensuring Maloid-DS remains an invaluable asset for current and future malware detection and analysis efforts. The update strategy is articulated through several core components:

- **Automated Collection Mechanisms:** Developing and running automated scripts at scheduled intervals to scrape new malware samples from a pre-defined list of reputable and authoritative sources in the cybersecurity domain, including cybersecurity databases, malware repositories, and submissions to platforms like VirusTotal by security researchers, ensuring a continuous and timely addition of new samples to the dataset.
- **Community Contributions and Crowd-Sourcing:** Leveraging the collective knowledge and resources of the cybersecurity research community by inviting researchers, practitioners, and enthusiasts to contribute new malware samples, with a stringent validation process before inclusion.
- **Periodic Expert Review and Validation:** Implementing a regular review process conducted by a panel of

experts to examine the dataset's composition, integrate new malware families, and adjust the categorization schema to reflect emerging trends.
- **Feedback Loop for Continuous Improvement:** Establishing a feedback mechanism for users to report discrepancies, suggest improvements and contribute to the dataset's evolution, ensuring its ongoing quality, relevance, and effectiveness.

By adopting this comprehensive and multifaceted updating approach, we ensure the Maloid dataset's leading role in Android malware studies. This strategy keeps the dataset relevant and adaptable and solidifies its role as a pivotal resource within the cybersecurity domain.

Furthermore, to address the dynamic nature of malware and the invaluable role of community contributions in enhancing the Maloid dataset, we outline a structured mechanism for facilitating community feedback, corrections, and new sample submissions:

- **Online Contribution Portal:** Create a dedicated online portal that serves as the central platform for community contributions. This portal will be designed with a focus on user security and ease of use, ensuring that researchers and practitioners can easily submit their contributions.
- **Submission Process:** The portal will allow for the submission of new malware samples, feedback on existing dataset entries, and suggestions for corrections or enhancements. Submissions can include a variety of formats, such as binary files, feature sets, and annotations.
- **Verification Process:** Each submission will undergo a rigorous verification process. This includes automated checks for relevance and integrity, followed by expert review. The process ensures that all contributions meet our standards for accuracy and relevance.
- **Integration into the Dataset:** Contributions that pass the verification process will be integrated into the Maloid dataset. For new malware samples, this includes categorization and annotation based on our dataset schema. For feedback and corrections, appropriate adjustments will be made to ensure the dataset's ongoing accuracy and comprehensiveness.
- **Acknowledgment and Recognition:** Contributors whose submissions are integrated into the dataset will receive acknowledgment through our portal. This recognition aims to encourage ongoing community participation and highlight the collaborative effort behind the dataset's development.
- **Continuous Improvement Cycle:** The mechanism is designed to be a continuous cycle of contribution, review, and integration, allowing the dataset to evolve in response to new threats and community insights. This cycle ensures that the Maloid dataset remains a relevant and valuable resource for malware research.

Implementing this community engagement mechanism will improve the Maloid dataset and foster a collaborative ecosystem for advancing malware analysis.

## VIII. CONCLUSION AND FUTURE WORK

The Android operating system is very popular with smartphone users worldwide, especially with its customization feature. However, a consequence of this popularity is that Android users are more likely to be targeted by attackers. One of these attacks includes infecting the Android device with malicious software. Although many existing ways try to protect from these attacks, the continued increase in the number of Android malware and their impact is a clear sign of the inefficiency of the current solutions. Many of these solutions depend on collected datasets that we believe have many shortcomings.

Therefore, this paper introduced a unique, labeled, up-to-date dataset called Maloid-DS (Malicious Android DataSet) that succeeded in tackling the lack of existing datasets used by current malware detection solutions. The uniqueness of this dataset is due to the (1) comprehensiveness of malware categories and families that reached 345 different families, (2) the well-structuring of these malware families, (3) accurate mapping of large malware samples with their corresponding families, (4) precise and profound descriptions of all these malware families, and (5) expose the source of all collected malware samples. All these distinguished characteristics are found in one reference, Maloid-DS.

This paper began by providing a comprehensive review of related work. We reviewed previous work that developed their datasets or provided an analysis of malware families. We focused on the number of samples and families the papers used and the diversity of the dataset sources. Additionally, we analyzed papers that developed malware analysis tools based on datasets. Moreover, we summarized all the analyses and comparisons in a tabular format.

After that, we started detailing our own developed dataset. First, we specified the process we followed to create the Maloid dataset and the classification we used to categorize the families. Then, we described the categories that we devised when creating the dataset. Moreover, we described in detail each malware family's attack behavior and characteristics in the seven categories. Finally, after detailing the dataset, we provided three case studies as examples to guide how researchers and developers can utilize Maloid dataset.

In summary, this paper produced a comprehensive dataset containing many families and a high number of up-to-date samples. We classified these families into different categories based on their behavior. Furthermore, we provided a detailed and specific description of the families we collected. As a result, these findings and the dataset created will be shared with the research, academic, and industrial communities.

In our pursuit of advancing the Maloid dataset, we are introducing an ambitious plan to extend its scope and enhance its utility for the cybersecurity research community. The expansion strategy of the dataset considers (a) increasing the number of samples, especially for the malware families with fewer samples than others. (b) moving beyond our Android-centric focus to incorporate essential platforms such as Windows, Linux, and iOS. This initiative offers a comprehensive, diverse, cross-platform resource for contemporary cybersecurity threats, facilitating a more holistic malware analysis approach. To ensure the dataset remains timely and representative of the dynamic threat landscape, we will adopt a structured methodology for continuously integrating new malware variants, supported by automated collection mechanisms and invaluable contributions from the broader cybersecurity community. Collaboration will be a cornerstone in this strategy as we seek to establish partnerships with entities across academia, research, and industry.

However, we acknowledge that realizing these ambitious goals is challenging. Key among these is the feasibility of extending the dataset across multiple operating systems, which necessitates overcoming technical, logistical, and legal hurdles. For instance, collecting and integrating malware samples from platforms like iOS needs to address privacy policies and security measures. Additionally, continuously updating the dataset to include new malware variants requires significant computational resources and ongoing community engagement to ensure a steady flow of relevant and diverse contributions. Resource constraints also present a potential roadblock, particularly regarding the funding needed to support the expansion efforts, develop new dataset formats, and maintain a high-quality, up-to-date resource. Moreover, fostering productive collaborations and partnerships demands effective coordination and alignment of goals among diverse stakeholders in the cybersecurity ecosystem.

We are committed to finding innovative and practical solutions to address these challenges by utilizing existing relationships within the cybersecurity community, exploring funding opportunities to support dataset development and expansion, and adopting flexible, scalable approaches to dataset management and update processes. We also plan to dialogue with platform providers and regulatory bodies to address legal and policy-related considerations, ensuring our dataset expansion efforts comply with all relevant standards and regulations. Through acknowledging and planning for these potential challenges, we aim to ensure that our efforts to enhance and expand the Maloid dataset are both realistic and sustainable. By doing so, we hope the Maloid dataset becomes an indispensable tool for cybersecurity research, contributing significantly to advancing malware detection and analysis methodologies and bolstering global cybersecurity defenses.

## ACKNOWLEDGMENT

The authors would like to thank the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

## REFERENCES

[1] Kaspersky. (Jan. 2021). *Can You Get Viruses on Android? Every Android User is At Risk*. [Online]. Available: https://www.kaspersky.com/resource-center/preemptive-safety/android-malware-risk

[2] CTIC Team. (2023). *Top 10 Malware Q1 2023*. [Online]. Available: https://www.cisecurity.org/insights/blog/top-10-malware-q1-2023

[3] CYBERGRX. (2020). *Cyber Threats on the Rise Due to COVID-19*. [Online]. Available: https://www.cybergrx.com/resources/research-and-insights/blog/cyber-threats-on-the-rise-due-to-covid-19

[4] R. Kumar, M. Alenezi, M. Ansari, B. Gupta, A. Agrawal, and R. Khan, "Evaluating the impact of malware analysis techniques for securing web applications through a decision-making framework under fuzzy environment," *Int. J. Intell. Eng. Syst.*, vol. 13, no. 6, pp. 94–109, Dec. 2020.

[5] S. Ullah, W. Boulila, A. Koubaa, and J. Ahmad, "MAGRU-IDS: A multi-head attention-based gated recurrent unit for intrusion detection in IIoT networks," *IEEE Access*, vol. 11, pp. 114590–114601, 2023.

[6] S. Ullah, J. Ahmad, M. A. Khan, M. S. Alshehri, W. Boulila, A. Koubaa, S. U. Jan, and M. M. Iqbal Ch, "TNN-IDS: Transformer neural network-based intrusion detection system for MQTT-enabled IoT networks," *Comput. Netw.*, vol. 237, Dec. 2023, Art. no. 110072. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128623005170

[7] A. Rahali, A. H. Lashkari, G. Kaur, L. Taheri, F. Gagnon, and F. Massicotte, "DIDroid: Android malware classification and characterization using deep image learning," in *Proc. 10th Int. Conf. Commun. Netw. Secur.* New York, NY, USA: Association for Computing Machinery, Nov. 2020, pp. 70–82, doi: 10.1145/3442520.3442522.

[8] S. Lee, W. Jung, W. Lee, H. G. Oh, and E. T. Kim, "Android malware dataset construction methodology to minimize bias-variance tradeoff," *ICT Exp.*, vol. 8, no. 3, pp. 444–462, Sep. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959521001351

[9] H. Fereidooni, V. Moonsamy, M. Conti, and L. Batina, "Efficient classification of Android malware in the wild using robust static features," in *Proc. Mobile Netw. Devices*, 2016, pp. 195–222.

[10] O. Mirzaei, "Techniques for advanced Android malware triage," Ph.D. dissertation, Dept. Comput. Sci. Eng., Universidad Carlos III de Madrid, Madrid, Spain, Feb. 2019.

[11] K. A. Kumar, A. Raman, C. Gupta, and R. R. Pillai, "The recent trends in malware evolution, detection and analysis for Android devices," *J. Eng. Sci. Technol. Rev.*, vol. 13, no. 4, pp. 240–248, Aug. 2020.

[12] M. Ashawa and S. Morris, "Analysis of mobile malware: A systematic review of evolution and infection strategies," *J. Inf. Secur. Cybercrimes Res.*, vol. 4, no. 2, pp. 103–131, Dec. 2021.

[13] F. Alswaina and K. Elleithy, "Android malware family classification and analysis: Current status and future directions," *Electronics*, vol. 9, no. 6, p. 942, Jun. 2020. [Online]. Available: https://www.mdpi.com/2079-9292/9/6/942

[14] A. Saracino, D. Sgandurra, G. Dini, and F. Martinelli, "MADAM: Effective and efficient behavior-based Android malware detection and prevention," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 1, pp. 83–97, Jan. 2018.

[15] F. Wei, Y. Li, S. Roy, X. Ou, and W. Zhou, "Deep ground truth analysis of current Android malware," in *Proc. Int. Conf. Detection Intrusions Malware, Vulnerability Assessment*. Bonn, Germany: Springer, 2017, pp. 252–276.

[16] S. Suresh, F. Di Troia, K. Potika, and M. Stamp, "An analysis of Android adware," *J. Comput. Virol. Hacking Techn.*, vol. 15, no. 3, pp. 147–160, Sep. 2019.

[17] B. Wu, S. Chen, C. Gao, L. Fan, Y. Liu, W. Wen, and M. R. Lyu, "Why an Android app is classified as malware: Toward malware classification interpretation," *ACM Trans. Softw. Eng. Methodol.*, vol. 30, no. 2, pp. 1–29, Mar. 2021, doi: 10.1145/3423096.

[18] H. L. Thanh, "Analysis of malware families on Android mobiles: Detection characteristics recognizable by ordinary phone users and how to fix it," *J. Inf. Secur.*, vol. 4, no. 4, pp. 213–224, 2013.

[19] Y. Zhou and X. Jiang, "Dissecting Android malware: Characterization and evolution," in *Proc. IEEE Symp. Secur. Privacy*, May 2012, pp. 95–109.

[20] V. G. Shankar, M. Jangid, B. Devi, and S. Kabra, "Mobile big data: Malware and its analysis," in *Proc. 1st Int. Conf. Smart Syst., Innov. Comput.*, A. K. Somani, S. Srivastava, A. Mundra, and S. Rawat, Eds. Singapore: Springer, 2018, pp. 831–842.

[21] A. F. A. Kadir, N. Stakhanova, and A. A. Ghorbani, "Understanding Android financial malware attacks: Taxonomy, characterization, and challenges," *J. Cyber Secur. Mobility*, vol. 7, no. 3, pp. 1–52, 2018.

[22] (2020). *Cic Maldroid 2020 Dataset*. [Online]. Available: https://www.unb.ca/cic/datasets/maldroid-2020.html

[23] (2017). *Cic-Andmal 2017 Dataset*. [Online]. Available: https://www.unb.ca/cic/datasets/andmal2017.html

[24] D. Arp. (2022). *The Drebin Dataset*. [Online]. Available: https://www.sec.tu-bs.de/~danarp/drebin/index.html

[25] (2022). *The Amd Dataset*. [Online]. Available: https://amd.arguslab.org/

[26] S. Alsoghyer and I. Almomani, "Ransomware detection system for Android applications," *Electronics*, vol. 8, no. 8, p. 868, Aug. 2019, doi: 10.3390/electronics8080868.

[27] B. Lenaerts-Bergmans. (May 2023). *What is Adware? | Crowdstrike*. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/adware/

[28] H. Loi and A. Olmsted, "Low-cost detection of backdoor malware," in *Proc. 12th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2017, pp. 197–198.

[29] S. Gupta, H. Sharma, and S. Kaur, "Malware characterization using windows api call sequences," in *Proc. Int. Conf. Secur., Privacy, Appl. Cryptography Eng.* Hyderabad, India: Springer, 2016, pp. 271–280.

[30] J. Firch. (Oct. 2022). *Free It & Cyber Security Policy Templates for 2022*. [Online]. Available: https://purplesec.us/resources/prevent-cyber-attacks/backdoor/

[31] B. H. Custers, R. L. Pool, and R. Cornelisse, "Banking malware and the laundering of its profits," *Eur. J. Criminol.*, vol. 16, no. 6, pp. 728–745, Nov. 2019.

[32] (Feb. 2024). *What is a Banking Trojan and How Do You Stop One?* [Online]. Available: https://cybersmart.co.uk/blog/what-is-a-banking-trojan-and-how-do-you-stop-one/

[33] Q. Chen and R. A. Bridges, "Automated behavioral analysis of malware: A case study of WannaCry ransomware," in *Proc. 16th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2017, pp. 454–460.

[34] *What is Ransomware As a Service (RAAS)*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-ransomware-as-a-service

[35] A. Kapoor, A. Gupta, R. Gupta, S. Tanwar, G. Sharma, and I. E. Davidson, "Ransomware detection, avoidance, and mitigation scheme: A review and future directions," *Sustainability*, vol. 14, no. 1, p. 8, Dec. 2021.

[36] NCS Center. (Feb. 2020). *Mitigating Malware and Ransomware Attacks*. [Online]. Available: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

[37] W. F. Waheed and H. Alyasiri, "Evolving trees for detecting Android malware using evolutionary learning," *Int. J. Nonlinear Anal. Appl.*, vol. 14, no. 1, pp. 753–761, 2022.

[38] S. Rani and K. Dhindsa, "Behavioural characterization of Android malware to detect similar malware," *Int. J. Res. Electron. Comput. Eng.*, vol. 5, no. 4, pp. 1–6, 2017.

[39] F-Secure. *Android.Riskware | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/sw-desc/riskware-android.shtml

[40] Kaspersky. *Riskware (Not-A-Virus)*. Accessed: Mar. 10, 2024. [Online]. Available: https://encyclopedia.kaspersky.com/knowledge/riskware/

[41] A. Chehab and I. H. Elhajj, "Android SMS malware: Vulnerability and mitigation," Amer. Univ. Beirut, Beirut, Lebanon, Tech. Rep. AUB-CSE-2013-TR01, 2013.

[42] S. Feldman, D. Stadther, and B. Wang, "Manilyzer: Automated Android malware detection through manifest analysis," in *Proc. IEEE 11th Int. Conf. Mobile Ad Hoc Sensor Syst.*, Oct. 2014, pp. 767–772.

[43] Kaspersky. (Feb. 2021). *SMS Attacks and SMS Mobile Threats*. [Online]. Available: https://www.kaspersky.com/resource-center/threats/sms-attacks

[44] K. Hamandi, A. Chehab, I. H. Elhajj, and A. Kayssi, "Android SMS malware: Vulnerability and mitigation," in *Proc. 27th Int. Conf. Adv. Inf. Netw. Appl. Workshops*, Mar. 2013, pp. 1004–1009.

[45] D. Javaheri, M. Hosseinzadeh, and A. M. Rahmani, "Detection and elimination of spyware and ransomware by intercepting kernel-level system routines," *IEEE Access*, vol. 6, pp. 78321–78332, 2018.

[46] M. McDowell and M. Lytle. (Sep. 2019). *Recognizing and Avoiding Spyware | Cisa*. [Online]. Available: https://www.cisa.gov/news-events/news/recognizing-and-avoiding-spyware

[47] P. Seguin. (Apr. 2023). *Spyware: Detection, Prevention, and Removal*. [Online]. Available: https://www.avast.com/c-spyware

[48] A. Rahali and M. A. Akhloufi, "MalBERT: Using transformers for cybersecurity and malicious software detection," 2021, *arXiv:2103.03806*.

[49] I. Almomani, M. Ahmed, and W. El-Shafai, "Android malware analysis in a nutshell," *PLoS ONE*, vol. 17, no. 7, Jul. 2022, Art. no. e0270647, doi: 10.1371/journal.pone.0270647.

[50] J. Brownlee, *Deep Learning With Python: Develop Deep Learning Models on Theano and TensorFlow Using Keras*. Birmingham, U.K.: Machine Learning Mastery, 2016.

[51] M. Hodnett and J. F. Wiley, *R Deep Learning Essentials: A Step-by-Step Guide to Building Deep Learning Models Using TensorFlow, Keras, and MXNet*. Birmingham, U.K.: Packt, 2018.

[52] I. Vasilev, D. Slater, G. Spacagna, P. Roelants, and V. Zocca, *Python Deep Learning: Exploring Deep Learning Techniques and Neural Network Architectures With PyTorch, Keras, and TensorFlow*. Birmingham, U.K.: Packt, 2019.

[53] *Trojan: Android/Airpush Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_airpush.shtml

[54] *Adware: Android/Airpush Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/sw-desc/adware_android_airpush.shtml

[55] *Adware: Android/Dowgin.Variant! Online Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/sw-desc/adware_android_dowgin_online.shtml

[56] *Adware: Android/Dowgin Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/sw-desc/adware_android_dowgin.shtml

[57] VirusTotal. *Virustotal*. Accessed: Mar. 10, 2024. [Online]. Available: https://rb.gy/gn8rv

[58] Z. Li, "Advanced techniques to detect complex Android malware," Ph.D. dissertation, Dept. Comput. Sci. Eng., Univ. Nebraska-Lincoln, Lincoln, NE, USA, 2020.

[59] *How to Remove Android.Feiwo—Adware Removal Guide*. Accessed: Mar. 10, 2024. [Online]. Available: http://windowsbulletin.com/malware/adware/android-feiwo

[60] *Fortiguard*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.fortiguard.com/encyclopedia/virus/6576990

[61] (Nov. 11, 2020). *Gooligan: 8 Things You Need to Know About the Virus That Has Infected Over 1 Million Android Gadgets*. [Online]. Available: https://www.gadgetsnow.com/slideshows/gooligan-8-things-you-need-to-know-about-the-virus-that-has-infected-over-1-million-android-gadgets/apps-affected-by-gooligan/photolist/55756894.cms

[62] N. J. Cybersecurity and C. I. Cell. (2016). *Njccic Threat Profile Gooligan*. [Online]. Available: https://www.cyber.nj.gov/threat-center/threat-profiles/android-malware-variants/gooligan

[63] (2015). *Research | Trellix Stories*. [Online]. Available: https://www.fireeye.com/blog/threat-research/2015/10/kemoge_another_mobi.html

[64] M. Mimoso. (2015). *Kemoge Android Adware Campaign Can Lead to Device Takeover*. [Online]. Available: https://threatpost.com/kemoge-android-adware-campaign-can-lead-to-device-takeover/114946/

[65] *Android/adware.mobidash*. Accessed: Mar. 10, 2024. [Online]. Available: https://blog.malwarebytes.com/detections/android-adware-mobidash/

[66] Kaspersky. (Jan. 2015). *Kaspersky Threats—Mobidash*. [Online]. Available: https://threats.kaspersky.com/en/threat/Adware.AndroidOS.Mobidash/

[67] L. Constantin. (Oct. 2014). *Android SMS Worm Selfmite is Back, More Aggressive Than Ever*. [Online]. Available: https://www.computerworld.com/article/2824619/android-sms-worm-selfmite-is-back-more-aggressive-than-ever.html

[68] *Selfmite: Mobogenie Malware Attack Using SMS Worm to Boost PPI Income*. Accessed: Mar. 10, 2024. [Online]. Available: https://blog.adaptivemobile.com/selfmite-worm

[69] R. Millman. (Oct. 2014). *Selfmite Android Malware Returns, Bigger & Badder*. IT PRO. [Online]. Available: https://www.itpro.co.uk/malware/23268/selfmite-android-malware-returns-bigger-badder

[70] P. Paganini. (Jun. 2014). *Selfmite, the Rare Android Worm Which Spreads Itself By Sending SMS*. [Online]. Available: https://securityaffairs.co/wordpress/26187/cyber-crime/selfmite-rare-android-worm.html

[71] I. Martín, J. A. Hernández, and S. de los Santos, "On labeling Android malware signatures using minhashing and further classification with structural equation models," 2017, *arXiv:1709.04186*.

[72] J. Cox. (2015). *The Youmi Adware That Plagued Ios Apps Also Affects Android*. [Online]. Available: https://www.vice.com/en/article/9a399y/the-youmi-adware-that-plagued-ios-apps-also-affects-android

[73] (2017). *Detailed Analysis—Android Youmi—Adware and Puas—Advanced Network Threat Protection | Atp From Targeted Malware Attacks and Persistent Threats | Sophos.com—Threat Center*. [Online]. Available: https://www.sophos.com/en-us/threat-center/threat-analyses/adware-and-puas/Android%20Youmi/detailed-analysis

[74] *Android/Adware.Youmi.C*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.virusradar.com/en/Android_Adware.Youmi.C/description

[75] G. Meng, M. Patrick, Y. Xue, Y. Liu, and J. Zhang, "Securing Android app markets via modeling and predicting malware spread between markets," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 7, pp. 1944–1959, Jul. 2019.

[76] Sophos. (2014). *Detailed Analysis—Android Kuguo—Adware and Puas—Advanced Network Threat Protection | Atp From Targeted Malware Attacks and Persistent Threats | Sophos.com—Threat Center*. [Online]. Available: https://www.sophos.com/en-us/threat-center/threat-analyses/adware-and-puas/Android%20Kuguo/detailed-analysis

[77] R. Surendran and T. Thomas, "Detection of malware applications from centrality measures of syscall graph," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 10, p. e6835, 2022.

[78] G. Data, "Mobile malware report," *Retrieved September*, vol. 2, p. 2015, Jan. 2015.

[79] M. Ghosh. (Sep. 2015). *[updated] Security Research Firm Gdata Finds Over 20 Smartphones Pre-Installed With Malwares*. [Online]. Available: https://trak.in/tags/business/2015/09/04/smartphones-xiaomi-lenovo-huawei-pre-installed-malwares/

[80] N. Security. (Apr. 2018). *Mobile Devices Bundled With Malware?* [Online]. Available: https://blog.newskysecurity.com/mobile-devices-bundled-with-malware-e50e3207913d

[81] G. Suarez-Tangil and G. Stringhini, "Eight years of rider measurement in the Android malware ecosystem: Evolution and lessons learned," 2018, *arXiv:1801.08115*.

[82] H. Fereidooni, V. Moonsamy, M. Conti, and L. Batina, "Efficient classification of Android malware in the wild using robust static features," in *Protecting Mobile Networks and Devices: Challenges and Solutions*, vol. 1. New York, NY, USA: Association for Computing Machinery (ACM), 2016, pp. 181–209.

[83] G. Kaur and A. H. Lashkari. (Jan. 2021). *Understanding Android Malware Families (UAMF)—The Foundations (Article 1)*. [Online]. Available: https://www.itworldcanada.com/blog/understanding-android-malware-families-uamf-the-foundations-article-1/441562

[84] TBA. *Utchi Variety1*. Accessed: Mar. 10, 2024. [Online]. Available: https://amd.arguslab.org/families/Utchi/variety1.html

[85] *Potentially Unwanted Application Troubleshooting*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.solvusoft.com/en/malware/potentially-unwanted-application/

[86] F. Turangan, D. A. Utari, and K. Mawuntu, "Comparative study of Android smartphone-based antivirus performance using the tam method," *Int. J. Inf. Technol. Educ.*, vol. 1, no. 1, pp. 59–67, 2021.

[87] E. J. Alqahtani, R. Zagrouba, and A. Almuhaideb, "A survey on Android malware detection techniques using machine learning algorithms," in *Proc. 6th Int. Conf. Softw. Defined Syst. (SDS)*, Jun. 2019, pp. 110–117.

[88] Bferrite. (May 2017). *The Judy Malware: Possibly the Largest Malware Campaign Found on Google Play*. [Online]. Available: https://blog.checkpoint.com/2017/05/25/judy-malware-possibly-largest-malware-campaign-found-google-play/

[89] C. Albanesius. (May 2017). *'Judy' Malware Potentially Hits Up to 36.5m Android Users*. [Online]. Available: https://www.pcmag.com/news/judy-malware-potentially-hits-up-to-365m-android-users

[90] A. Fraudwatch. (Jun. 2017). *Beware*. [Online]. Available: https://fraudwatch.com/beware-of-judy-the-latest-android-mobile-app-malware/

[91] (May 2017). *Millions of Android Phones Hit By 'Judy' Malware*. BBC News. [Online]. Available: https://www.bbc.com/news/technology-40092540

[92] M. T. Kyaw and N. S. M. Kham, "Machine learning based Android malware detection using significant permission identification," Ph.D. dissertation, Dept. Comput. Sci. Inf. Technol., Univ. Malaya, Kuala Lumpur, Malaysia, 2019.

[93] O. Sahin, A. K. Coskun, and M. Egele, "Proteus: Detecting Android emulators from instruction-level profiles," in *Proc. Int. Symp. Res. Attacks, Intrusions, Defenses*. Springer, 2018, pp. 3–24.

[94] E. Xu. (2017). *Xavier: An Information-stealing Ad Library on Android*. [Online]. Available: https://www.trendmicro.com/en_us/research/17/f/analyzing-xavier-information-stealing-ad-library-android.html

[95] *What is an Info-stealing Ad Library?* Accessed: Mar. 10, 2024. [Online]. Available: https://au.norton.com/blog/emerging-threats/what-is-info-stealing-library

[96] C. Jeffrey. (Jun. 2017). *New Android Malware Xavier Quietly Steals Your Data*. [Online]. Available: https://www.techspot.com/news/69756-new-android-malware-xavier-quietly-steals-data.html

[97] K. Wiggers. (Jun. 2017). *Xavier Android Malware Steals Personal Data*. [Online]. Available: https://www.digitaltrends.com/mobile/xavier-andoid-malware/

[98] A. Kuprins. (Jul. 2019). *'Updates for Samsung'—From a Blog to an Android Advertisement Revenue Goldmine of 10,000,000+*. [Online]. Available: https://medium.com/csis-techblog/updates-for-samsung-from-a-blog-to-an-android-advertisement-revenue-goldmine-of-10-000-000-166585e34ad0

[99] zLabs. (Aug. 2017). *Fake Snapchat in Google Play Store*. Zimperium. [Online]. Available: https://www.zimperium.com/blog/fake-snapchat-google-play-store/

[100] P. Newsroom. (Apr. 2018). *Snapchat Users Subjected to Malicious Phishing Attack*. PSafe Blog. [Online]. Available: https://www.psafe.com/en/blog/snapchat-users-subjected-to-malicious-phishing-attack/

[101] G. E. Hall. (May 2020). *Remove Snapchat Virus (Updated May 2020)—Removal Guide*. [Online]. Available: https://www.2-spyware.com/remove-snapchat-virus.html

[102] (Aug. 2017). *Fake Snapchat in Google Play Store_hackdig*. [Online]. Available: http://en.hackdig.com/08/62240.htm

[103] A. Spadafora. (Jan. 2020). *Android Beauty Apps Could Give Your Phone a Black Eye*. [Online]. Available: https://www.techradar.com/news/android-beauty-apps-could-give-your-phone-a-black-eye

[104] (May 2022). *Android Users Attacked By Malicious*. ITRC. [Online]. Available: https://www.idtheftcenter.org/post/android-users-attacked-by-malicious-beauty-camera-app/

[105] V. Malhotra. (Jan. 2020). *These Android Beauty Apps Won't Give You Beauty but Malware; Delete Them Now*. [Online]. Available: https://www.indiatvnews.com/technology/news-android-beauty-apps-with-malware-delete-now-581679

[106] K. Threats. (Jan. 2017). *Kaspersky Threats—Hiddad*. [Online]. Available: https://threats.kaspersky.com/en/threat/Trojan.AndroidOS.Hiddad/

[107] E. Xu. (Jan. 2019). *Disguised Adware Infect 9 Million Google Play Users*. Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/research/19/a/adware-disguised-as-game-tv-remote-control-apps-infect-9-million-google-play-users.html

[108] J. Xiung. (Feb. 2021). *This Qr Code Scanner Was Infected By Malware After an Update, Over 10 Million Android Devices Are Affected*. [Online]. Available: https://soyacincau.com/2021/02/10/this-qr-code-scanner-was-infected-by-malware-after-an-update-over-10-million-android-devices-are-affected/

[109] N. Collier. (2021). *Barcode Scanner App on Google Play Infects 10 Million Users With One Update | Malwarebytes Labs*. [Online]. Available: https://www.malwarebytes.com/blog/news/2021/02/barcode-scanner-app-on-google-play-infects-10-million-users-with-one-update

[110] M. Y. Tee and M. Zhang. (Sep. 2019). *More Hidden App Malware Found on Google Play With Over 2.1 Million Downloads*. [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/hidden-adware-google-play

[111] S. T. Intelligence and R. Team. (Nov. 2019). *Twoshu, Electric Boogaloo*. [Online]. Available: https://www.humansecurity.com/learn/blog/twoshu-electric-boogaloo

[112] V. Mirchandani. (Jan. 2018). *Adultswine Malware Inserts Porn Ads and More in Android Games on Google Play Store*. [Online]. Available: https://beebom.com/adultswine-malware-inserts-porn-ads-android-games-google-play-store/

[113] M. Adams. (2018). *New 'Adultswine' Malware Could Display Pornographic Images to Children*. Android Authority. [Online]. Available: https://www.androidauthority.com/adultswine-play-store-pornographic-images-830045/

[114] A. Conway. (Jan. 2018). *'Adultswine' Play Store Malware Shows Pornography in Games for Kids*. XDA Developers. [Online]. Available: https://www.xda-developers.com/adultswine-malware-pornography-kids-games-apps/

[115] E. Root and B. Melnykov. (Jan. 2018). *Malware Displaying Porn Ads Discovered in Game Apps on Google Play*. [Online]. Available: https://research.checkpoint.com/2018/malware-displaying-porn-ads-discovered-in-game-apps-on-google-play/

[116] (Apr. 2018). *Android Security: Click Fraud Apps Drove 100% Malware Increase in Google Play for 2018—Security News*. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/mobile-safety/android-security-click-fraud-apps-drove-100-malware-increase-in-google-play-for-2018

[117] O. Lynch. (Jun. 2020). *Click Fraud Malware 2020: Tekya*. [Online]. Available: https://www.clickcease.com/blog/click-fraud-malware-2020-tekya/

[118] K. Sun. (Jan. 2018). *Ghostteam Adware Can Steal Facebook Credentials*. [Online]. Available: https://www.trendmicro.com/en_us/research/18/a/ghostteam-adware-can-steal-facebook-credentials.html

[119] C. Cimpanu. (Jan. 2018). *Ghostteam Android Malware Can Steal Facebook Credentials*. [Online]. Available: https://www.bleepingcomputer.com/news/security/ghostteam-android-malware-can-steal-facebook-credentials/

[120] V. Tiwari. (Jan. 2018). *Beware-Ghostteam, a New Android Malware Can Steal Your Facebook Password*. We The Geek. [Online]. Available: https://wethegeek.com/beware-ghostteam-a-new-android-malware-can-steal-your-facebook-password/

[121] V. Soni. (Jan. 2018). *Ghostteam Malware Stealing Facebook Credentials of Android Users for Almost a Year*. Web Hosting | Cloud Computing | Datacenter | Domain News. [Online]. Available: https://www.dailyhostnews.com/ghostteam-stealing-fb-credentials-of-android-users

[122] SCLTR Team. (Oct. 2018). *Panini Adware for Android Soaks Network Bandwidth, Bad News for Users With Limited Data—Sonicwall*. [Online]. Available: https://securitynews.sonicwall.com/xmlpost/panini-adware-for-android-soaks-network-bandwidth-bad-news-for-users-with-limited-data/

[123] (Mar. 2018). *Android Malware Rottensys Has Infected 5 Million Smartphones*. 360 Total Security Blog. [Online]. Available: https://blog.360totalsecurity.com/en/android-malware-rottensys-infected-phones/

[124] McAfee. (Mar. 2018). *Rottensys Malware Reminds Users to Think Twice Before Buying a Bargain Phone*. McAfee Blog. [Online]. Available: https://www.mcafee.com/blogs/mobile-security/rottensys-malware/

[125] L. Frink. (Mar. 2018). *Rottensys: Some Smartphones Are Coming With Malware Already Installed*. Avira Blog. [Online]. Available: https://www.avira.com/en/blog/rottensys-preinstalled-malware

[126] M. Zhang and S. Aimoto. (May 2018). *Malicious Apps Persistently Appearing on Google Play and Using Google Icons*. [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/persistent-malicious-apps-google-play

[127] TI Team. (Apr. 2019). *Android Apps on Google Play Store Come With Nasty Surprise*. [Online]. Available: https://blog.avast.com/adware-plagues-google-play

[128] K. Balaam. (Jun. 2019). *Adware 'Beitaad' Found Hidden in Popular Applications | Lookout*. [Online]. Available: https://www.lookout.com/blog/beitaplugin-adware

[129] L. Stefanko. (2019). *Cometbot*. Twitter. [Online]. Available: https://twitter.com/LukasStefanko/status/1102889352118616064

[130] J. Huang. (Nov. 2019). *Fake Apps Read SMS Codes to Trigger Wap, Carrier Bill*. Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/research/19/k/49-disguised-adware-apps-with-optimized-evasion-features-found-on-google-play.html

[131] D. Web. (Jun. 2019). *Doctor Web: Android Users Threatened By Fraudulent Push Notifications*. [Online]. Available: https://news.drweb.com/show/?i=13313&lng=en

[132] SCLTR Team. (Apr. 2019). *Analyzing Gretel A7 Android Device for Pre-installed Malware—Part II—Sonicwall*. [Online]. Available: https://securitynews.sonicwall.com/xmlpost/analyzing-gretel-a7-android-device-for-pre-installed-malware-part-2/

[133] L. Stefanko. (2019). *Gretel*. [Online]. Available: https://twitter.com/lukasstefanko/status/1110470964549173248

[134] (Mar. 2019). *Found the APK + Files of a Chinese Malware That Automatically Installed on My Android Phone*. [Online]. Available: https://www.reddit.com/r/Malware/comments/b5ddri/found_the_apk_files_of_a_chinese_malware_that/

[135] D. Web. (Apr. 2019). *Doctor Web: Trojan Android.infectionads Exploits Critical Vulnerabilities of Android to Infect and Install Other Software*. [Online]. Available: https://news.drweb.com/show/?i=13108&lng=en

[136] E. Xu. (Aug. 2019). *Adware Posing as 85 Photography and Gaming Apps on Google Play Installed Over 8 Million Times*. Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/research/19/h/adware-posing-as-85-photography-and-gaming-apps-on-google-play-installed-over-8-million-times.html

[137] V. Palladino. (Nov. 2019). *Evina's Cybersecurity Analysts Found a New Trojan Family on Google Play Store*. Evina. [Online]. Available: https://www.evina.com/evinas-cybersecurity-analysts-found-a-new-trojan-family-on-google-play-store/

[138] B. N. (Dec. 2019). *New Malware Family 'Venus' Infects 285,000 Android Users*. GBHackers On Security. [Online]. Available: https://gbhackers.com/venus-google-play/

[139] D. Eugenio. (Jul. 2019). *Agent Smith: A New Species of Mobile Malware*. Check Point Research. [Online]. Available: https://research.checkpoint.com/2019/agent-smith-a-new-species-of-mobile-malware/

[140] P. Kohli. (Oct. 2019). *Icon-hiding Android Adware Returns to the Play Market*. Sophos News. [Online]. Available: https://news.sophos.com/en-us/2019/10/08/icon-hiding-android-adware-returns-to-the-play-market/

[141] Mobilesecurity. (2019). *Iconhiding*. Twitter. [Online]. Available: https://twitter.com/mobilesecurity_/status/1181846475829059584

[142] I. Ilascu. (Sep. 2019). *Selfie Android Apps With 1.5m+ Installs Push Ads, Can Record Audio*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/selfie-android-apps-with-15m-installs-push-ads-can-record-audio/

[143] P. Paganini. (Sep. 2019). *Two Selfie Android Adware Apps With 1.5m+ Downloads Removed From Play Store*. Security Affairs. [Online]. Available: https://securityaffairs.co/wordpress/91540/malware/android-adware-apps-play-store.html

[144] E. Montalbano. (Mar. 2020). *Tekya Malware Threatens Millions of Android Users Via Google Play*. [Online]. Available: https://threatpost.com/tekya-malware-android-google-play/154064/

[145] F. Quin. (Jun. 2020). *New Tekya Ad Fraud Found on Google Play*. Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/research/20/f/new-tekya-ad-fraud-found-on-google-play.html

[146] I. Wernik, D. Golubenko, and A. Hazum. (Mar. 2020). *Google Play Store Played Again—Tekya Clicker Hides in 24 Children's Games and 32 Utility Apps—Check Point Research*. Check Point Research. [Online]. Available: https://research.checkpoint.com/2020/google-play-store-played-again-tekya-clicker-hides-in-24-childrens-games-and-32-utility-apps/

[147] (Nov. 2020). *Fake 'Among Us' Apps Surface, But They Might Actually Be Malware*. Tech Times. [Online]. Available: https://www.techtimes.com/articles/254507/20201126/among-us-fake-versions-malware-experts-warn.htm

[148] (Nov. 2020). *Don't Download That Among Us App—It Could Be Malware*. TechRadar. [Online]. Available: https://www.techradar.com/news/dont-download-that-among-us-app-it-could-be-malware

[149] (Nov. 2020). *Expert Reaction on News: Among Us App Used to Distribute Malware*. Information Security Buzz. [Online]. Available: https://informationsecuritybuzz.com/expert-comments/expert-reaction-on-news-among-us-app-used-to-distribute-malware/

[150] I. Golovin and A. Kivva. (Jul. 2020). *Pig in a Poke: Smartphone Adware*. [Online]. Available: https://securelist.com/pig-in-a-poke-smartphone-adware/97607/

[151] D. Kerr. (Jun. 2013). *Malware Masquerading As Bad Piggies Found on Google Play*. CNET. [Online]. Available: https://www.cnet.com/news/privacy/malware-masquerading-as-bad-piggies-found-on-google-play/

[152] E. Montalbano. (Jul. 2020). *Malicious 'Blur' Photo App Campaign Discovered on Google Play*. [Online]. Available: https://threatpost.com/malicious-photo-app-campaign-google-play/157712/

[153] A. Hashim. (Aug. 2020). *Numerous Malicious Photo Blur Apps Appeared on Play Store*. Latest Hacking News | Cyber Security News, Hacking Tools and Penetration Testing Courses. [Online]. Available: https://latesthackingnews.com/2020/08/01/numerous-malicious-photo-blur-apps-appeared-on-play-store/

[154] D. Web. (Mar. 2020). *Android.Circle.1 Adware Trojan Found on Google Play is Capable of Executing Beanshell Scripts*. [Online]. Available: https://news.drweb.com/show/?i=13740

[155] (Mar. 2020). *Beanshell*. Twitter. [Online]. Available: https://mobile.twitter.com/m0br3v/status/1242437741562015744

[156] I. Golovin. (Jun. 2021). *Malware Disguised As Minecraft Mods on Google Play, Continued*. [Online]. Available: https://www.kaspersky.com/blog/minecraft-mod-adware-google-play-revisited/40202/

[157] I. Ilascu. (Nov. 2020). *Fake Minecraft Mods Swamp Over 1m Android Devices With Ads*. [Online]. Available: https://www.bleepingcomputer.com/news/security/fake-minecraft-mods-swamp-over-1m-android-devices-with-ads/

[158] M. M. published. (Jun. 2021). *Beware—Those New Minecraft Mods Could Be Harmful Malware*. TechRadar. [Online]. Available: https://www.techradar.com/news/watch-out-that-minecraft-mod-could-be-dangerous-malware

[159] B. Bracken. (Oct. 2020). *Rainbowmix Apps in Google Play Serve Up Millions of Ad Fraud Victims*. [Online]. Available: https://threatpost.com/rainbowmix-apps-google-play-ad-fraud/159982/

[160] I. Ilascu. (Oct. 2020). *Rainbowmix Apps Generate $150,000 in Daily Ad Fraud Profit*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/rainbowmix-apps-generate-150-000-in-daily-ad-fraud-profit/

[161] S. T. Intelligence and R. Team. (Oct. 2020). *Somewhere Over the Rainbow(mix)*. [Online]. Available: https://www.humansecurity.com/learn/blog/somewhere-over-the-rainbowmix

[162] K. O'Flaherty. (Oct. 2020). *Android Users Beware: Delete These 240 Malicious Apps Now*. Forbes. [Online]. Available: https://www.forbes.com/sites/kateoflahertyuk/2020/10/08/android-users-beware-delete-these-240-malicious-apps-now/?sh=6a782be14a41

[163] B. Bracken. (Apr. 2021). *Adware Spreads Via Fake Tiktok App, Laptop Offers*. [Online]. Available: https://threatpost.com/adware-tiktok-laptop-offers/165318/

[164] Kaspersky. (Jun. 2021). *Tiktok Privacy and Security—Is Tiktok Safe to Use?* [Online]. Available: https://usa.kaspersky.com/resource-center/preemptive-safety/is-tiktok-safe

[165] BusinessTechSA. (2013). *Warning: Free Apps May Be Loaded With Malware*. [Online]. Available: https://businesstech.co.za/news/mobile/41208/warning-free-apps-may-be-loaded-with-malware/

[166] Kaspersky. (May 2021). *99% of All Mobile Threats Target Android Devices*. [Online]. Available: https://www.kaspersky.com/about/press-releases/2013_99-of-all-mobile-threats-target-android-devices

[167] R. Singha. (Oct. 2013). *The Top 20 Android Malware—How They Work*. Quick Heal Blog | Latest Computer Security News, Tips, and Advice. [Online]. Available: https://blogs.quickheal.com/top-20-android-malware-how-they-work/

[168] Z. Zorz. (Apr. 2017). *Ewind Android Adware is Actually a Full-fledged Trojan*. Help Net Security. [Online]. Available: https://www.helpnetsecurity.com/2017/04/12/russian-android-adware-trojan/

[169] N. J. Cybersecurity and C. I. Cell. (2017). *Ewind Njccic Threat Profile*. [Online]. Available: https://www.cyber.nj.gov/threat-center/threat-profiles/android-malware-variants/ewind

[170] Kaspersky. (Sep. 2016). *Kaspersky Threats—Ewind*. [Online]. Available: https://threats.kaspersky.com/en/threat/Adware.AndroidOS.Ewind/

[171] S. Barker. (Apr. 2017). *Unit 42 Researchers Suspect Ewind Adware Trojan is 100% Russian*. SecurityBrief Asia. [Online]. Available: https://securitybrief.asia/story/unit-42-researchers-suspect-ewind-adware-trojan-100-russian

[172] TBA. *Minimob Variety1*. Accessed: Mar. 10, 2024. [Online]. Available: http://amd.arguslab.org/families/Minimob/variety1.html

[173] Sophos. (2015). *Detailed Analysis—Android Minimob—Adware and Puas—Advanced Network Threat Protection | Atp From Targeted Malware Attacks and Persistent Threats | Sophos.com—Threat Center*. [Online]. Available: https://www.sophos.com/en-us/threat-center/threat-analyses/adware-and-puas/Android%20Minimob/detailed-analysis

[174] M. Mimoso. (Nov. 2015). *Shuanet Adware Rooting Android Devices Via Trojanized Apps*. [Online]. Available: https://threatpost.com/shuanet-adware-rooting-android-devices-via-trojanized-apps/115265/

[175] (Oct. 2022). *Shedun, Shuanet, and Shiftybug: Android Protect Smartphone From Malware*. [Online]. Available: https://technical-tips.com/blog/android/shedun-shuanet-and-shiftybug-android-19560

[176] D. Web. (2016). *Android.Spy.277.Origin—Dr.Web Malware Description Library*. [Online]. Available: https://vms.drweb.com/virus/?_is=1&i=8020079&lng=en

[177] A. Sangal and H. K. Verma, "A static feature selection-based Android malware detection using machine learning techniques," in *Proc. Int. Conf. Smart Electron. Commun. (ICOSEC)*, Sep. 2020, pp. 48–51.

[178] T. S. R. Pimenta, R. D. C. D. Santos, and A. Grégio, "Family matters: On the investigation of [malicious] mobile apps clustering," in *Proc. Int. Conf. Comput. Sci. Appl.* Dordrecht, Holland: Springer, 2021, pp. 79–94.

[179] M. K. A. Abuthawabeh and K. W. Mahmoud, "Android malware detection and categorization based on conversation-level network traffic features," in *Proc. Int. Arab Conf. Inf. Technol. (ACIT)*, Dec. 2019, pp. 42–47.

[180] J. Murdock. (Aug. 2017). *'Ghostclicker' Malware Found in 340 Apps on Google Play Had 'Millions' of Downloads*. International Business Times U.K. [Online]. Available: https://www.ibtimes.co.uk/ghostclicker-malware-found-340-apps-google-play-had-millions-downloads-1635511

[181] E. Duan and R. Sun. (Aug. 2017). *Ghostclicker Adware: A Phantomlike Android Click Fraud*. [Online]. Available: https://www.trendmicro.com/en_us/research/17/h/ghostclicker-adware-is-a-phantomlike-android-click-fraud.html

[182] C. Cimpanu. (Aug. 2017). *Auto-Clicking Android Adware Found in 340 Apps on the Google Play Store*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/auto-clicking-android-adware-found-in-340-apps-on-the-google-play-store/

[183] CPST. (2017). *An In-depth Analysis of the Copycat Android Malware Campaign Copycat*. [Online]. Available: https://www.checkpoint.com/downloads/resources/copycat-research-report.pdf

[184] Bferrite. (Jul. 2017). *How the Copycat Malware Infected Android Devices Around the World*. Check Point Software. [Online]. Available: https://blog.checkpoint.com/2017/07/06/how-the-copycat-malware-infected-android-devices-around-the-world/

[185] A. Ng. (Jul. 2017). *14 Million Android Devices Got Hit by This Fake App's Virus*. CNET. [Online]. Available: https://www.cnet.com/news/privacy/android-hack-copycat-malware-device-outdated-14-million/

[186] (Oct. 2011). *Current Android Malware*. [Online]. Available: https://forensics.spreitzenbarth.de/android-malware/

[187] H.-S. Ham, H.-H. Kim, M.-S. Kim, and M.-J. Choi, "Linear SVM-based Android malware detection for reliable IoT services," *J. Appl. Math.*, vol. 2014, pp. 1–10, Jan. 2014.

[188] M. Corporation. (2017). *Trojan: Androidos/Spygold.a Threat Description—Microsoft Security Intelligence*. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:AndroidOS/SpyGold.A

[189] L. Shi, J. Ming, J. Fu, G. Peng, D. Xu, K. Gao, and X. Pan, "VAHunt: Warding off new repackaged Android malware in app-virtualization's clothing," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2020, pp. 535–549.

[190] K.-C. Lee, C.-H. Hsieh, L.-J. Wei, C.-H. Mao, J.-H. Dai, and Y.-T. Kuang, "Sec-buzzer: Cyber security emerging topic mining with open threat intelligence retrieval and timeline event annotation," *Soft Comput.*, vol. 21, no. 11, pp. 2883–2896, Jun. 2017.

[191] J. Snow. (Mar. 2016). *Triada: Truly Scary Malware for Android*. [Online]. Available: https://www.kaspersky.com/blog/triada-trojan/11481/

[192] K. Threats. (Sep. 2016). *Kaspersky Threats—Triada*. [Online]. Available: https://threats.kaspersky.com/en/threat/Backdoor.AndroidOS.Triada/

[193] N. Buchka and M. Kuzin. (Mar. 2016). *Attack on Zygote: A New Twist in the Evolution of Mobile Threats*. [Online]. Available: https://securelist.com/attack-on-zygote-a-new-twist-in-the-evolution-of-mobile-threats/74032/

[194] G. Suarez-Tangil, J. E. Tapiador, P. Peris-Lopez, and A. Ribagorda, "Evolution, detection and analysis of malware for smart devices," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 961–987, 2nd Quart., 2014.

[195] F-Secure. *Trojan: Android/Fjcon.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_fjcon.shtml

[196] I. Adegbola and R. Jimoh, "Spambot detection: A review of techniques and trends," *Network*, vol. 6, no. 9, pp. 1–4, 2014.

[197] B. Reed. (Dec. 2013). *How to Make Money By Turning Your Android Phone Into an SMS Spambot*. BGR. [Online]. Available: https://bgr.com/general/android-text-messaging-spam-apps/

[198] O. Mirzaei, "Techniques for advanced Android malware triage," Univ. California, Santa Barbara, CA, USA, Tech. Rep. UCSB-CS-2019-02, 2019.

[199] F-Secure. *Trojan: Android/Fakeangry Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_fakeangry.shtml

[200] D. Web. (Jun. 2014). *Mobile Threats*. [Online]. Available: https://news.drweb.com/show/?i=5827&lng=en&c=9

[201] A. Karim, S. A. Ali Shah, R. B. Salleh, M. Arif, R. M. Noor, and S. Shamshirband, "Mobile botnet attacks-an emerging threat: Classification, review and open issues," *KSII Trans. Internet Inf. Syst. (TIIS)*, vol. 9, no. 4, pp. 1471–1492, 2015.

[202] I. Burke and H. Pieterse, "How to tame your Android malware," in *Proc. 10th Int. Conf. Cyber Warfare Secur.*, 2015, pp. 54–65.

[203] McAfee. (Jun. 2013). *What You Need to Know About the Latest Android Threat*. McAfee Blog, [Online]. Available: https://www.mcafee.com/blogs/mobile-security/obad-a-what-you-need-to-know-about-the-latest-android-threat/

[204] GoldSparrow. (Jun. 2013). *Backdoor.Androidos.Obad.A May Be the Most Difficult Mobile Trojan to Remove*. Remove Spyware & Malware with SpyHunter—EnigmaSoft. [Online]. Available: https://www.enigmasoftware.com/backdoor-androidos-obad-a-may-be-most-difficult-mobile-trojan-remove/

[205] R. Unuchek. (Sep. 2013). *Trojan Now Being Distributed Via Mobile Botnets*. [Online]. Available: https://securelist.com/obad-a-trojan-now-being-distributed-via-mobile-botnets/57453/

[206] T. Desk. (Nov. 2020). *New Android Malware Uses Google Firebase Cloud Messaging to Infect Devices: Report*. The Indian Express. [Online]. Available: https://indianexpress.com/article/technology/tech-news-technology/new-malware-using-googles-firebase-cloud-messaging-to-infect-devices-6920889/

[207] V. A. Singh. (Nov. 2020). *Donot Firestarter Malware Using Google Firebase Cloud Messaging: Report*. Gadgets 360. [Online]. Available: https://www.gadgets360.com/mobiles/news/donot-firestarter-android-malware-google-firebase-cloud-messaging-cisco-talos-report-2319530

[208] K. SinhaChaudhury. (Nov. 2020). *Donot Firestarter is the New Android Malware That Uses Google Firebase Cloud Messaging to Spread Infection*. [Online]. Available: https://www.timesnownews.com/technology-science/article/donot-firestarter-is-the-new-android-malware-that-uses-google-firebase-cloud-messaging-to-spread-infection/676641

[209] V. Zhang. (Jun. 2016). *'Godless' Mobile Malware Roots Devices*. Trend Micro. [Online]. Available: https://www.trendmicro.com/tr_tr/research/16/f/godless-mobile-malware-uses-multiple-exploits-root-devices.html

[210] NJCCIC. (2022). *Godless Njccic Threat Profile*. [Online]. Available: https://www.cyber.nj.gov/threat-center/threat-profiles/android-malware-variants/godless

[211] S. News. (Jun. 2016). *'Godless' Android Malware Uses Multiple Rooting Exploits | Securityweek.com*. [Online]. Available: https://www.securityweek.com/godless-android-malware-uses-multiple-rooting-exploits

[212] D. Bisson. (Jun. 2016). *Godless Mobile Malware Can Root 90% of Android Devices*. Graham Cluley. [Online]. Available: https://grahamcluley.com/godless-android-malware/

[213] *Virustotal—Rogue_Skype*. Accessed: Mar. 10, 2024. [Online]. Available: https://rb.gy/h11d6

[214] D. Lukic. (Jan. 2021). *Rogue Malware on Android: What to Know About It*. IDStrong. [Online]. Available: https://www.idstrong.com/sentinel/android-users-watch-out-for-rogue-malware/

[215] M. Kumar. (Jan. 2019). *New Android Malware Apps Use Motion Sensor to Evade Detection*. The Hacker News,. [Online]. Available: https://thehackernews.com/2019/01/android-malware-play-store.html

[216] W. Chalk. (Feb. 2019). *New Android Malware Uses Motion Sensor Data to Avoid Detection By William Chalk*. [Online]. Available: https://hakin9.org/new-android-malware/

[217] J. Stone. (Jan. 2019). *Sneaky Motion-detection Feature Found on Android Malware*. CyberScoop. [Online]. Available: https://www.cyberscoop.com/android-malware-motion-detection-trend-micro/

[218] K. Sun. (Jan. 2019). *Google Play Apps Drop Anubis, Use Motion-Based Evasion*. Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/research/19/a/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics.html

[219] V. Chebyshev and N. Buchka. (Mar. 2015). *SMS Trojan Bypasses Captcha*. [Online]. Available: https://securelist.com/sms-trojan-bypasses-captcha/69169/

[220] J. Sirmer. (Jan. 2015). *Fobus, the Sneaky Little Thief That Could*. [Online]. Available: https://blog.avast.com/2015/01/15/fobus-the-sneaky-little-thief-that-could/

[221] F-Secure. *Trojan: Android/Stiniter.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_stiniter.shtml

[222] M. S. Intelligence. (Sep. 2017). *Trojan: Androidos/Stiniter.A Threat Description—Microsoft Security Intelligence*. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:AndroidOS/Stiniter.A

[223] F-Secure. *Monitoring-Tool: Android/Spyhasb.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/sw-desc/monitoring-tool_android_spyhasb.shtml

[224] (Sep. 2018). *Android/Fakengry.Ct!Tr.Bdr*. FortiGuard. [Online]. Available: https://www.fortiguard.com/encyclopedia/virus/7905755

[225] M. Corporation. (2017). *Trojan: Androidos/Smshider.A Threat Description—Microsoft Security Intelligence*. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:AndroidOS/SmsHider.A

[226] L. Bermejo, J. Pan, and C. Pernet. (Jul. 2017). *Android Backdoor Ghostctrl Records Your Audio, Video*. Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/research/17/g/android-backdoor-ghostctrl-can-silently-record-your-audio-video-and-more.html

[227] M. Yang. (Jul. 2017). *Ghostctrl Android Malware Hijacks Audio, Roots Devices*. Pindrop. [Online]. Available: https://www.pindrop.com/blog/ghostctrl-android-malware-hijacks-audio-roots-devices

[228] C. Cimpanu. (Jul. 2017). *Ghostctrl is an Android Rat That Also Doubles as Ransomware*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/ghostctrl-is-an-android-rat-that-also-doubles-as-ransomware/

[229] I. Group. (Mar. 2014). *Dendroid Rat: The Next Stage of Android Malware Evolution*. Infosecurity Magazine. [Online]. Available: https://www.infosecurity-magazine.com/news/dendroid-rat-the-next-stage-of-android-malware/

[230] F-Secure. *Backdoor: Android/Dendroid.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/backdoor_android_dendroid_a.shtml

[231] (Mar. 2014). *Endpoint Protection—Symantec Enterprise*. [Online]. Available: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=a29d7d7a-f150-46cf-9bb9-a1f9f4d32a80&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

[232] Wikipedia. (Nov. 2021). *Dendroid (Malware)*. Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Dendroid_(malware)

[233] E. Kovacs. (Jul. 2015). *Google Play Checks Bypassed By Hacking Team Android Backdoor | Securityweek.com*. [Online]. Available: https://www.securityweek.com/google-play-checks-bypassed-hacking-team-android-backdoor

[234] T. Gurus. (Jul. 2015). *Trend Micro Discovers Hacking Team Android Malware App That Avoids Google Play Checks*. IT Secur. Guru. [Online]. Available: https://www.itsecurityguru.org/2015/07/17/trend-micro-discovers-hacking-team-android-malware-app-that-avoids-google-play-checks/

[235] Vijay. (Jul. 2015). *Benews Android App Developed By the Hacking Team Escaped Google Play Vetting and Installed Malware*. TechWorm. [Online]. Available: https://www.techworm.net/2015/07/hacking-team-made-a-snooping-app-benews-that-could-avoid-google-play-vetting.html

[236] CPMT Prevention. (Sep. 2015). *Braintest—A New Level of Sophistication in Mobile Malware*. Check Point Software. [Online]. Available: https://blog.checkpoint.com/2015/09/21/braintest-a-new-level-of-sophistication-in-mobile-malware/

[237] S. News. (Jan. 2016). *'Nasty' Brain Test Android Malware Returns to Google Play*. [Online]. Available: https://www.securityweek.com/nasty-brain-test-android-malware-returns-google-play

[238] GoldSparrow. (Jan. 2016). *Malicious 'brain Test' App Reappears on Google Play Store Infecting Android Devices Via Affiliate Program*. Remove Spyware & Malware with SpyHunter—EnigmaSoft. [Online]. Available: https://www.enigmasoftware.com/malicious-brain-test-app-reappears-google-play-store-infect-android-devices/

[239] S. M. Kerner. (Sep. 2015). *Malicious Brain Test App Thwarts Google Play Android Security*. eWEEK. [Online]. Available: https://www.eweek.com/security/malicious-brain-test-app-thwarts-google-play-android-security/

[240] Wikipedia. (Nov. 2021). *Brain Test*. [Online]. Available: https://en.wikipedia.org/wiki/Brain_Test

[241] C. Osborne. (Feb. 2019). *Farseer Malware Brings Windows Exploits to Attack Group's Android Arsenal*. ZDNET. [Online]. Available: https://www.zdnet.com/article/new-farseer-malware-brings-windows-exploits-to-chinese-attacker-arsenal/

[242] A. Hinchliffe. (Feb. 2019). *Farseer: Previously Unknown Malware Family Bolsters the Chinese Armoury*. [Online]. Available: https://unit42.paloaltonetworks.com/farseer-previously-unknown-malware-family-bolsters-the-chinese-armoury/

[243] (2019). *New 'Farseer' Malware Designed to SPY on Windows Users | Tripwire*. [Online]. Available: https://www.tripwire.com/state-of-security/new-farseer-malware-designed-to-spy-on-windows-users

[244] B. Barth. (Feb. 2019). *'Farseer' Backdoor Targets Windows Systems, Linked to 'Henbox' Malware*. SC Media. [Online]. Available: https://www.scmagazine.com/news/cybercrime/farseer-backdoor-targets-windows-systems-linked-to-henbox-malware

[245] McAfee. (Feb. 2019). *Malbus: Popular South Korean Bus App Series in Google Play Found Dropping Malware After 5 Years of Development*. McAfee Blog. [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/malbus-popular-south-korean-bus-app-series-in-google-play-found-dropping-malware-after-5-years-of-development/

[246] GoldSparrow. (Mar. 2020). *'Malbus' Remove Spyware & Malware With SpyHunter—EnigmaSoft*. [Online]. Available: https://www.enigmasoftware.com/malbus-removal/

[247] J. Carey. (Mar. 2020). *Android Warning: Three Dangerous Malware Strains You Need to Avoid*. [Online]. Available: https://www.express.co.uk/life-style/science-technology/1251889/Android-warning-dangerous-smartphone-malware-revealed

[248] K. Lu. (Jan. 2017). *Deep Analysis of Android Rootnik Malware Using Advanced Anti-debug and Anti-Hook, Part I: Debugging in the Scope of Native Layer*. [Online]. Available: https://www.fortinet.com/blog/threat-research/deep-analysis-of-android-rootnik-malware-using-advanced-anti-debug-and-anti-hook-part-i-debugging-in-the-scope-of-native-layer

[249] (Jul. 2019). *Cyber Swachhta Kendra: Android Rootnik Malware*. [Online]. Available: https://www.csk.gov.in/alerts/AndroidRootnik.html

[250] W. Hu. (Dec. 2015). *Rootnik Android Trojan Abuses Commercial Rooting Tool and Steals Private Information*. Unit 42. [Online]. Available: https://unit42.paloaltonetworks.com/rootnik-android-trojan-abuses-commercial-rooting-tool-and-steals-private-information/

[251] L. Stefanko. (Jun. 2018). *New Telegram-abusing Android Rat Discovered in the Wild*. WeLiveSecurity. [Online]. Available: https://www.welivesecurity.com/2018/06/18/new-telegram-abusing-android-rat/

[252] I. Arghire. (Jun. 2018). *Herorat Controls Infected Android Devices Via Telegram | Securityweek.com*. [Online]. Available: https://www.securityweek.com/herorat-controls-infected-android-devices-telegram

[253] N. Digital. (Jun. 2018). *Herorat Android Rat*. NHS Digit. [Online]. Available: https://digital.nhs.uk/cyber-alerts/2018/cc-2506

[254] P. Paganini. (Jun. 2018). *Herorat—A Totally New Telegram-based Android Rat is Spreading in the Wild*. Security Affairs. [Online]. Available: https://securityaffairs.co/wordpress/73669/malware/herorat-telegram-based-android-rat.html

[255] L. Wu. (Mar. 2018). *Hiddenminer Android Malware Can Cause Device Failure*. Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/research/18/c/monero-mining-hiddenminer-android-malware-can-potentially-cause-device-failure.html

[256] Waqas. (Mar. 2018). *Hiddenminer Android Monero Mining Malware Cause Device Failure*. [Online]. Available: https://www.hackread.com/hiddenminer-android-monero-mining-malware-cause-device-failure/

[257] P. Paganini. (Apr. 2018). *Hiddenminer Android Cryptocurrency Miner Can Brick Your Device*. Security Affairs. [Online]. Available: https://securityaffairs.co/wordpress/70968/malware/hiddenminer-android-miner.html

[258] (Apr. 2018). *New Monero Mining Android Malware Hiddenminer Can Cause Device Failure*. SecureReading. [Online]. Available: https://securereading.com/new-monero-mining-android-malware-hiddenminer-can-cause-device-failure/

[259] Z. Whittaker. (Nov. 2018). *Half a Million Android Users Tricked Into Downloading Malware From Google Play*. TechCrunch. [Online]. Available: https://techcrunch.com/2018/11/20/half-a-million-android-users-tricked-into-downloading-malware-from-google-play/

[260] L. Stefanko. (Nov. 2018). *Malicious Dev*. Twitter. [Online]. Available: https://twitter.com/LukasStefanko/status/1064507886896844800

[261] C. Castillo. (Oct. 2018). *Android/Timpdoor Turns Mobile Devices Into Hidden Proxies*. McAfee Blog. [Online]. Available: https://securingtomorrow.mcafee.com/mcafee-labs/android-timpdoor-turns-mobile-devices-into-hidden-proxies/

[262] N. Digital. (Oct. 2018). *Timpdoor Android Proxy Malware*. NHS Digita. [Online]. Available: https://digital.nhs.uk/cyber-alerts/2018/cc-2748

[263] D. Bisson. (Oct. 2018). *Cybercriminals Distribute Timpdoor Malware to Turn Android Devices Into Network Proxies*. Security Intelligence. [Online]. Available: https://securityintelligence.com/news/cybercriminals-distribute-timpdoor-malware-to-turn-android-devices-into-network-proxies/

[264] I. Arghire. (Oct. 2018). *'Timpdoor' Malware Turns Android Devices Into Proxies | Securityweek.com*. [Online]. Available: https://www.securityweek.com/timpdoor-malware-turns-android-devices-proxies

[265] H. Hiroaki, L. Wu, and L. Wu. (Apr. 2019). *Xloader Disguises As Android Apps, Has Fakespy Links*. [Online]. Available: https://www.trendmicro.com/en_us/research/19/d/new-version-of-xloader-that-disguises-as-android-apps-and-an-ios-profile-holds-new-links-to-fakespy.html

[266] T. Micro. (Apr. 2018). *Xtrat and Dunihi Backdoors Sent With Adwind in Spam*. Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/research/18/d/xloader-android-spyware-and-banking-trojan-distributed-via-dns-spoofing.html

[267] (Apr. 2019). *Xloader: A Deep Insight Into the Android Malware's Various Campaigns | Cyware Hacker News*. Cyware Labs. [Online]. Available: https://cyware.com/news/xloader-a-deep-insight-into-the-android-malwares-various-campaigns-462d6020

[268] L. Abrams. (May 2020). *Fake Valorant Mobile App Pushes Scams on Eager Gamers*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/fake-valorant-mobile-app-pushes-scams-on-eager-gamers/

[269] B. Toulas. (May 2022). *Fake Valorant Cheats on Youtube Infect You With Redline Stealer*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/fake-valorant-cheats-on-youtube-infect-you-with-redline-stealer/

[270] U. Kiguolis. (May 2020). *Video Games Exploited Again: Fake Valorant Mobile App Promoted Online*. [Online]. Available: https://www.2-spyware.com/video-games-exploited-again-fake-valorant-mobile-app-promoted-online

[271] S. Asif. (May 2020). *Fake Mobile Version of Valorant Game Spreading Malware*. [Online]. Available: https://www.hackread.com/fake-mobile-game-version-valorant-malware/

[272] D. Web. (May 2020). *Fraudsters Spread a Mobile Trojan Disguised As a Valorant Game*. [Online]. Available: https://news.drweb.com/show/?i=13838&lng=en&c=5

[273] (Sep. 2016). *Trojan for Android Android.xiny*. GBHackers On Security. [Online]. Available: https://gbhackers.com/torjan-android-android-xiny/

[274] D. Web. (Jan. 2020). *Yet Another [Almost] Non-removable Trojan for Android*. [Online]. Available: https://news.drweb.com/show/?i=13627

[275] GS. (Jan. 2020). *Android Non-Removable Android.Xiny Malware Infects System Process*. GBHackers On Security. [Online]. Available: https://gbhackers.com/android-xiny-malware/

[276] A. Yaswant. (Jun. 2020). *Zimperium Discovers Mobok Malware Left Undetected By AV Industry for Months*. Zimperium. [Online]. Available: https://www.zimperium.com/blog/zimperium-discovers-mobok-malware-left-undetected-by-mobile-av-industry-for-months/

[277] T. Seals. (Jun. 2019). *Mobok Malware Hides in Photo Editors on Google Play, Siphons Cash*. [Online]. Available: https://threatpost.com/mobok-malware-google-photo-editor/145932/

[278] BN. (Jul. 2018). *Hackers Selling Parasite Http Rat Via in Underground Market*. GBHackers On Security. [Online]. Available: https://gbhackers.com/hackers-selling-http-rat/

[279] E. Simion and A. Patrascu, "Applied cryptography and practical scenarios for cyber security defense," Polytech. Univ. Bucharest, Bucharest, Romania, Tech. Rep. 11, 2020.

[280] V. N. Cooper, H. Shahriar, and H. M. Haddad, "A survey of Android malware characterisitics and mitigation techniques," in *Proc. 11th Int. Conf. Inf. Technol., New Generat.*, Apr. 2014, pp. 327–332.

[281] (Jun. 2012). *Unified Protection, Secured Search Trust & Go!* [Online]. Available: http://blog.trustgo.com/mmarketpay/

[282] FortiGuard Labs. (Aug. 2013). *Android/Mmarketpay.A!Tr*. FortiGuard. [Online]. Available: https://www.fortiguard.com/encyclopedia/virus/4721252/android-mmarketpay-a-tr

[283] J. Russell. (Jul. 2012). *New Android Virus Lands on 100,000 Chinese Smartphones & 9 App Stores*. TNW | Asia. [Online]. Available: https://thenextweb.com/news/new-android-virus-mmarketpay-a-found-on-100000-chinese-smartphones-and-in-9-app-stores

[284] M. Botacin, H. Aghakhani, S. Ortolani, C. Kruegel, G. Vigna, D. Oliveira, P. L. D. Geus, and A. Grégio, "One size does not fit all: A longitudinal analysis of Brazilian financial malware," *ACM Trans. Privacy Secur.*, vol. 24, no. 2, pp. 1–31, May 2021.

[285] (2010). *CVE—CVE-2010–2568*. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568

[286] BetaFred. (Aug. 2010). *Microsoft Security Bulletin Ms10-046—Critical*. [Online]. Available: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-046

[287] R. Yu, "Ginmaster: A case study in Android malware," in *Proc. Virus Bull. Conf.*, 2013, pp. 92–104.

[288] *Trojan: Android/Ginmaster.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_ginmaster.shtml

[289] P. Johnson, P. Harris, K. Henderson, X. Yuan, and L. Yang, ''Intructional perspective: A course module on mobile malware,'' Univ. Nebraska-Lincoln, Lincoln, NE, USA, Tech. Rep. TR-UNL-CSE-2020-09, 2020.

[290] M. Huang, K. Bu, H. Wang, and K. Zhu, ''Reviving Android malware with DroidRide: And how not to,'' in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery (CyberC)*, Oct. 2016, pp. 27–34.

[291] *Trojan: Android/Androrat Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_androrat.shtml

[292] N. Collier. (Jan. 2017). *Mobile Menace Monday: Androrat Evolved | Malwarebytes Labs*. Malwarebytes. [Online]. Available: https://www.malwarebytes.com/blog/news/2017/01/mobile-menace-monday-androrat-evolved

[293] K. Threats. (Sep. 2010). *Kaspersky Threats—Lotoor*. [Online]. Available: https://threats.kaspersky.com/en/threat/Exploit.Linux.Lotoor/

[294] E. V. Radar. (Dec. 2012). *Android/exploit.lotoor.aa | Eset Virusradar*. [Online]. Available: https://www.virusradar.com/en/Android_Exploit.Lotoor.AA/description

[295] S.-H. Seo, A. Gupta, A. Mohamed Sallam, E. Bertino, and K. Yim, ''Detecting mobile malware threats to homeland security through static analysis,'' *J. Netw. Comput. Appl.*, vol. 38, pp. 43–53, Feb. 2014.

[296] D. Kortepeter. (Mar. 2017). *Android Malware Cloaks Itself As Fake Adobe Flash Download*. TechGenix. [Online]. Available: https://techgenix.com/android-malware-fake-flash/

[297] *Android/trojan.downloader | Malwarebytes Labs*. Malwarebytes. Accessed: Mar. 10, 2024. [Online]. Available: https://www.malwarebytes.com/blog/detections/android-trojan-downloader

[298] D. Palmer. (Feb. 2017). *This Android Trojan Pretends to be Flash Security Update but Downloads Additional Malware*. ZDNET. [Online]. Available: https://www.zdnet.com/article/this-android-trojan-pretends-to-be-flash-security-update-but-downloads-additional-malware/

[299] L. Stefanko. (Feb. 2017). *New Android Trojan Mimics User Clicks to Download Dangerous Malware*. WeLiveSecurity. [Online]. Available: https://www.welivesecurity.com/2017/02/14/new-android-trojan-mimics-user-clicks-download-dangerous-malware/

[300] S. B. Andarzian and B. T. Ladani, ''ISeCure,'' Sharif Univ. Technol., Tehran, Iran, Tech. Rep. SUT-CSE-2018-TR01, 2018.

[301] N. B. Abdullah, ''Android malware detection system using genetic programming,'' Ph.D. dissertation, Dept. Comput. Sci., Univ. York, York, U.K., 2019.

[302] bferrite. (May 2016). *Viking Horde: A New Type of Android Malware on Google Play*. Check Point Software. [Online]. Available: https://blog.checkpoint.com/2016/05/09/viking-horde-a-new-type-of-android-malware-on-google-play/

[303] R. Surendran, T. Thomas, and S. Emmanuel, ''A TAN based hybrid model for Android malware detection,'' *J. Inf. Secur. Appl.*, vol. 54, Oct. 2020, Art. no. 102483.

[304] *Trojan: Android/Boqx Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_boqx.shtml

[305] N. Buchka. (Aug. 2015). *Taking Root*. [Online]. Available: https://securelist.com/taking-root/71981/

[306] R. Unuchek. (Jun. 2017). *Ztorg: From Rooting to SMS*. [Online]. Available: https://securelist.com/ztorg-from-rooting-to-sms/78775/

[307] M. Koomen, L. L. Batina, and V. V. Moonsamy, ''Using power analysis to differentiate between malicious repackaged apps and clean apps,'' Radboud Univ., Nijmegen, The Netherlands, Tech. Rep. RU-SCS-TR-2018-05, 2018.

[308] L. Arsene. (May 2012). *Android Malware Report*. Hot for Security. [Online]. Available: https://www.bitdefender.com/blog/hotforsecurity/android-malware-report-april-2012

[309] (Dec. 2011). *Android/Fakedoc.A!Tr*. FortiGuard. [Online]. Available: https://www.fortiguard.com/encyclopedia/virus/3304615

[310] M. S. Intelligence. (May 2020). *Trojan: Androidos/Fakedoc.A Threat Description—Microsoft Security Intelligence*. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:AndroidOS/FakeDoc.A&ThreatID=2147755398

[311] L. De Carli, R. Torres, G. Modelo-Howard, A. Tongaonkar, and S. Jha, ''Botnet protocol inference in the presence of encrypted traffic,'' in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, May 2017, pp. 1–9.

[312] C. Chen. (Nov. 2012). *Fighting Malware and Spam: Ramnit Bot*. [Online]. Available: https://www.virusbulletin.com/virusbulletin/2012/11/ramnit-bot/

[313] A. Orozco. (Nov. 2014). *Infected Html Files Bundled in Android Apps | Malwarebytes Labs*. Malwarebytes. [Online]. Available: https://www.malwarebytes.com/blog/news/2014/11/infected-html-files-bundled-in-android-apps

[314] M. S. Intelligence. (May 2011). *Win32/ramnit Threat Description—Microsoft Security Intelligence*. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Ramnit

[315] NHS Digital. (Apr. 2017). *Ramnit Trojan*. [Online]. Available: https://digital.nhs.uk/cyber-alerts/2017/cc-1370

[316] C. Xiao. (Sep. 2016). *Dualtoy: New Windows Trojan Sideloads Risky Apps to Android and Ios Devices*. Unit42. [Online]. Available: https://unit42.paloaltonetworks.com/dualtoy-new-windows-trojan-sideloads-risky-apps-to-android-and-ios-devices/

[317] T. Spring. (Sep. 2016). *Dualtoy Windows Trojan Attacks Android, Ios Devices*. [Online]. Available: https://threatpost.com/dualtoy-windows-trojan-attacks-android-ios-devices/120556/

[318] NJCCIC. (Sep. 2017). *Dualtoy—Njccic Threat Profile*. [Online]. Available: https://www.cyber.nj.gov/threat-center/threat-profiles/ios-malware-variants/dualtoy

[319] S. News. (Sep. 2016). *Dualtoy Windows Trojan Covertly Sideloads Apps on Ios and Android Devices*. [Online]. Available: http://www.spamfighter.com/News-20490-DualToy-Windows-Trojan-Covertly-Sideloads-Apps-on-iOS-and-Android-Devices.htm

[320] G. Nellaivadivelu, F. Di Troia, and M. Stamp, ''Black box analysis of Android malware detectors,'' *Array*, vol. 6, Jul. 2020, Art. no. 100022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2590005620300072

[321] T. Bar and T. Lancaster. (Apr. 2017). *Targeted Attacks in the Middle East Using Kasperagent and Micropsia*. Unit 42. [Online]. Available: https://unit42.paloaltonetworks.com/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/

[322] E. Kovacs. (Apr. 2017). *Cyberspies Target Middle East With Windows, Android Malware | Securityweek.com*. [Online]. Available: https://www.securityweek.com/cyberspies-target-middle-east-windows-android-malware

[323] CagedTech. (Jul. 2019). *Secureupdate Removal Report*. Remove Spyware & Malware with SpyHunter—EnigmaSoft. [Online]. Available: https://www.enigmasoftware.com/secureupdate-removal/

[324] D. Brecht. (Aug. 2020). *Xhelper Malware: What It Is, How It Works and How to Prevent It | Malware Spotlight*. Infosec Resources. [Online]. Available: https://resources.infosecinstitute.com/topic/xhelper-malware-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/

[325] C. Cimpanu. (Feb. 2020). *There's Finally a Way to Remove Xhelper, the Unremovable Android Malware*. ZDNET. [Online]. Available: https://www.zdnet.com/article/theres-finally-a-way-to-remove-xhelper-the-unremovable-android-malware/

[326] N. Collier. (Feb. 2020). *Android Trojan Xhelper Uses Persistent Re-infection Tactics: Here's How to Remove | Malwarebytes Labs*. Malwarebytes. [Online]. Available: https://www.malwarebytes.com/blog/news/2020/02/new-variant-of-android-trojan-xhelper-reinfects-with-help-from-google-play

[327] N. Collier. (Aug. 2019). *Mobile Menace Monday: Android Trojan Raises Xhelper | Malwarebytes Labs*. Malwarebytes. [Online]. Available: https://www.malwarebytes.com/blog/news/2019/08/mobile-menace-monday-android-trojan-raises-xhelper

[328] Ashishb. (Apr. 2016). *Android-Malware/Break Bottleneck.Pdf At Master Ashishb/Android-Malware*. GitHub. [Online]. Available: https://github.com/ashishb/android-malware/blob/master/BreakBottleneck/Break%20Bottleneck.pdf

[329] (Feb. 2013). *Android/Claco.A!Tr*. FortiGuard. [Online]. Available: https://www.fortiguard.com/encyclopedia/virus/4585895/android-claco-a-tr

[330] M. Sanghavi. (Feb. 2013). *Android.Claco, Trojan.Picebot, Osx.Netweird and Osx.Getshell*. The Spiceworks Community. [Online]. Available: https://community.spiceworks.com/topic/299938-android-claco-trojan-picebot-osx-netweird-and-osx-getshell

[331] C. Paoli and 01/23/2014. (Jan. 2014). *Android Malware Infects Devices When Connected to Windows PCS*. Microsoft Certified Professional Magazine. [Online]. Available: https://mcpmag.com/articles/2014/01/23/android-malware-infects-devices.aspx?m=1

[332] (Jan. 2014). *Windows Malware Attempts to Infect Android Devices*. [Online]. Available: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=0543e340-a06b-4e55-8e18-b0a5823547ca&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

[333] *Trojan-Proxy: Android/Notcompatible.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan-proxy_android_notcompatible.shtml

[334] I. Paul. (May 2012). *Notcompatible Android Trojan: What You Need to Know*. PCWorld. [Online]. Available: https://www.pcworld.com/article/464236/notcompatible_android_trojan_what_you_need_to_know.html

[335] J. Gold. (Mar. 2013). *'notcompatible' Android Malware Rears Its Ugly Head, Again*. InfoWorld. [Online]. Available: https://www.infoworld.com/article/2613803/-notcompatible–android-malware-rears-its-ugly-head–again.html

[336] (Jul. 2014). *Android/Focobers.A*. FortiGuard. [Online]. Available: https://www.fortiguard.com/encyclopedia/virus/6286911

[337] P. Stancik. (Jul. 2017). *Malware Found Lurking Behind Every App At Alternative Android Store*. WeLiveSecurity. [Online]. Available: https://www.welivesecurity.com/2017/07/25/malware-found-lurking-behind-every-app-alternative-android-store/

[338] (Jul. 2017). *Android App Store*. GBHackers On Security. [Online]. Available: https://gbhackers.com/alternative-android-app-store-cepkutusu-com-spreading-malware/

[339] R. Moore-Colyer. (Jul. 2017). *Malware Discovered Hidden Behind Every App on an Alternative Android Play Store*. Silicon U.K. [Online]. Available: https://www.silicon.co.uk/security/android-malware-app-218543

[340] Root. (Jul. 2017). *Alternative Android App Store 'cepkutusu.com' Spreading Malware From Every Downloaded Apps | Mrhacker*. [Online]. Available: https://mrhacker.co/, 07 2017. https://mrhacker.co/malware/alternative-android-app-store-cepkutusu-com-spreading-malware-from-every-downloaded-apps

[341] *Trojan: Android/Fakeupdates Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_fakeupdates.shtml

[342] B. Abdo, B. Schondorfer, K. Hamdan, K. Goody, N. Klapprodt, and M. Bromiley. (Oct. 2019). *Head Fake: Tackling Disruptive Ransomware Attacks*. Mandiant. [Online]. Available: https://www.mandiant.com/resources/blog/head-fake-tackling-disruptive-ransomware-attacks

[343] M. Brian. (Jun. 2011). *Droidkungfu Android Malware Steals Data, Avoids Anti-virus Detection*. TNW | Google. [Online]. Available: https://thenextweb.com/news/droidkungfu-android-malware-steals-sensitive-data-avoids-anti-virus-detection

[344] K. Team. (Aug. 2019). *Malicious Android App Had More Than 100 Million Downloads in Google Play*. [Online]. Available: https://www.kaspersky.com/blog/camscanner-malicious-android-app/28156/

[345] S. T. R. Team. (Dec. 2019). *Malicious Android Apps Observed During Thanksgiving Season of 2019—Sonicwall*. Securitynews SonicWall. [Online]. Available: https://securitynews.sonicwall.com/xmlpost/malicious-android-apps-observed-during-thanksgiving-season-of-2019/

[346] A. Bilal. *Ahmet Bilal Can Profile*. Accessed: Mar. 10, 2024. [Online]. Available: http://eybisi.run/

[347] D. Eugenio. (Jul. 2019). *Operation Tripoli*. Check Point Research. [Online]. Available: https://research.checkpoint.com/2019/operation-tripoli/

[348] Cirt Team. *Operation Tripoli*. BGD e-GOV CIRT | Bangladesh e-Government Computer Incident Response Team. Accessed: Mar. 10, 2024. [Online]. Available: https://www.cirt.gov.bd/operation-tripoli/

[349] M. Y. Tee and M. Zhang. (Jul. 2019). *Unofficial Telegram App Secretly Loads Infinite Malicious Sites*. [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/unofficial-telegram-app-malicious-sites

[350] I. Golovin. (Jan. 2020). *Smartphone Shopaholic*. [Online]. Available: https://securelist.com/smartphone-shopaholic/95544/

[351] R. Kvn. (Jan. 2020). *'Shopper' Trojan Can Hijack Your Android Phone*. Deccan Herald. [Online]. Available: https://www.deccanherald.com/specials/shopper-trojan-can-hijack-your-android-phone-794104.html

[352] *Virustotal—Starswallpaper*. Accessed: Mar. 10, 2024. [Online]. Available: https://rb.gy/eveq7

[353] T. Bao. (Dec. 2018). *Android Wallpaper Apps Found Running Ad Fraud Scheme*. Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/research/18/l/android-wallpaper-apps-found-running-ad-fraud-scheme.html

[354] O. Topgul and E. Tatli, "The past and future of mobile malwares," in *Proc. 7th Int. Conf. Inf. Secur. Cryptol.* Berlin, Germany: Springer, 2014, pp. 1–7.

[355] Z. Xiao, Q. Dong, H. Zhang, and X. Jiang. (Jan. 2014). *Oldboot: The First Bootkit on Android*. [Online]. Available: https://blogs.360.net/post/oldboot-the-first-bootkit-on-android.html

[356] Cyware Labs. (Sep. 2018). *New Mirai Variant Fbot Found Wiping Out Cryptomining Malware From Android Devices | Cyware Hacker News*. [Online]. Available: https://cyware.com/news/new-mirai-variant-fbot-found-wiping-out-cryptomining-malware-from-android-devices-95fdb59c

[357] N. Digital. (Sep. 2018). *Fbot Botnet*. NHS Digit. [Online]. Available: https://digital.nhs.uk/cyber-alerts/2018/cc-2677

[358] C. Cimpanu. (2018). *Two Botnets are Fighting Over Control of Thousands of Unsecured Android Devices*. ZDNET. [Online]. Available: https://www.zdnet.com/article/two-botnets-are-fighting-over-control-of-thousands-of-unsecured-android-devices/

[359] H. Wang. (Sep. 2018). *Fbot, a Satori Related Botnet Using Blockchain Dns System*. 360 Netlab Blog—Network Security Research Lab at 360. [Online]. Available: https://blog.netlab.360.com/threat-alert-a-new-worm-fbot-cleaning-adbminer-is-using-a-blockchain-based-dns-en/

[360] R. Unuchek. (Jun. 2017). *Dvmap: The First Android Malware With Code Injection*. [Online]. Available: https://securelist.com/dvmap-the-first-android-malware-with-code-injection/78648/

[361] (May 2021). *Dvmap: Android Malware With a New Technique for Controlling Devices Appears on Google Play*. [Online]. Available: https://www.kaspersky.com/about/press-releases/2017_dvmap-android-malware-with-a-new-technique-for-controlling-devices-appears-on-google-play

[362] (Jun. 2017). *Cyber Swachhta Kendra: Dvmap-android Malware*. [Online]. Available: https://www.csk.gov.in/alerts/dvmap.html

[363] (Jun. 2017). *Android Malware 'Dvmap' Infects Devices Via Google Play Store—First Android Malware That Has Code Injection Capabilities | Red Piranha*. [Online]. Available: https://redpiranha.net/news/android-malware-dvmap-infects-devices-google-play-store-first-android-malware-has-code

[364] A. Eremin. (Jan. 2020). *The Faketoken Trojan Sends Out Offensive Texts*. [Online]. Available: https://www.kaspersky.com/blog/faketoken-trojan-sends-offensive-sms/32048/

[365] V. Chebyshev. (Aug. 2017). *Booking a Taxi for Faketoken*. [Online]. Available: https://securelist.com/booking-a-taxi-for-faketoken/81457/

[366] *Trojan: Android/Faketoken Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_faketoken.shtml

[367] K. Threats. (Aug. 2015). *Kaspersky Threats—Faketoken*. [Online]. Available: https://threats.kaspersky.com/en/threat/Trojan-Banker.AndroidOS.Faketoken/

[368] L. Christou. (Aug. 2017). *What is Faketoken, the Latest Android Malware Trying to Steal Your Bank Details?* Verdict. [Online]. Available: https://www.verdict.co.uk/faketoken-android-malware-bank-details/

[369] V. Kouliaridis, K. Barmpatsalou, G. Kambourakis, and S. Chen, "A survey on mobile malware detection techniques," *IEICE Trans. Inf. Syst.*, vol. 103, no. 2, pp. 204–211, 2020.

[370] A. Kadir and A. Fitriah, "A detection framework for Android financial malware," Ph.D. dissertation, Dept. Comput. Sci., Univ. New Brunswick, Fredericton, NB, Canada, 2018.

[371] M. Kumar. (Nov. 2017). *Bankbot Returns on Play Store—A Never Ending Android Malware Story*. Hacker News. [Online]. Available: https://thehackernews.com/2017/11/bankbot-android-malware.html

[372] D. Palmer. (Nov. 2017). *Bankbot Android Malware Sneaks Into the Google Play Store—For the Third Time*. ZDNet. [Online]. Available: https://www.zdnet.com/article/bankbot-android-malware-sneaks-into-the-google-play-store-for-the-third-time/

[373] T. Fabric. (Jun. 2018). *Mysterybot; A New Android Banking Trojan Ready for Android 7 and 8—Threatfabric*. [Online]. Available: https://www.threatfabric.com/blogs/mysterybot__a_new_android_banking_trojan_ready_for_android_7_and_8.html

[374] C. Cimpanu. (Jun. 2018). *New Mysterybot Android Malware Packs a Banking Trojan, Keylogger, and Ransomware*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/new-mysterybot-android-malware-packs-a-banking-trojan-keylogger-and-ransomware/

[375] P. Paganini. (Jun. 2018). *Mysterybot, a New Lokibot-linked Android Trojan Emerges*. Security Affairs. [Online]. Available: https://securityaffairs.co/wordpress/73551/malware/mysterybot-android-trojan.html

[376] D. Palmer. (Jun. 2018). *This New Android Malware Delivers Banking Trojan, Keylogger and Ransomware*. ZDNET. [Online]. Available: https://www.zdnet.com/article/this-new-android-malware-delivers-banking-trojan-keylogger-and-ransomware/

[377] T. Robinson. (Dec. 2015). *Slembunk Trojan Family Targeting Android Worldwide Banking App Users*. SC Media. [Online]. Available: https://www.scmagazine.com/news/architecture/slembunk-trojan-family-targeting-android-worldwide-banking-app-users

[378] J. Liu, D. Wu, and J. Xue, "Tdroid: Exposing app switching attacks in Android with control flow specialization," in *Proc. 33rd IEEE/ACM Int. Conf. Automated Softw. Eng. (ASE)*, Sep. 2018, pp. 236–247.

[379] B. Staff. (Jul. 2013). *Android.bankun: Bank Information Stealing Application on Your Android Device*. Webroot Blog. [Online]. Available: https://www.webroot.com/blog/2013/07/03/android-bankun-bank-information-stealing-application-on-your-android-device/

[380] N. Etaher, G. R. Weir, and M. Alazab, "From Zeus to zitmo: Trends in banking malware," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Oct. 2015, pp. 1386–1391.

[381] D. Maslennikov. (Oct. 2011). *Zeus-in-the-Mobile—Facts and Theories*. [Online]. Available: https://securelist.com/zeus-in-the-mobile-facts-and-theories/36424/

[382] Kaspersky. (Oct. 2011). *Teamwork: How the Zitmo Trojan Bypasses Online Banking Security*. [Online]. Available: https://www.kaspersky.com/about/press-releases/2011_teamwork-how-the-zitmo-trojan-bypasses-online-banking-security

[383] *Trojan: Android/Spitmo Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_spitmo.shtml

[384] J. Umawing. (Mar. 2022). *Escobar is the New Android Banking Trojan We've Met Before*. Malwarebytes. [Online]. Available: https://www.malwarebytes.com/blog/news/2022/03/escobar-is-the-new-android-banking-trojan-weve-met-before

[385] Cybleinc. (Mar. 2022). *Aberebot Returns As Escobar*. Cyble. [Online]. Available: https://blog.cyble.com/2022/03/10/aberebot-returns-as-escobar/

[386] Cybleinc. (Jul. 2021). *Aberebot on the Rise: New Banking Trojan Targeting Users Through Phishing*. Cyble. [Online]. Available: https://blog.cyble.com/2021/07/30/aberebot-on-the-rise-new-banking-trojan-targeting-users-through-phishing/

[387] B. Dhawan. (Mar. 2022). *Android Banking Trojan Returns in New Avatar: All You Need to Know About Escobar*. Financialexpress. [Online]. Available: https://www.financialexpress.com/industry/technology/android-banking-trojan-returns-in-new-avatar-all-you-need-to-know-about-escobar/2463797/

[388] CP Research. (Apr. 2022). *Mar. 2022's Most Wanted Malware: Easter Phishing Scams Help Emotet Assert Its Dominance*. Check Point Softw. [Online]. Available: https://www.checkpoint.com/press-releases/march-2022s-most-wanted-malware-easter-phishing-scams-help-emotet-assert-its-dominance/

[389] GoldSparrow. (Mar. 2021). *Alienbot Malware*. Remove Spyware & Malware with SpyHunter—EnigmaSoft. [Online]. Available: https://www.enigmasoftware.com/alienbotmalware-removal/

[390] Malpedia. *Alien (Malware Family)*. Accessed: Mar. 10, 2024. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/details/apk.alien

[391] B. Bracken. (Dec. 2021). *400 Banks' Customers Targeted With Anubis Trojan*. [Online]. Available: https://threatpost.com/400-banks-targeted-anubis-trojan/177038/

[392] B. Toulas. (Dec. 2021). *Anubis Android Malware Returns to Target 394 Financial Apps*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/anubis-android-malware-returns-to-target-394-financial-apps/

[393] J. Samhi and A. Bartel, "On the (in)effectiveness of static logic bomb detector for Android apps," 2021, *arXiv:2108.10381*.

[394] T. Trieu, "Android malware analysis," Univ. California, Berkeley, CA, USA, Tech. Rep. UCB-EECS-2021-03, 2021.

[395] B. Ning, "Analysis of the latest trojans on Android operating system," Ph.D. dissertation, Dept. Eng. Inf. Technol., Univ. Technol. Sydney (UTS), Sydney, NSW, Australia, 2021.

[396] T. Seals. (Aug. 2019). *Cerberus Enters the Android Malware Rental Scene*. [Online]. Available: https://threatpost.com/cerberus-android-malware-rental/147280/

[397] T. Meskauskas. (Jan. 2022). *Cerberus Banking Trojan (Android)*. [Online]. Available: https://www.pcrisk.com/removal-guides/17387-cerberus-banking-trojan-android

[398] Kaspersky. (Sep. 2020). *The Rise of Cerberus: Android Banking Malware is Available for Free in Underground Forums*. [Online]. Available: https://www.kaspersky.com/about/press-releases/2020_the-rise-of-cerberus

[399] L. Ali, F. Ali, P. Surendran, and B. Thomas, "The effects of cyber threats on Customer's behaviour in e-banking services," *Int. J. e-Educ., e-Bus., e-Manag. e-Learn.*, vol. 7, no. 1, pp. 70–78, 2017.

[400] M. Goncharov, "Russian underground 101," Trend Micro Incorporated, Tokyo, Japan, Tech. Rep. TM-TR-2012-01, 2012.

[401] AB Can. (Jul. 2019). *Android Malware Analysis: Dissecting Hydra Dropper—Pentest Blog*. [Online]. Available: https://pentest.blog/android-malware-analysis-dissecting-hydra-dropper/

[402] I. Bucur and A. P. Labs. (Mar. 2022). *Avira Labs Research Reveals Hydra Banking Trojan 2.0 Targeting a Wider Network of German and Austrian Banks*. [Online]. Available: https://www.avira.com/en/blog/avira-labs-research-reveals-hydra-banking-trojan-2-0

[403] Cybleinc. (Sep. 2021). *A New Variant of Hydra Banking Trojan Targeting European Banking Users*. Cyble. [Online]. Available: https://blog.cyble.com/2021/09/30/a-new-variant-of-hydra-banking-trojan-targeting-european-banking-users/

[404] T. Micro. (2016). *Fake Bank App Phishes Credentials, Locks Users Out Appendix*. [Online]. Available: http://documents.trendmicro.com/assets/pdf/appendix_fake-bank-app-phishes-credentials-locks-users-out.pdf

[405] (Nov. 2021). *Sharkbot: A New Generation of Android Trojans is Targeting Banks in Europe | Cleafy Labs*. [Online]. Available: https://www.cleafy.com/cleafy-labs/sharkbot-a-new-generation-of-android-trojan-is-targeting-banks-in-europe

[406] (2022). *Sharkbot: A 'New' Generation Android Banking Trojan Being Distributed on Google Play Store*. NCC Group Research. [Online]. Available: https://research.nccgroup.com/2022/03/03/sharkbot-a-new-generation-android-banking-trojan-being-distributed-on-google-play-store/

[407] T. Meskauskas. (Sep. 2022). *Sharkbot Malware (Android)*. [Online]. Available: https://www.pcrisk.com/removal-guides/22402-sharkbot-malware-android

[408] B. Toulas. (Mar. 2022). *Sharkbot Malware Hides as Android Antivirus in Google Play*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/sharkbot-malware-hides-as-android-antivirus-in-google-play/

[409] I. Arghire. (Apr. 2022). *Sharkbot Android Malware Continues Popping Up on Google Play | Securityweek.com*. [Online]. Available: https://www.securityweek.com/sharkbot-android-malware-continues-popping-google-play

[410] P. Wagenseil. (Mar. 2022). *This Nasty Android Malware Steals Your Passwords—What You Need to Know [Update]*. Tom's Guide. [Online]. Available: https://www.tomsguide.com/news/xenomorph-teabot-android-trojans

[411] T. Meskauskas. (Jul. 2022). *Teabot Malware (Android)*. [Online]. Available: https://www.pcrisk.com/removal-guides/20844-teabot-malware-android

[412] C. Osborne. (Mar. 2022). *Teabot Android Banking Trojan Continues Its Global Conquest With New Upgrades*. ZDNET. [Online]. Available: https://www.zdnet.com/article/teabot-android-banking-trojan-continues-its-global-conquest-with-new-upgrades/

[413] N. Nelson. (Mar. 2022). *Teabot Trojan Haunts Google Play Store, Again*. [Online]. Available: https://threatpost.com/teabot-trojan-haunts-google-play-store/178738/

[414] *Exobot Android Malware—IBM X-Force Collection*. Accessed: Mar. 10, 2024. [Online]. Available: https://exchange.xforce.ibmcloud.com/collection/ExoBot-Android-Malware-e112e0be1fefdcfbc013f6202a6fcaff

[415] T. Fabric. (Feb. 2017). *Exobot (Marcher)—Android Banking Trojan on the Rise—Threatfabric*. [Online]. Available: https://www.threatfabric.com/blogs/exobot_android_banking_trojan_on_the_rise.html

[416] K. Zurkus. (Jul. 2018). *Exobot Android Malware Targets Banking Apps*. Infosecurity Magazine. [Online]. Available: https://www.infosecurity-magazine.com/news/exabot-android-malware-targets/
[417] VirusTotal. *Virustotal—Comebot*. Accessed: Mar. 10, 2024. [Online]. Available: https://rb.gy/oyopm
[418] M. Ziad. (Aug. 2020). *Hatching—Automated Malware Analysis Solutions*. [Online]. Available: https://hatching.io/blog/triage-for-android/
[419] J. Piskácek. (May 2016). *Android Banker Trojan Preys on Credit Card Information*. [Online]. Available: https://blog.avast.com/android-banker-trojan-preys-on-credit-card-information
[420] C. Cimpanu. (May 2016). *Android Trojan Pesters Users for Administrator Rights Non-stop*. Softpedia. [Online]. Available: https://news.softpedia.com/news/android-trojan-pesters-users-for-administrator-rights-non-stop-503730.shtml
[421] E. Borel. (May 2020). *Diving Into Dsencrypt—Android Malware Analysis*. Testeur de Stylos. [Online]. Available: https://borelenzo.github.io/malware/2020/05/05/dsencrypt.html
[422] J. Zhai and J. Su. (Jun. 2014). *What Are You Doing—Dsencrypt Malware*. FireEye. [Online]. Available: https://www.fireeye.de/blog/threat-research/2014/06/what-are-you-doing-dsencrypt-malware.html
[423] P. Paganini. (Jul. 2016). *Android.Fakebank.B Inhibits Outgoing Calls to Bank Customer Services*. Security Affairs. [Online]. Available: https://securityaffairs.co/wordpress/49443/malware/fakebank-android-malware.html
[424] S. Meyer. (Mar. 2018). *Fakebank Android Malware Evolves Into Vishing Attack*. CPO Magazine. [Online]. Available: https://www.cpomagazine.com/cyber-security/fakebank-android-malware-evolves-into-vishing-attack/
[425] T. Seals. (Mar. 2018). *Android Banking Trojan Fakebank Adds Vishing Dimension*. Infosecurity Magazine. [Online]. Available: https://www.infosecurity-magazine.com/news/fakebank-android-banking-trojan/
[426] S. Aimoto and M. Zhang. (Mar. 2018). *New Fakebank Variant Intercepts Calls to Connect Banking Users to Scammers*. [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/fakebank-intercepts-calls-banks
[427] S. Desai. (2016). *Android Banker Malware Goes Social | Zscaler*. Zscaler. [Online]. Available: https://www.zscaler.com/blogs/security-research/android-banker-malware-goes-social
[428] STR Team. (Dec. 2018). *Dew18 Banker for Android Targets Korean Financial Institutions—Sonicwall*. [Online]. Available: https://securitynews.sonicwall.com/xmlpost/dew18-banker-for-android-targets-korean-financial-institutions/
[429] L. Stefanko. (Dec. 2018). *Android Trojan Steals Money From Paypal Accounts Even With 2fa on | Welivesecurity*. WeLiveSecurity. [Online]. Available: https://www.welivesecurity.com/2018/12/11/android-trojan-steals-money-paypal-accounts-2fa/
[430] C. Cimpanu. (Dec. 2018). *Android Malware Steals Money From Paypal Accounts While Users Watch Helpless*. ZDNET. [Online]. Available: https://www.zdnet.com/article/android-malware-steals-money-from-paypal-accounts-while-users-watch-helpless/
[431] I. Ilascu. (Dec. 2018). *Android Malware Tricks User to Log Into Paypal to Steal Funds*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/android-malware-tricks-user-to-log-into-paypal-to-steal-funds/
[432] G. Phillips. (Jan. 2019). *Warning: Android Malware Can Empty Your Paypal Account*. MUO. [Online]. Available: https://www.makeuseof.com/tag/android-malware-paypal-accounts/
[433] L. Stefanko. (Jun. 2019). *Malware Sidesteps Google Permissions Policy With New 2FA Bypass Technique*. WeLiveSecurity. [Online]. Available: https://www.welivesecurity.com/2019/06/17/malware-google-permissions-2fa-bypass/
[434] VirusTotal. *Virustotal—Coybolt*. Accessed: Mar. 10, 2024. [Online]. Available: https://rb.gy/olcuw
[435] T. Meskauskas. (Sep. 2021). *Basbanke Trojan (Android)*. [Online]. Available: https://www.pcrisk.com/removal-guides/17933-basbanke-trojan-android
[436] KL Global Research & Analysis Team. (Apr. 2019). *Basbanke: Trend-setting Brazilian Banking Trojan*. [Online]. Available: https://securelist.com/basbanke-trend-setting-brazilian-banking-trojan/90365/
[437] J. Karasek. (Jun. 2019). *Cryptocurrency-Mining Botnet Spreads Via Adb, Ssh*. Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/research/19/f/cryptocurrency-mining-botnet-arrives-through-adb-and-spreads-through-ssh.html
[438] L. Stefanko. *Lukas Stefanko*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.welivesecurity.com/author/lstefanko/
[439] V. Ventura. (Oct. 2019). *Gustuff Return, New Features for Victims*. Cisco Talos Blog. [Online]. Available: https://blog.talosintelligence.com/gustuffv2/
[440] V. Ventura. (Apr. 2019). *Gustuff Banking Botnet Targets Australia*. Cisco Talos Blog. [Online]. Available: https://blog.talosintelligence.com/gustuff-targets-australia/
[441] C. Cimpanu. (Apr. 2019). *Gustuff Android Banking Trojan Targets 125+ Banking, IM, and Cryptocurrency Apps*. ZDNet. [Online]. Available: https://www.zdnet.com/article/gustuff-android-banking-trojan-targets-100-banking-im-and-cryptocurrency-apps/
[442] T. Shishkova. (Jun. 2019). *Riltok Mobile Trojan: A Banker With Global Reach*. [Online]. Available: https://securelist.com/mobile-banker-riltok/91374/
[443] L. Stefanko. (Feb. 2019). *First Clipper Malware Discovered on Google Play*. WeLiveSecurity. [Online]. Available: https://www.welivesecurity.com/2019/02/08/first-clipper-malware-google-play/
[444] L. Stefanko. (May 2019). *Fake Cryptocurrency Apps Crop Up on Google Play as Bitcoin Price Rises*. WeLiveSecurity. [Online]. Available: https://www.welivesecurity.com/2019/05/23/fake-cryptocurrency-apps-google-play-bitcoin/
[445] S. Garcia, M. J. Erquiaga, and A. Shirokova, "Geost botnet. The story of the discovery of a new Android banking trojan from an OpSec error," ESET Res., Bratislava, Slovakia, Tech. Rep. ESET-TR-2019-05, 2019.
[446] T. Fabric. (Nov. 2019). *Ginp—A Malware Patchwork Borrowing From Anubis—Threatfabric*. [Online]. Available: https://www.threatfabric.com/blogs/ginp_a_malware_patchwork_borrowing_from_anubis.html
[447] A. Eremin. (Mar. 2020). *People Infected With Coronavirus Are All Around You, Says Ginp Trojan*. [Online]. Available: https://www.kaspersky.com/blog/ginp-trojan-coronavirus-finder/34338/
[448] (2019). *PDAFT PRODAFT*. Twitter. [Online]. Available: https://twitter.com/prodaft/status/1103646943299989506
[449] VirusTotal. *Virustotal—Covidmap*. Accessed: Mar. 10, 2024. [Online]. Available: https://t.ly/W7Q9L
[450] L. Stefanko. (2020). *Covid Map*. Twitter. [Online]. Available: https://twitter.com/lukasstefanko/status/1249979996585762818
[451] A. Ojah. (Jun. 2020). *Eventbot Malware a New Mobile Banking Trojan*. Quick Heal Blog | Latest computer security news, tips, and advice. [Online]. Available: https://blogs.quickheal.com/eventbot-malware-need-know-new-mobile-banking-trojan/
[452] C. Nocturnus. (Apr. 2020). *Eventbot: A New Mobile Banking Trojan is Born*. [Online]. Available: https://www.cybereason.com/blog/research/eventbot-a-new-mobile-banking-trojan-is-born
[453] Z. Whittaker. (Apr. 2020). *Meet Eventbot, a New Android Malware Targeting Banking Apps*. TechCrunch. [Online]. Available: https://techcrunch.com/2020/04/29/eventbot-android-malware-banking/
[454] GoldSparrow. (Jul. 2020). *Xerxes Malware*. Remove Spyware & Malware with SpyHunter—EnigmaSoft. [Online]. Available: https://www.enigmasoftware.com/xerxesmalware-removal/
[455] A. Reiger. (Jul. 2020). *New Blackrock Android Trojan is Successor to Xerxes, Lokibot*. Binary Defense. [Online]. Available: https://www.binarydefense.com/threat_watch/new-blackrock-android-trojan-is-successor-to-xerxes-lokibot/
[456] A. Ahmed. (Jul. 2020). *Researchers Discovered a New Android Malware That Steals Credentials From Banking Apps As Well As Shopping, Communication and Bus. Category Apps*. Digital Information World. [Online]. Available: https://www.digitalinformationworld.com/2020/07/researchers-discovered-a-new-android-malware-that-steals-credentials-from-almost-all-category-of-apps.html
[457] QATI Center. (May 2020). *Blackloan: A New Black Industry Organization Targeting Visa Users in China, Vietnam and Malaysia*. [Online]. Available: https://www.freebuf.com/articles/terminal/233411.html
[458] VirusTotal. *Virustotal—Blackloan*. Accessed: Mar. 10, 2024. [Online]. Available: https://t.ly/YuLrp
[459] @Cryptax. (May 2020). *'Reversing 'V-Alert COVID-19' Android/Bankbot'*. Medium. [Online]. Available: https://cryptax.medium.com/reversing-v-alert-covid-19-android-bankbot-8809c7389f13
[460] (Jul. 2020). *COVID-19 Cybersecurity Update—Global Travel Media*. [Online]. Available: https://eglobaltravelmedia.com.au/2020/07/22/covid-19-cybersecurity-update/

[461] VirusTotal. *Virustotal—Fakecoronatest*. Accessed: Mar. 10, 2024. [Online]. Available: https://t.ly/4EX18

[462] J. Stone. (Jun. 2020). *Hackers Use Fake Contact Tracing Apps in Attempt to Install Banking Malware on Android Phones*. [Online]. Available: https://www.cyberscoop.com/contact-tracing-hacking-security-anomali/

[463] A. Scroxton. (Jun. 2020). *Fake Contact-tracing Apps Delivering Banking Trojans*. ComputerWeekly. [Online]. Available: https://www.computerweekly.com/news/252484584/Fake-contact-tracing-apps-delivering-banking-trojans

[464] VirusTotal. *Virustotal—Fakecontact*. Accessed: Mar. 10, 2024. [Online]. Available: https://t.ly/7z8Xw

[465] (Mar. 2019). *Doctor Web: Android Banker Flexnet Uses Computer Games to Steal Money From Users*. [Online]. Available: https://news.drweb.com/show/?i=13146

[466] S. Tavor. (Nov. 2021). *Brazking Android Malware Upgraded and Targeting Brazilian Banks*. Security Intelligence. [Online]. Available: https://securityintelligence.com/posts/brazking-android-malware-upgraded-targeting-brazilian-banks/

[467] F. Assolini. (Nov. 2014). *Brazilian Trojan Bankers—Now on Your Android Play Store!*. [Online]. Available: https://securelist.com/brazilian-trojan-bankers-now-on-your-android-play-store/67661/

[468] R. Lakshmanan. (Dec. 2021). *New Android Malware Targeting Brazil's Itaú Unibanco Bank Customers*. Hacker News. [Online]. Available: https://thehackernews.com/2021/12/new-android-malware-targeting-brazils_27.html

[469] E. Roth. (Aug. 2020). *What is Blackrock Android Malware and How Can You Avoid It?* MUO. [Online]. Available: https://www.makeuseof.com/blackrock-android-malware/

[470] A. Bhatia. (Jul. 2020). *Explained: What is Blackrock Android Malware? Are You Vulnerable?* The Indian Express. [Online]. Available: https://indianexpress.com/article/explained/blackrock-android-malware-337-apps-data-privacy-6513223/

[471] C. Cimpanu. (Jul. 2020). *New Blackrock Android Malware Can Steal Passwords and Card Data From 337 Apps*. ZDNet. [Online]. Available: https://www.zdnet.com/article/new-blackrock-android-malware-can-steal-passwords-and-card-data-from-337-applications/

[472] T. Fabric. (Jul. 2020). *Blackrock—The Trojan That Wanted to Get Them All*. [Online]. Available: https://www.threatfabric.com/blogs/blackrock_the_trojan_that_wanted_to_get_them_all.html

[473] P. Tavares. (Mar. 2021). *Ghimob Trojan Banker: What It Is, How It Works and How to Prevent It | Malware Spotlight*. [Online]. Available: https://resources.infosecinstitute.com/topic/ghimob-trojan-banker-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/

[474] L. O'Donnell. (Nov. 2020). *Ghimob Android Banking Trojan Targets 153 Mobile Apps*. Accessed: Mar. 10, 2024. [Online]. Available: https://threatpost.com/ghimob-android-banking-trojan/161075/

[475] D. Bisson. (May 2021). *What is Ghimob Malware?* Security Intelligence. [Online]. Available: https://securityintelligence.com/articles/what-is-ghimob-malware/

[476] T. Meskauskas. (Jul. 2021). *How to Remove the Ghimob Trojan?* PC Risk. [Online]. Available: https://www.pcrisk.com/removal-guides/20840-ghimob-trojan-android

[477] B. Security. (2020). *Thiefbot—Bank Security*. Twitter. [Online]. Available: https://twitter.com/bank_security/status/1301147777423077376?lang=en

[478] Xunison. (2020). *Thiefbot—Xunison*. Twitter. [Online]. Available: https://twitter.com/XunisonOfficial/status/1300795851460280326

[479] PC Risk. *Thiefbot Malware (Android)—Malware Removal Instructions*. [Online]. Available: https://www.pcrisk.com/removal-guides/18783-thiefbot-malware-android

[480] Malwarebytes. *What is Trickbot?* Malwarebytes. Accessed: Mar. 10, 2024. [Online]. Available: https://www.malwarebytes.com/trickbot

[481] *Trojan.trickbot | Malwarebytes Labs*. Malwarebytes. Accessed: Mar. 10, 2024. [Online]. Available: https://www.malwarebytes.com/blog/detections/trojan-trickbot

[482] R. Lakshmanan. (Mar. 2020). *Trickbot Mobile App Bypasses 2-factor Authentication for Net Banking Services*. Hacker News. [Online]. Available: https://thehackernews.com/2020/03/trickbot-two-factor-mobile-malware.html

[483] I. Golovin. (Jun. 2019). *Not-so-dear Subscribers*. [Online]. Available: https://securelist.com/mobile-subscriptions/91211/

[484] M. Beltov. (Jan. 2017). *Android Charger Ransomware Identified*. Best Security Search. [Online]. Available: https://bestsecuritysearch.com/android-charger-ransomware-identified/

[485] H. N. Security. (Jan. 2017). *Charger Mobile Ransomware Steals Contacts and SMS Messages*. Help Net Security. [Online]. Available: https://www.helpnetsecurity.com/2017/01/24/charger-mobile-ransomware/

[486] Bferrite. (Jan. 2017). *Charger Malware Calls and Raises the Risk on Google Play*. Check Point Software. [Online]. Available: https://blog.checkpoint.com/2017/01/24/charger-malware/

[487] A. Martín, J. Hernandez-Castro, and D. Camacho, "An in-depth study of the jisut family of Android ransomware," *IEEE Access*, vol. 6, pp. 57205–57218, 2018.

[488] (2014). *Jisut Ransomware: Infomation, Encryption Type, Symptoms, Distribution Method—Vinransomware*. [Online]. Available: https://www.vinransomware.com/jisut-ransomware

[489] V. Radar. *Android/lockscreen.jisut.ep | Eset Virusradar*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.virusradar.com/en/Android_LockScreen.Jisut.EP/description

[490] *Android/Ransom.Koler*. Malwarebytes. Accessed: Mar. 10, 2024. [Online]. Available: https://www.malwarebytes.com/blog/detections/android-ransom-koler

[491] Kaspersky. (Jan. 2021). *Koler 'police' Mobile Ransomware*. [Online]. Available: https://www.kaspersky.com/resource-center/threats/koler-police-ransomware-virus

[492] R. Lipovský, L. Stefanko, and G. Branisa. (2016). *The Rise of Android Ransomware Document Version: 1.0 the Rise of Android Ransomware 2 Contents*. [Online]. Available: https://www.welivesecurity.com/wp-content/uploads/2016/02/Rise_of_Android_Ransomware.pdf

[493] S. Khandelwal. (Sep. 2015). *Lockerpin Ransomware Resets Pin and Permanently Locks Your Smartphones*. Hacker News. [Online]. Available: https://thehackernews.com/2015/09/android-lock-ransomware.html

[494] C. Osborne. (Sep. 2015). *Lockerpin Ransomware Steals Pins, Locks Android Devices Permenantly*. ZDNET. [Online]. Available: https://www.zdnet.com/article/lockerpin-ransomware-steals-pins-locks-android-devices-permenantly/

[495] M. Mimoso. (Jun. 2014). *Android Ransomware First to Encrypt Data on Mobile Devices*. [Online]. Available: https://threatpost.com/android-ransomware-first-to-encrypt-data-on-mobile-devices/106535/

[496] S. Malenkovich. (Jun. 2014). *Protecting Computers and Smartphones From Cryptolocker, Pletor Aka Simplocker and Other Ransomware*. [Online]. Available: https://www.kaspersky.com/blog/ransomware-outbreak/5045/

[497] DSTRTeam. (Sep. 2015). *Android Porndroid Ransomware With Updated Features*. [Online]. Available: https://securitynews.sonicwall.com/xmlpost/android-porndroid-ransomware-with-updated-features-september-25-2015/

[498] (2016). *Porndroid Ransomware: Infomation, Encryption Type, Symptoms, Distribution Method—Vinransomware*. [Online]. Available: https://www.vinransomware.com/porndroid-ransomware

[499] V. Gandhi. (2015). *Android Ransomware—Porn Droid | Zscaler*. Zscaler. [Online]. Available: https://www.zscaler.it/blogs/security-research/android-ransomware-porn-droid

[500] A. Blogs. (Jun. 2015). *New 'Porn Droid' Ransomware Hits Android New 'Porn Droid' Ransomware Hits Android*. [Online]. Available: https://now.avg.com/new-porn-droid-ransomware-hits-android

[501] P. Paganini. (Jun. 2014). *Simplocker, the First Android File-encrypting Ransomware*. Security Affairs. [Online]. Available: https://securityaffairs.co/wordpress/25504/malware/simplocker-first-android-ransomware.html

[502] V. Radar. *Android/Simplocker.A | Eset Virusradar*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.virusradar.com/en/Android_Simplocker.A/description

[503] *Trojan: Android/Slocker Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_slocker.shtml

[504] F. Quin. (Jul. 2017). *Slocker Mobile Ransomware Starts Mimicking Wannacry*. Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/research/17/g/slocker-mobile-ransomware-starts-mimicking-wannacry.html

[505] KnowBe4. *Svpeng Mobile Ransomware | Knowbe4*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.knowbe4.com/svpeng-mobile-ransomware

[506] K. Threats. (Aug. 2015). *Kaspersky Threats—Svpeng*. [Online]. Available: https://threats.kaspersky.com/en/threat/Trojan-Banker.AndroidOS.Svpeng/

[507] D. H. Kass. (Jul. 2019). *Wannalocker Malware Variant Combines Spyware, Rat, Banking Trojan*. MSSP Alert, [Online]. Available: https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/wannalocker-malware-variant/

[508] C. S. Kendra. (Jul. 2019). *Cyber Swachhta Kendra: Wannalocker/slocker Android Ransomware*. [Online]. Available: https://www.csk.gov.in/alerts/WannaLocker.html

[509] NJCCIC. (2016). *Fusob Njccic Threat Profile*. [Online]. Available: https://www.cyber.nj.gov/threat-center/threat-profiles/ios-malware-variants/fusob

[510] J. Snow. (Jun. 2016). *Ransomware on Mobile Devices: Knock-knock-block*. [Online]. Available: https://www.kaspersky.com/blog/mobile-ransomware-2016/12491/

[511] A. Ali-Gombe, S. Sudhakaran, A. Case, and G. G. Richard III, "Droidscraper: A tool for Android in-memory object recovery and reconstruction," in *Proc. 22nd Int. Symp. Res. Attacks, Intrusions Defenses*, 2019, pp. 547–559.

[512] O. Ahmed and O. Al-Dabbagh, "Ransomware detection system based on machine learning," *J. Educ. Sci.*, vol. 30, no. 5, pp. 86–102, Dec. 2021.

[513] C. Zheng, N. Dellarocca, N. Andronio, S. Zanero, and F. Maggi, "Greateatlon: Fast, static detection of mobile ransomware," in *Proc. Int. Conf. Secur. Privacy Commun. Syst.*, Springer, 2016, pp. 617–636.

[514] GoldSparrow. (Aug. 2015). *'Simplelocker' Ransomware—Remove Spyware & Malware With Spyhunter—Enigmasoft*. Remove Spyware & Malware with SpyHunter—EnigmaSoft. [Online]. Available: https://www.enigmasoftware.com/simplelockerransomware-removal/

[515] P. Wongsupa, "Deep learning for Android application ransomware," Chulalongkorn Univ., Bangkok, Thailand, Tech. Rep. CU-CSEC-TR-2018-01, 2018.

[516] M. Labs. *Mobile Ransomware | Malwarebytes Labs*. Malwarebytes. Accessed: Mar. 10, 2024. [Online]. Available: https://www.malwarebytes.com/blog/threats/mobile-ransomware

[517] S. Sjouwerman. (2012). *The Evolution of Mobile Ransomware*. [Online]. Available: https://blog.knowbe4.com/evolution-of-mobile-ransomware

[518] D. Web. (Nov. 2014). *Android.Locker.38.Origin—Dr.Web Malware Description Library*. [Online]. Available: https://vms.drweb.com/virus/?i=4240914

[519] A. Tufts. (Sep. 2014). *Beware of New Locker 38 Android Ransomware Which Locks Your Phone Behind a Pin*. [Online]. Available: https://oneclickroot.com/android-security/beware-of-new-locker-38-android-ransomware-which-locks-your-phone-behind-a-pin/

[520] T. S. John, T. Thomas, and M. M. Uddin, "A multifamily Android malware detection using deep autoencoder based feature extraction," in *Proc. 9th Int. Conf. Adv. Comput. (ICoAC)*, 2017, pp. 1–8.

[521] F. Ruiz. (Jul. 2017). *LeakerLocker: Mobile Ransomware Acts Without Encryption*. McAfee Blog. [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/leakerlocker-mobile-ransomware-acts-without-encryption/

[522] M. Samuels. (Jul. 2017). *New Leakerlocker Ransomware Puts Android Users at Risk*. Security Intelligence. [Online]. Available: https://securityintelligence.com/news/new-leakerlocker-ransomware-puts-android-users-at-risk/

[523] C. Cimpanu. (Jul. 2017). *Leakerlocker Ransomware Found in Two Apps on the Google Play Store*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/leakerlocker-ransomware-found-in-two-apps-on-the-google-play-store/

[524] A. Fraudwatch. (Jul. 2017). *Android Users: Beware the New Malware Leakerlocker*. Digital Brand Protection—FraudWatch. [Online]. Available: https://fraudwatch.com/android-users-beware-the-new-malware-leakerlocker/

[525] M. ATT&CK. (Oct. 2017). *Xbot, Software S0298 | Mitre Att&ck*. [Online]. Available: https://attack.mitre.org/software/S0298/

[526] C. Zheng, C. Xiao, and Z. Xu. (Feb. 2016). *New Android Trojan 'Xbot' Phishes Credit Cards and Bank Accounts, Encrypts Devices for Ransom*. Unit 42. [Online]. Available: https://unit42.paloaltonetworks.com/new-android-trojan-xbot-phishes-credit-cards-and-bank-accounts-encrypts-devices-for-ransom/

[527] M. Yang. (Feb. 2016). *Xbot Android Ransomware Can Steal Bank Info, Encrypt Devices*. Pindrop. [Online]. Available: https://www.pindrop.com/blog/xbot-android-ransomware-can-steal-bank-info-encrypt-devices

[528] J. Kirk. (Feb. 2016). *Newest Android Banking Trojan, Xbot, is Also Ransomware*. Computerworld. [Online]. Available: https://www.computerworld.com/article/3035497/newest-android-banking-trojan-xbot-is-also-ransomware.html

[529] D. Bisson. (Apr. 2020). *'Black Rose Lucy' Malware Botnet Returns With Ransomware Capabilities*. Security Intelligence. [Online]. Available: https://securityintelligence.com/news/black-rose-lucy-malware-botnet-returns-with-ransomware-capabilities/

[530] T. Spring. (Apr. 2020). *'Black Rose Lucy' is Back, Now Pushing Ransomware*. [Online]. Available: https://threatpost.com/black-rose-lucy-is-back-now-pushing-ransomware/155265/

[531] N. Goud. (Apr. 2020). *Black Rose Lucy Ransomware Attack on Android Devices*. Cybersecurity Insiders. [Online]. Available: https://www.cybersecurity-insiders.com/black-rose-lucy-ransomware-attack-on-android-devices/

[532] L. Hongzuo. (Apr. 2020). *Evolved Android Malware Black Rose Lucy Now Holds Smartphones Ransom*. [Online]. Available: https://www.hardwarezone.com.sg/tech-news-evolved-android-malware-ransomware-black-rose-lucy-smartphone

[533] F. He, B. Melnykov, and A. Polkovnichenko. (Sep. 2018). *Meet Black Rose Lucy, the Latest Russian Maas Botnet*. Check Point Research. [Online]. Available: https://research.checkpoint.com/2018/meet-black-rose-lucy-the-latest-russian-maas-botnet/

[534] GoldSparrow. (Apr. 2019). *Sauron Locker Ransomware*. Remove Spyware & Malware with SpyHunter—EnigmaSoft. [Online]. Available: https://www.enigmasoftware.com/sauronlockerransomware-removal/

[535] S. Remove. (Apr. 2019). *Sauron Locker Ransomware*. Remove Spyware & Malware with SpyHunter—EnigmaSoft. [Online]. Available: https://www.spywareremove.com/removesauronlockerrnsomware.html

[536] N. Digital. (Jun. 2020). *Crycryptor Ransomware*. NHS Digital. [Online]. Available: https://digital.nhs.uk/cyber-alerts/2020/cc-3523

[537] T. Shishkova. (Dec. 2077). *Ransomware Disguised As a Mobile Version of Cyberpunk 2077*. [Online]. Available: https://www.kaspersky.com/blog/cyberpunk-2077-ransomware/38196/

[538] A. Nair. (Dec. 2020). *Cyberpunk 2077 Android Malware*. [Online]. Available: https://medium.com/cyber-security-gectcr/cyberpunk-2077-android-malware-d58b50ab13f2

[539] L. Abrams. (Dec. 2020). *Ransomware Masquerades As Mobile Version of Cyberpunk 2077*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/ransomware-masquerades-as-mobile-version-of-cyberpunk-2077/

[540] Z. Zorz. (Mar. 2020). *Fake COVID-19 Tracker App Delivers Ransomware, Disinformation Abounds*. Help Net Security. [Online]. Available: https://www.helpnetsecurity.com/2020/03/16/fake-covid-19-tracker/

[541] R. KVN. (Mar. 2020). *Ransomware Alert: Hackers Using Fake Coronavirus Tracker App to Lock Android Phones*. Deccan Herald. [Online]. Available: https://www.deccanherald.com/specials/ransomware-alert-hackers-using-fake-coronavirus-tracker-app-to-lock-android-phones-814608.html

[542] A. Villas-Boas. (Mar. 2020). *A Fake Coronavirus Tracking App is Actually Ransomware That Threatens to Leak Social Media Accounts and Delete a Phone's Storage Unless a Victim Pays $100 in Bitcoin*. Business Insider. [Online]. Available: https://www.businessinsider.com/coronavirus-fake-app-ransomware-malware-bitcoin-android-demands-ransom-domaintools-2020-3

[543] MDTI Team. (Oct. 2020). *Sophisticated New Android Malware Marks the Latest Evolution of Mobile Ransomware*. Microsoft Security Blog. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2020/10/08/sophisticated-new-android-malware-marks-the-latest-evolution-of-mobile-ransomware/

[544] C. Cimpanu. (Oct. 2020). *Microsoft Warns of Android Ransomware That Activates When You Press the Home Button*. ZDNET. [Online]. Available: https://www.zdnet.com/article/microsoft-warns-of-android-ransomware-that-activates-when-you-press-the-home-button/

[545] *Riskware: Android/Mobiletx.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/sw-desc/riskware_android_mobiletx.shtml

[546] *Riskware: Android/Smsreg Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/sw-desc/riskware_android_smsreg.shtml

[547] M. A. Pinto. (Dec. 2020). *Is Tubemate Youtube Downloader Safe?* Malavida. [Online]. Available: https://www.malavida.com/en/soft/tubemate-youtube-downloader/android/q/is-tubemate-youtube-downloader-safe.html#gref

[548] (Mar. 2019). *Are You Using Tubemate for Downloading Videos? Beware of These Hidden Secretes!!!*. [Online]. Available: https://medium.com/janardhana.s/are-you-using-tubemate-for-downloading-videos-beware-of-these-hidden-secretes-baaa0a09e4b5

[549] B. Skies. (May 2017). *Tubemate 'Viru' Android Removal*. Virus Removal Guides. [Online]. Available: https://howtoremove.guide/tubemate-virus-android-remove/

[550] M. A. Rajab, L. Ballard, P. Marvrommatis, N. Provos, and X. Zhao, "The nocebo effect on the web: An analysis of fake anti-virus distribution," Google Inc., Mountain View, CA, USA, Tech. Rep. GOOGLE-TR-2010-02, 2010.

[551] KLG Global Research & Analysis Team. (Dec. 2013). *Trojan-fakeav*. [Online]. Available: https://encyclopedia.kaspersky.com/knowledge/trojan-fakeav/

[552] Y. Chen, W. Hu, X. Zhang, and Z. Xu. (Jul. 2018). *Hidden Devil in the Development Life Cycle: Google Play Apps Infected With Windows Executable Files*. Unit 42. [Online]. Available: https://unit42.paloaltonetworks.com/unit42-hidden-devil-development-life-cycle-google-play-apps-infected-windows-executable-files/

[553] J. Chandraiah. (Sep. 2019). *'Fleeceware' Apps Overcharge Users for Basic App Functionality*. Sophos News. [Online]. Available: https://news.sophos.com/en-us/2019/09/25/fleeceware-apps-overcharge-users-for-basic-app-functionality/

[554] A. Orozco. (Apr. 2014). *Scam Virus Shield App Top Paid App in Play Store | Malwarebytes Labs*. Malwarebytes. [Online]. Available: https://www.malwarebytes.com/blog/news/2014/04/scam-virus-shield-app-top-paid-app-in-play-store

[555] T. T. Gotora, K. Zvarevashe, and P. Nandan, "A survey on the security fight against ransomware and trojans in android," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 2, no. 5, pp. 4115–4123, 2014.

[556] E. Palermo. (May 2013). *Fake 'Android Defender' Promises Security, Delivers Malware*. NBC News. [Online]. Available: https://www.nbcnews.com/id/wbna52060727

[557] P. Ducklin. (May 2013). *Android Malware in Pictures—A Blow-by-blow Account of Mobile Scareware*. Naked Security. [Online]. Available: https://nakedsecurity.sophos.com/2013/05/31/android-malware-in-pictures-a-blow-by-blow-account-of-mobile-scareware/

[558] L. Stefanko. (May 2015). *Scareware: Fake Minecraft Apps Scare Hundreds of Thousands on Google Play*. WeLiveSecurity. [Online]. Available: https://www.welivesecurity.com/2015/05/22/scareware-fake-minecraft-apps-scare-hundreds-thousands-google-play/

[559] N. Kitson. (May 2015). *Minecraft Used As Cover to Push Android Scareware Apps on Google Play*. [Online]. Available: https://www.techcentral.ie/minecraft-used-as-cover-to-push-android-scareware-apps-on-google-play/

[560] A. Greenberg. (Jun. 2014). *Towelroot App Exploit That 'Roots' Android Devices Could Be Repackaged By Attackers*. SC Media. [Online]. Available: https://www.scmagazine.com/news/architecture/towelroot-app-exploit-that-roots-android-devices-could-be-repackaged-by-attackers

[561] J. Long. (Jun. 2014). *'Towelroot' Exploit Reveals Security Nightmare for Android*. GeekSided. [Online]. Available: https://geeksided.com/2014/06/16/towelroot-exploit-reveals-security-nightmare-android/

[562] M. Well. (Jul. 2018). *Why You Need to Use Towelroot Apk for Android*. Medium. [Online]. Available: https://medium.com/@yamee452/why-you-need-to-use-towelroot-apk-for-android-65f90878bad5

[563] P. Paganini. (Jun. 2014). *Towelroot, How to Root a Android Devices With a Click*. Security Affairs. [Online]. Available: https://securityaffairs.co/wordpress/25861/hacking/towelroot-root-android-devices-click.html

[564] M. Shipman. (Jun. 2011). *More Bad News: Two New Pieces of Android Malware—Plankton and Yzhcsms*. NC State News. [Online]. Available: https://news.ncsu.edu/2011/06/wms-android-plankton/

[565] *Trojan: Android/Plankton Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_plankton.shtml

[566] V. Svajcer. (Jun. 2011). *Plankton Malware Drifts Into Android Market*. Naked Security. [Online]. Available: https://nakedsecurity.sophos.com/2011/06/14/plankton-malware-drifts-into-android-market/

[567] K. Threats. (Sep. 2015). *Kaspersky Threats—Opfake*. [Online]. Available: https://threats.kaspersky.com/en/threat/Trojan-SMS.AndroidOS.Opfake/

[568] *Trojan: Android/Opfake Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_opfake.shtml

[569] *Trojan: Android/Beanbot.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_beanbot.shtml

[570] R. Nigam, "A timeline of mobile botnets," *Virus Bull., March*, vol. 1630, pp. 1–15, Mar. 2015.

[571] (Aug. 2012). *AndROID/fAKEMART.a!tR*. FortiGuard. [Online]. Available: https://www.fortiguard.com/encyclopedia/mobile/4117117

[572] ThreatSolutions. (Dec. 2011). *Trojan: Android/Smstado.A and Trojan: Android/Fakenotify.A*. [Online]. Available: https://archive.f-secure.com/weblog/archives/00002278.html

[573] *Trojan: Android/Fakenotify Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_fakenotify.shtml

[574] *Trojan: Android/Jifake Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_jifake.shtml

[575] NortonLifeLock. *Mazar Bot Malware Invades and Erases Android Devices*. Accessed: Mar. 10, 2024. [Online]. Available: https://us.norton.com/blog/emerging-threats/mazar-bot-malware-invades-and-erases-android-devices

[576] *Trojan: Android/Nandrobox.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_nandrobox.shtml

[577] *Trojan: Android/Zsone.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_zsone.shtml

[578] V. Kouliaridis, K. Barmpatsalou, G. Kambourakis, and G. Wang, "Mal-warehouse: A data collection-as-a-service of mobile malware behavioral patterns," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Advanced Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Mar. 2018, pp. 1503–1508.

[579] E. Borel. (May 2020). *Diving Into Rumms—Android Malware Analysis*. Testeur de Stylos. [Online]. Available: https://borelenzo.github.io/malware/2020/05/05/rumms.html

[580] U. Amir. (Apr. 2016). *New Android Malware Rumms Targeting Users Through Smishing*. Hackread. [Online]. Available: https://www.hackread.com/new-android-smishing-malware-hits-users/

[581] *Don't Let These Top 10 Android Threats Infect Your Mobile World | F-secure Press Room*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/en/press/p/dont-let-these-top-10-android-threats-infect-your-mobile-world

[582] zLabs. (Mar. 2016). *Taking a Deeper Dive Into Leech: One of the Three Families of Malware Dubbed As Triada*. Zimperium. [Online]. Available: https://www.zimperium.com/blog/taking-a-deeper-dive-into-leech-one-of-the-three-families-of-malware-dubbed-as-triada/

[583] T.-P. Doan, L. Nguyen-Vu, H.-H. Nguyen, and S. Jung, "An empirical study on Android malware behavior signature extraction," *Res. Briefs Inf. Commun. Technol. Evol.*, vol. 5, pp. 102–110, Nov. 2019.

[584] O. Olukoya, L. Mackenzie, and I. Omoronyia, "Towards using unstructured user input request for malware detection," *Comput. Secur.*, vol. 93, Jun. 2020, Art. no. 101783.

[585] K. Threats. (Jun. 2016). *Kaspersky Threats—Erop*. [Online]. Available: https://threats.kaspersky.com/en/threat/Trojan-SMS.AndroidOS.Erop/

[586] F. Chytrý. (Dec. 2014). *Mobile Advertising Firms Spread Malware By Posing As Official Google Play Apps*. [Online]. Available: https://blog.avast.com/2014/12/12/mobile-advertising-firms-spread-malware-by-posing-as-official-google-play-apps/

[587] L. Zhang, V. L. L. Thing, and Y. Cheng, "A scalable and extensible framework for Android malware detection and family attribution," *Comput. Secur.*, vol. 80, pp. 120–133, Jan. 2019.

[588] J.-W. Jang, J. Yun, A. Mohaisen, J. Woo, and H. K. Kim, "Detecting and classifying method based on similarity matching of Android malware behavior with profile," *SpringerPlus*, vol. 5, no. 1, pp. 1–23, Dec. 2016.

[589] A. Goujon and P. Ramos. (2011). *Boxer SMS Trojan Android/trojansms.boxer.aa*. [Online]. Available: https://www.welivesecurity.com/wp-content/uploads/200x/SMS_Trojan_Whitepaper.pdf

[590] E. Virusradar. (2011). *Android/Trojansms.Boxer | Eset Virusradar*. [Online]. Available: https://www.virusradar.com/en/Android_TrojanSMS.Boxer/description

[591] *Trojan: Android/Boxer Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_boxer.shtml

[592] D. Emm, M. Garnaeva, A. Ivanov, D. Makrushin, and R. Unuchek, "It threat evolution in Q2 2015," Kaspersky Lab, Moscow, Russia, Tech. Rep. KLAB-TR-2015-Q2, 2015.

[593] K. Threats. (Sep. 2015). *Kaspersky Threats—Stealer*. [Online]. Available: https://threats.kaspersky.com/en/threat/Trojan-SMS.AndroidOS.Stealer/

[594] V. Chebyshev. (Apr. 2014). *New Threat: Trojan-Sms.Androidos.Stealer.A*. [Online]. Available: https://securelist.com/new-threat-trojan-sms-androidos-stealer-a/59384/

[595] *Trojan: Android/Vidro.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_vidro.shtml

[596] D. Maslennikov. (Aug. 2012). *Vidro: How Deep and Mobile is the Rabbit Hole?* [Online]. Available: https://securelist.com/vidro-how-deep-and-mobile-is-the-rabbit-hole/33654/

[597] *Trojan: Android/Fakeplayer.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_fakeplayer.shtml

[598] M. S. Intelligence. (Aug. 2010). *Trojan: Androidos/Fakeplayer.A*. Microsoft. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan: AndroidOS/Fakeplayer.A

[599] F. Wei, X. Lin, X. Ou, T. Chen, and X. Zhang, "JN-SAF: Precise and efficient NDK/JNI-aware inter-language static analysis framework for security vetting of Android applications with native code," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2018, pp. 1137–1150.

[600] *Trojan: Android/Tesbo.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_tesbo.shtml

[601] M. S. Intelligence. (Apr. 2011). *Trojanspy: Androidos/Lanucher.A*. Microsoft. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy%3AAndroidOS%2FLanucher.A

[602] A. Calleja, A. Martín, H. D. Menéndez, J. Tapiador, and D. Clark, "Picking on the family: Disrupting Android malware triage by forcing misclassification," *Exp. Syst. Appl.*, vol. 95, pp. 113–126, Apr. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417417307881

[603] R. P. Pinheiro, S. M. Lima, D. M. Souza, S. H. Silva, P. G. Lopes, R. D. de Lima, J. R. de Oliveira, T. D. A. Monteiro, S. M. Fernandes, and E. D. Q. Albuquerque, "Antivirus applied to JAR malware detection based on runtime behaviors," *Sci. Rep.*, vol. 12, no. 1, pp. 1–17, Feb. 2022.

[604] *Trojan: Android/Fakelogo Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_fakelogo.shtml

[605] *Trojan: Android/Yzhcsms.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_yzhcsms.shtml

[606] M. Bidar. (Aug. 2021). *New Malware Seizes on COVID-19 to Target Android Users*. [Online]. Available: https://www.cbsnews.com/news/tanglebot-android-malware-covid-19/

[607] L. Whitney. (Aug. 2021). *New SMS Malware Targets Android Users Through Fake Covid Messages*. TechRepublic. [Online]. Available: https://www.techrepublic.com/article/new-sms-malware-targets-android-users-through-fake-covid-messages/

[608] S. Magazine. (Aug. 2021). *New Malware Uses COVID-19 Lure to Target Android Users | Security Magazine*. [Online]. Available: https://www.securitymagazine.com/articles/96195-new-malware-uses-covid-19-lure-to-target-android-users

[609] VirusTotal. *Virustotal—Android.troj.at_fonefee.b*. Accessed: Mar. 10, 2024. [Online]. Available: https://t.ly/NCpr3

[610] F. Broderick. (Mar. 2015). *More Apps in Google Play Subscribing to SMS Premium Numbers: Jssmsers*. Think Big. [Online]. Available: https://business.blogthinkbig.com/more-apps-in-google-play-subscribing-to_23/

[611] R. Lipovsky. (Apr. 2014). *Android Malware Worm Catches Unwary Users*. WeLiveSecurity. [Online]. Available: https://www.welivesecurity.com/2014/04/30/android-sms-malware-catches-unwary-users/

[612] *Worm: Android/Samsapo Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/worm_android_samsapo.shtml

[613] D. Palmer. (Jan. 2018). *Android Security: First Kotlin-Based Malware Found in Google Play Store*. ZDNET. [Online]. Available: https://www.zdnet.com/article/android-security-first-kotlin-based-malware-found-in-google-play-store/

[614] L. Wu. (Jan. 2018). *First Kotlin-Developed Malicious App Spotted*. Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/research/18/a/first-kotlin-developed-malicious-app-signs-users-premium-sms-services.html

[615] Cyber Inject. (Jan. 2018). *This is the First Android Malware Written in Kotlin*. Medium. [Online]. Available: https://medium.com/@itscyberinject/this-is-the-first-android-malware-written-in-kotlin-4f0abc8b2662

[616] C. Cimpanu. (Jan. 2018). *First Android Malware Developed in Kotlin Programming Language Discovered*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/first-android-malware-developed-in-kotlin-programming-language-discovered/

[617] B. Toulas. (Feb. 2022). *Roaming Mantis Android Malware Campaign Sets Sights on Europe*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/roaming-mantis-android-malware-campaign-sets-sights-on-europe/

[618] S. Ishimaru. (Feb. 2022). *Roaming Mantis Reaches Europe*. [Online]. Available: https://securelist.com/roaming-mantis-reaches-europe/105596/

[619] R. Lakshmanan. (Feb. 2022). *'Roaming Mantis' Android Malware Targeting Europeans Via Smishing Campaigns*. Hacker News. [Online]. Available: https://thehackernews.com/2022/02/roaming-mantis-android-malware.html

[620] Z. Chen. (May 2021). *Roaming Mantis Amplifies Smishing Campaign With Os-specific Android Malware*. McAfee Blog. [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/roaming-mantis-amplifies-smishing-campaign-with-os-specific-android-malware/

[621] VirusTotal. *Virustotal—Premiumratesms*. Accessed: Mar. 10, 2024. [Online]. Available: https://rb.gy/83epd

[622] *Trojan: Android/Mseg Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_mseg.shtml

[623] (Aug. 2011). *Android/Roguesppush.A!tr*. FortiGuard. [Online]. Available: https://www.fortiguard.com/encyclopedia/virus/2971291/android-roguesppush-a-tr

[624] M. S. Intelligence. (Aug. 2011). *Trojan: Androidos/Shastrosms.A Threat Description—Microsoft Security Intelligence*. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan%3AAndroidOS%2FShastroSms.A

[625] *Trojan: Android/Kmin Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_kmin.shtml

[626] S. Ma, Z. Tang, Q. Xiao, J. Liu, T. T. Duong, X. Lin, and H. Zhu, "Detecting GPS information leakage in Android applications," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 826–831.

[627] L. Xue, C. Qian, H. Zhou, X. Luo, Y. Zhou, Y. Shao, and A. T. S. Chan, "NDroid: Toward tracking information flows across multiple Android contexts," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 814–828, Mar. 2019.

[628] *Monitoring-Tool: Android/Spybubble.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/sw-desc/monitoring-tool_android_spybubble.shtml

[629] (Jul. 2020). *In Depth Analysis of Darkshades. A Rat Infecting Android Devices*. [Online]. Available: https://www.avira.com/en/blog/in-depth-analysis-of-darkshades-a-rat-infecting-android-devices

[630] Sophos. (Jul. 2013). *Detailed Analysis—Andr/Mtk-A—Viruses and Spyware—Advanced Network Threat Protection | Atp From Targeted Malware Attacks and Persistent Threats | Sophos.com—Threat Center*. [Online]. Available: https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Andr MTK-A/detailed-analysis

[631] J. Jung, C. Jeon, M. Wolotsky, I. Yun, and T. Kim, "AVPASS: Automatically bypassing Android malware detection system," Georgia Inst. Technol., Atlanta, GA, USA, Tech. Rep. GT-CS-TR-2017-05, 2017.

[632] *Trojan: Android/Avpass.C Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_avpass_c.shtml

[633] T. Gaffney, "Following in the footsteps of windows: How Android malware development is looking very familiar," *Netw. Secur.*, vol. 2013, no. 8, pp. 7–10, Aug. 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1353485813700928

[634] McAfee. (Mar. 2013). *Android Malware Goes Bollywood*. McAfee Blog. [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/android-malware-goes-bollywood/

[635] TaintBench. (Jul. 2021). *Taintbench/Faketaobao*. GitHub. [Online]. Available: https://github.com/TaintBench/faketaobao

[636] J. Minor. (Jan. 2016). *Mobile Threat Monday: Fake Shopping App is So Real It's Scary*. PCMAG. [Online]. Available: https://www.pcmag.com/news/mobile-threat-monday-fake-shopping-app-is-so-real-its-scary

[637] M. Chua and V. Balachandran, "Effectiveness of Android obfuscation on evading anti-malware," in *Proc. 8th ACM Conf. Data Appl. Secur. Privacy*, Mar. 2018, pp. 143–145.

[638] M. S. Intelligence. (Dec. 2020). *Trojanspy: Androidos/VMVOL!RFN*. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy:AndroidOS/Vmvol!rfn&threatId=-2147196657

[639] M. Marquis-Boire, B. Marzcak, and C. Guarnieri, "The smartphone who loved me: Finfisher goes mobile," Citizen Lab, Munk School Global Affairs, Univ. Toronto, Toronto, ON, Canada, Tech. Rep. CL-TR-2012-02, 2012.

[640] W. R. Marczak, J. Scott-Railton, M. Marquis-Boire, and V. Paxson, "When governments hack opponents: A look at actors and technology," in *Proc. 23rd USENIX Secur. Symp.*, 2014, pp. 511–525.

[641] *New Finspy Ios and Android Implants Revealed ITW*, SecureList, KL Global Res. & Anal. Team AMR, Moscow, Russia, Jul. 2019.

[642] P. Shoshin. (Jul. 2019). *Finspy—Commercial Spyware*. [Online]. Available: https://www.kaspersky.com/blog/finspy-commercial-spyware/27606/

[643] S. Neuner, V. van der Veen, M. Lindorfer, M. Huber, G. Merzdovnik, M. Mulazzani, and E. Weippl, "Enter sandbox: Android sandbox comparison," 2014, *arXiv:1410.7749*.

[644] S. Mansfield-Devine, "Android malware and mitigations," *Netw. Secur.*, vol. 2012, no. 11, pp. 12–20, Nov. 2012.

[645] M. Lennon. (Aug. 2012). *Resilient 'Smszombie' Infects 500,000 Android Users in China | Securityweek.com*. [Online]. Available: https://www.securityweek.com/resilient-smszombie-infects-500000-android-users-china

[646] A. Shetty. (Aug. 2012). *Aggressive Android Trojan Smszombie Detected in China-Technology News, Firstpost*. [Online]. Available: https://www.firstpost.com/tech/news-analysis/aggressive-android-trojan-smszombie-detected-in-china-3606313.html

[647] *Trojan: Android/Smszombie.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_smszombie.shtml

[648] B. Donohue. (Sep. 2011). *Droidsheep Android App Hijacks Sessions in One Click, Developer Meant Well*. [Online]. Available: https://threatpost.com/droidsheep-android-app-hijacks-sessions-one-click-developer-meant-well-092211/75680/

[649] *Monitoring-Tool: Android/Accutrack.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/sw-desc/monitoring-tool_android_accutrack.shtml

[650] MS Intelligence. (Aug. 2011). *Trojanspy: Androidos/Cosha.A*. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy:AndroidOS/Cosha.A

[651] MS Intelligence. (Aug. 2011). *Trojanspy: Androidos/Nickispy.A*. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy:AndroidOS/Nickispy.A

[652] *Trojan: Android/Nickispy.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_nickispy.shtml

[653] Kaspersky. (Sep. 2011). *Malware in August: One Year After the First Android Malware Emerged, & the Clones of Zeus*. [Online]. Available: https://www.kaspersky.com/about/press-releases/2011_malware-in-august-one-year-after-the-first-android-malware-emerged–the-clones-of-zeus

[654] *Trojan: Android/Vdloader.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_vdloader.shtml

[655] E. V. Radar. (Apr. 2012). *Android/Dougalek.A | Eset Virusradar*. [Online]. Available: https://www.virusradar.com/Android_Dougalek.A/description

[656] *Trojan-Spy: Android/Smforw Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan-spy_android_smforw.shtml

[657] J. Siegal. (Mar. 2022). *100,000 Android Users Downloaded a Malware App That Steals Facebook Accounts*. BGR. [Online]. Available: https://bgr.com/tech/100000-android-users-downloaded-a-malware-app-that-steals-facebook-accounts/

[658] M. Labs. *Android/Trojan.Spy.Facestealer*. Malwarebytes. Accessed: Mar. 10, 2024. [Online]. Available: https://www.malwarebytes.com/blog/detections/android-trojan-spy-facestealer

[659] T. Seals. (Mar. 2022). *Facestealer Trojan Hidden in Google Play Plunders Facebook Accounts*. [Online]. Available: https://threatpost.com/facestealer-trojan-google-play-facebook/179015/

[660] Mezo. (Nov. 2021). *Fakecop Android Malware*. Remove Spyware & Malware with SpyHunter—EnigmaSoft. [Online]. Available: https://www.enigmasoftware.com/fakecopandroidmalware-removal/

[661] Cybleinc. (Oct. 2021). *New Variant of Fakecop Targeting Users From Japan*. [Online]. Available: https://blog.cyble.com/2021/10/28/new-variant-of-fakecop-targeting-users-from-japan/

[662] B. Toulas. (Oct. 2021). *Android Spyware Spreading As Antivirus Software in Japan*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/android-spyware-spreading-as-antivirus-software-in-japan/

[663] (Oct. 2019). *Android/Fakecop.D!Tr.Spy*. FortiGuard. [Online]. Available: https://www.fortiguard.com/encyclopedia/virus/8137645

[664] J. Bellizzi, M. Vella, C. Colombo, and J. Hernandez-Castro, "Responding to targeted stealthy attacks on Android using timely-captured memory dumps," *IEEE Access*, vol. 10, pp. 35172–35218, 2022.

[665] G. Aaron, L. Chapin, D. Piscitello, and C. Strutt, "Malware landscape 2021," Interisle Consulting Group, Boston, MA, USA, Tech. Rep. ICG-TR-2021-01, 2021.

[666] HS Today. (Jun. 2022). *Flubot Spyware Infecting Android Phones is Taken Down in International Operation—Hs Today*. [Online]. Available: https://www.hstoday.us/subject-matter-areas/cybersecurity/flubot-spyware-infecting-android-phones-is-taken-down-in-international-operation/

[667] V. Sharma. (Jun. 2022). *Flubot Malware: All You Need to Know and What to Do If Your Device is Infected*. [Online]. Available: https://odishatv.in/news/technology/flubot-malware-all-you-need-to-know-and-what-to-do-if-your-device-is-infected-178162

[668] A. Chawla, "Pegasus spyware—A privacy killer," Int. Inst. Inf. Technol. (IIIT), Hyderabad, India, Tech. Rep. IIIT-TR-2021-07, 2021.

[669] J. Scott-Railton, B. Marczak, S. Anstis, B. A. Razzak, M. Crete-Nishihata, and R. Deibert, "Reckless vii: Wife of journalist slain in cartel-linked killing targeted with NSO group's spyware," Citizen Lab, Munk School Global Affairs, Univ. Toronto, Toronto, ON, Canada, Tech. Rep. CL-TR-2019-01, 2019.

[670] G. Sims. (May 2022). *What is Pegasus and How is It Used for Spying?* Android Authority. [Online]. Available: https://www.androidauthority.com/pegasus-spyware-1646458/

[671] C. Raiu. (Feb. 2022). *How to Protect From Pegasus and Other Advanced Spyware*. [Online]. Available: https://www.kaspersky.com/blog/how-to-protect-from-pegasus-spyware/43453/

[672] D. Pegg and S. Cutler. (Jul. 2021). *What is Pegasus Spyware and How Does It Hack Phones?* Guardian. [Online]. Available: https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones

[673] *Trojan: Android/Smstealer Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_smstealer.shtml

[674] K. Threats. (Sep. 2015). *Kaspersky Threats—Smsthief*. [Online]. Available: https://threats.kaspersky.com/en/threat/Trojan-Spy.AndroidOS.SmsThief/

[675] W. Hu, C. Zheng, and Z. Xu. (Jul. 2017). *Spydealer: Android Trojan Spying on More Than 40 Apps*. Unit 42. [Online]. Available: https://unit42.paloaltonetworks.com/unit42-spydealer-android-trojan-spying-40-apps/

[676] *What is Spydealer—Zemana*. Accessed: Mar. 10, 2024. [Online]. Available: https://zemana.com/us/removal-guide/spydealer-android-malware.html

[677] I. Arghire. (Jul. 2017). *Spydealer Malware Steals Private Data From Popular Android Apps | Securityweek.com*. [Online]. Available: https://www.securityweek.com/spydealer-malware-steals-private-data-popular-android-apps

[678] A. D. Blog. (Apr. 2017). *An Investigation of Chrysaor Malware on Android*. Android Developers Blog. [Online]. Available: https://android-developers.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html

[679] P. Security. (Jul. 2017). *Chrysaor: The Most Dangerous Spyware Tool Also Affects Android Devices*. Panda Secur. Mediacenter. [Online]. Available: https://www.pandasecurity.com/en/mediacenter/security/chrysaor-dangerous-spyware-affects-android/

[680] B. Mangiaracina. (Apr. 2017). *Chrysaor Malware Found on Android Devices-here's What You Should Know & How to Protect Yourself*. Gadget Hacks. [Online]. Available: https://android.gadgethacks.com/news/chrysaor-malware-found-android-devices-heres-what-you-should-know-protect-yourself-0176913/

[681] R. G. Rubio. (Apr. 2017). *This is Chrysaor, the Dangerous Spy Malware That Threatens Android*. AndroidAyuda. [Online]. Available: https://androidayuda.com/en/asi-chrysaor-peligroso-malware-android/

[682] A. D. Blog. (Jul. 2017). *From Chrysaor to Lipizzan: Blocking a New Targeted Spyware Family*. Android Developers Blog. [Online]. Available: https://android-developers.googleblog.com/2017/07/from-chrysaor-to-lipizzan-blocking-new.html

[683] R. KVN. (Jul. 2017). *Google's Android Team Track, Kill Deadly Lipizzan Malware in Record Time*. [Online]. Available: https://www.ibtimes.co.in/googles-android-team-track-kill-deadly-lipizzan-malware-record-time-736394

[684] L. H. Newman. (Jul. 2017). *Google Finds and Blocks Spyware Linked to Cyberarms Group*. Wired. [Online]. Available: https://www.wired.com/story/lipizzan-android-malware-nation-state/

[685] C. Cimpanu. (Jul. 2017). *Google Discovers New Lipizzan Android Spyware*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/google-discovers-new-lipizzan-android-spyware/

[686] M. Flossman. (Aug. 2017). *Sonicspy: Over a Thousand Spyware Apps Discovered, Some in Google Play*. [Online]. Available: https://www.lookout.com/blog/sonicspy-spyware-threat-technical-research

[687] I.-A. N. Service. (Aug. 2017). *Sonicspy Android Malware Family Spotted on Google Play Store: Lookout*. Gadgets. [Online]. Available: https://www.gadgets360.com/apps/news/sonicspy-android-malware-family-1737516

[688] I. Arghire. (Aug. 2017). *Sonicspy Spyware Found in Over One Thousand Android Apps | Securityweek.com*. [Online]. Available: https://www.securityweek.com/sonicspy-spyware-found-over-one-thousand-android-apps

[689] T. Micro. (Aug. 2017). *Sonicspy Android Spyware Found in Google Play—Security News*. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/mobile-safety/sonicspy-android-spyware-found-in-google-play

[690] KL Global Research & Analysis Team. (Aug. 2019). *Fully Equipped Spying Android Rat From Brazil: Brata*. [Online]. Available: https://securelist.com/spying-android-rat-from-brazil-brata/92775/

[691] S. Gatlan. (Aug. 2019). *Brata Android Rat Used to Infect and Spy on Brazilian Users*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/brata-android-rat-used-to-infect-and-spy-on-brazilian-users/

[692] P. Paganini. (Jan. 2022). *Latest Version of Android Rat Brata Wipes Devices After Stealing Data*. Secur. Affairs. [Online]. Available: https://securityaffairs.co/wordpress/127131/cyber-crime/new-android-brata-rat.html

[693] A. Din. (Jan. 2022). *Android Malware Brata is More Dangerous Than Ever*. Heimdal Security Blog. [Online]. Available: https://heimdalsecurity.com/blog/android-malware-brata-is-more-dangerous-than-ever/

[694] AS Team. (Sep. 2018). *Malware is Still Spying on You Even When Your Mobile is Off*. [Online]. Available: https://www.avg.com/en/signal/android-spyware-that-works-when-your-phone-is-off

[695] S. Khandelwal. (Feb. 2015). *Android Malware Can Spy on You Even When Your Mobile is Off*. Hacker News. [Online]. Available: https://thehackernews.com/2015/02/poweroffhijack-android-malware.html

[696] P. Paganini. (Feb. 2015). *Poweroffhijack Malware Spies on User When Mobile is Off*. Security Affairs. [Online]. Available: https://securityaffairs.co/wordpress/33843/malware/poweroffhijack-android-malware.html

[697] E. V. Radar. (Jul. 2015). *Android/Spy.Feabme.A | Eset Virusradar*. [Online]. Available: https://www.virusradar.com/en/Android_Spy.Feabme.A/description

[698] R. Lipovsky and L. Stefanko. (Jul. 2015). *Apps on Google Play Steal Facebook Credentials*. WeLiveSecurity. [Online]. Available: https://www.welivesecurity.com/2015/07/09/apps-google-play-steal-facebook-credentials/

[699] K. Augusto. (2018). *Android-Malware/Smack*. GitLab. [Online]. Available: https://gitlab.c3sl.ufpr.br/kac14/tcc/-/tree/2b70fd217f8c6e3f03bd7864d6d92b26639a6784/android-malware/smack

[700] T. Micro. (Jan. 2018). *Dark Caracal Group Revealed: Group Used Trojanized Android Apps to Steal Data—Wiadomosci Bezpieczenstwa*. [Online]. Available: https://www.trendmicro.com/vinfo/pl/security/news/mobile-safety/dark-caracal-group-used-trojanized-android-apps-to-steal-data

[701] R. Report. (Jan. 2018). *Dark Caracal Cyber-espionage At a Global Scale*. [Online]. Available: https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

[702] S. Khandelwal. (Jan. 2012). *Researchers Uncover Government-sponsored Mobile Hacking Group Operating Since 2012*. Hacker News. [Online]. Available: https://thehackernews.com/2018/01/dark-caracal-android-malware.html

[703] I. Ilascu. (Oct. 2018). *New Android Trojan Gplayed Adapts to Attacker's Needs*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/new-android-trojan-gplayed-adapts-to-attackers-needs/

[704] T. Desk. (Oct. 2018). *Beware! Android Trojan Gplayed Disguises Itself As Google Play Store to Attack Your Phone*. Indian Exp. [Online]. Available: https://indianexpress.com/article/technology/tech-news-technology/beware-android-trojan-gplayed-disguises-as-google-play-store-to-attack-your-phone-5400243/

[705] D. Bisson. (Oct. 2018). *Gplayed Android Trojan Imitates Google Apps to Spy on and Steal Data From Victims*. Security Intelligence. [Online]. Available: https://securityintelligence.com/news/gplayed-android-trojan-imitates-google-apps-to-spy-on-and-steal-data-from-victims/

[706] T. Seals. (Oct. 2018). *Adaptable, All-in-one Android Trojan Shows the Future of Malware*. [Online]. Available: https://threatpost.com/adaptable-all-in-one-android-trojan-shows-the-future-of-malware/138215/

[707] I. Arghire. (Mar. 2018). *New 'Henbox' Android Malware Discovered*. [Online]. Available: https://www.securityweek.com/new-%E2%80%9Chenbox%E2%80%9D-android-malware-discovered

[708] A. Hinchliffe, M. Harbison, J. Miller-Osborn, and T. Lancaster. (Apr. 2018). *Henbox: Inside the Coop*. Unit 42. [Online]. Available: https://unit42.paloaltonetworks.com/unit42-henbox-inside-coop/

[709] NJCCIC. (2018). *Henbox Njccic Threat Profile*. [Online]. Available: https://www.cyber.nj.gov/threat-center/threat-profiles/android-malware-variants/henbox

[710] P. Paganini. (Apr. 2018). *Kevdroid Android Rat Can Steal Private Data and Record Phone Calls*. Security Affairs. [Online]. Available: https://securityaffairs.co/wordpress/71027/malware/kevdroid-android-rat.html

[711] A. Jain. (Apr. 2018). *Kevdroid Malware: Steals Your Private Data & Records Phone Calls*. We Geek. [Online]. Available: https://wethegeek.com/kevdroid-malware-steals-your-private-data-records-phone-calls/

[712] P. Rascagneres. (Apr. 2018). *Fake Av Investigation Unearths Kevdroid, New Android Malware*. Cisco Talos Blog. [Online]. Available: https://blog.talosintelligence.com/fake-av-investigation-unearths-kevdroid/

[713] BusinessToday. (Sep. 2018). *Whatsapp Under Threat! 'Ownme' Android Spyware Could Leak Critical Data, Private Chats*. [Online]. Available: https://www.businesstoday.in/technology/news/story/whatsapp-under-threat-ownme-android-spyware-could-leak-critical-data-private-chats-109974-2018-09-28

[714] A. Kotecha. (Oct. 2018). *Android Users Beware: New Virus Called Ownme Stealing Your Data*. DNA India. [Online]. Available: https://www.dnaindia.com/technology/report-android-users-beware-new-virus-called-ownme-stealing-your-data-2672370

[715] L. Coleman. (Sep. 2018). *Ownme Malware is Slowly Attacking Android Phones*. Research Snipers. [Online]. Available: https://researchsnipers.com/ownme-malware-is-slowly-attacking-android-phones/

[716] A. Sachdeva. (Sep. 2018). *'Ownme' Android Spyware Can Access Your Whatsapp Texts, Call Logs, Browsing History*. [Online]. Available: https://fossbytes.com/ownme-android-spyware-access-whatsapp-texts/

[717] B. Vigliarolo. (Jan. 2018). *Skygofree Android Malware is 'One of the Most Powerful Ever Seen'*. TechRepublic. [Online]. Available: https://www.techrepublic.com/article/skygofree-android-malware-is-one-of-the-most-powerful-ever-seen/

[718] L. Grustniy. (Jan. 2018). *Skygofree—A Hollywood-style Mobile SPY*. [Online]. Available: https://www.kaspersky.com/blog/skygofree-smart-trojan/20717/

[719] N. Buchka and A. Firsh. (Jan. 2018). *Skygofree: Following in the Footsteps of Hackingteam*. [Online]. Available: https://securelist.com/skygofree-following-in-the-footsteps-of-hackingteam/83603/

[720] Lookout. (2018). *Stealth Mango & Tangelo Selling Your Fruits to Nation State Actors Security Research Report 2 Contents*. [Online]. Available: https://info.lookout.com/rs/051-ESQ-475/images/lookout-stealth-mango-srr-us.pdf

[721] C. Franklin, O. 26, and 2018. (Jul. 2018). *Stealth Mango Proves Malware Success Doesn't Require Advanced Tech*. Dark Reading. [Online]. Available: https://www.darkreading.com/privacy/stealth-mango-proves-malware-success-doesn-t-require-advanced-tech

[722] Cyware Labs. (May 2018). *Stealth Mango and Tangelo Targets Government Officials in Middle East, India and Afghanistan in New Phishing Espionage Campaign*. [Online]. Available: https://cyware.com/news/stealth-mango-and-tangelo-targets-government-officials-in-middle-east-india-and-afghanistan-in-new-phishing-espionage-campaign-adb86cd8

[723] A. Blaich and M. Flossman. (2018). *Stealth Mango and the Prevalence of Mobile Surveillanceware*. [Online]. Available: https://i.blackhat.com/us-18/Thu-August-9/us-18-Blaich-Stealth-Mango-and-the-Prevalence-of-Mobile-Surveillanceware.pdf

[724] SCLTRteam (Aug. 2018). *A Long Running Android Spyware Which Targets Social Apps is Still Active—Sonicwall*. [Online]. Available: https://securitynews.sonicwall.com/xmlpost/a-long-running-android-spyware-which-targets-social-apps-is-still-active/

[725] L. Arsene. (Aug. 2018). *Triout—Spyware Framework for Android With Extensive Surveillance Capabilities*. Bitdefender Labs. [Online]. Available: https://www.bitdefender.com/blog/labs/triout-spyware-framework-for-android-with-extensive-surveillance-capabilities/

[726] T. Seals. (Aug. 2018). *Triout Malware Carries Out Extensive, Targeted Android Surveillance*. [Online]. Available: https://threatpost.com/triout-malware-carries-out-extensive-targeted-android-surveillance/136773/

[727] NJCCIC. (2022). *Triout Njccic Threat Profile*. [Online]. Available: https://www.cyber.nj.gov/threat-center/threat-profiles/android-malware-variants/triout

[728] (May 2018). *Zoopark: New Android-based Malware Campaign Spreading Through Compromised Legitimate Websites*. [Online]. Available: https://www.kaspersky.com/about/press-releases/2018_zoopark-new-android-based-malware

[729] L. Grustniy. (May 2018). *How to Avoid Turning Your Smartphone Into a Spyware Zoo*. [Online]. Available: https://www.kaspersky.com/blog/zoopark-attacks/22389/

[730] Waqas. (May 2018). *Android Users Hit By Zoopark Malware Stealing Data & Recording Calls*. [Online]. Available: https://www.hackread.com/android-zoopark-malware-stealing-data-recording-calls/

[731] R. Jennings. (Mar. 2019). *Exodus Spyware Exposes 'Sorry' State of Android Security*. TechBeacon. [Online]. Available: https://techbeacon.com/security/exodus-spyware-exposes-sorry-state-android-security

[732] K. Townsend. (Apr. 2019). *Exodus Android Spyware With Possible Links to Italian Government Analyzed | Securityweek.com*. [Online]. Available: https://www.securityweek.com/exodus-android-spyware-possible-links-italian-government-analyzed

[733] P. Paganini. (Mar. 2019). *Exodus, a Government Malware That Infected Innocent Victims*. Security Affairs. [Online]. Available: https://securityaffairs.co/wordpress/83102/breaking-news/exodus-malware-google-play.html

[734] L. Stefanko. (Aug. 2019). *First-of-Its-Kind Spyware Sneaks Into Google Play*. WeLiveSecurity. [Online]. Available: https://www.welivesecurity.com/2019/08/22/first-spyware-android-ahmyth-google-play/

[735] E. Xu and G. Guo. (Jun. 2019). *Mobile Campaign 'bouncing Golf' Affects Middle East*. Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/research/19/f/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east.html

[736] E. Xu. (Dec. 2019). *Mobile Campaign Start Targeted Attacks Using Callerspy*. Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/research/19/l/mobile-cyberespionage-campaign-distributed-through-callerspy-mounts-initial-phase-of-a-targeted-attack.html

[737] SCLTR Team. (Aug. 2019). *Android Scams Related to the New Viral Trend—Faceapp—Sonicwall*. [Online]. Available: https://securitynews.sonicwall.com/xmlpost/android-scams-related-to-the-new-viral-trend-faceapp/

[738] (Jul. 2019). *Lookout*. [Online]. Available: https://www.lookout.com/documents/threat-reports/lookout-discovers-monokle-threat-report.pdf

[739] D. Durando. (Sep. 2019). *Funkybot: A New Android Malware Family Targeting Japan*. [Online]. Available: https://www.fortinet.com/blog/threat-research/funkybot-malware-targets-japan

[740] T. Seals. (Sep. 2019). *Funkybot Malware Intercepts Android Texts, 2FA Codes*. [Online]. Available: https://threatpost.com/funkybot-malware-intercepts-android-texts-2fa-codes/148059/

[741] VirusTotal. *Virustotal—Impersonatekoreanpolice*. Accessed: Mar. 10, 2024. [Online]. Available: https://rb.gy/34zqf

[742] D. Sarkar. (Dec. 2021). *Joker Malware is Back: Delete These 15 Apps From Your Android Phones Right Now*. [Online]. Available: https://www.news18.com/news/tech/joker-malware-is-back-delete-these-15-apps-from-your-android-phones-right-now-4471529.html

[743] A. Kuprins. (Sep. 2019). *Analysis of Joker—A SPY & Premium Subscription Bot on Googleplay*. CSIS TechBlog. [Online]. Available: https://medium.com/csis-techblog/analysis-of-joker-a-spy-premium-subscription-bot-on-googleplay-9ad24f044451

[744] K. Lucic. (Jul. 2022). *The 'Joker' Virus: Everything You Need to Know*. Android Headlines. [Online]. Available: https://www.androidheadlines.com/joker-virus-malware-android

[745] I. Bureau. (Sep. 2020). *Google Identifies and Removes 17 Android Apps Infected By Joker Malware*. ITSecurityWire. [Online]. Available: https://itsecuritywire.com/quick-bytes/google-identifies-and-removes-17-android-apps-infected-by-joker-malware/

[746] SCLTR Team. (Sep. 2019). *An Android Spyware That Spreads Via a Clever Phishing Campaign—Sonicwall*. [Online]. Available: https://securitynews.sonicwall.com/xmlpost/an-android-spyware-that-spreads-via-a-clever-phishing-campaign/

[747] J. Elder. (Jul. 2019). *Google Pulls Stalker Apps Identified By Avast*. [Online]. Available: https://blog.avast.com/avast-identifies-stalker-apps

[748] S. Desai. (2019). *A New Wave of Stalkerware Apps*. Zscaler. [Online]. Available: https://www.zscaler.com/blogs/security-research/new-wave-stalkerware-apps

[749] VirusTotal. *Virustotal—Covid_agedetector*. Accessed: Mar. 10, 2024. [Online]. Available: https://rb.gy/846gl

[750] VirusTotal. *Virustotal—Covid_lures*. Accessed: Mar. 10, 2024. [Online]. Available: https://rb.gy/cdqkv

[751] T. Meskauskas. (Sep. 2022). *Spymax Spyware (Android)*. [Online]. Available: https://www.pcrisk.com/removal-guides/17617-spymax-spyware-android

[752] GoldSparrow. (Mar. 2020). *'Spymax Rat' Remove Spyware & Malware With SpyHunter—EnigmaSoft*. [Online]. Available: https://www.enigmasoftware.com/spymaxrat-removal/

[753] K. D. Rosso. (Mar. 2020). *New Threat—Commercial Surveillanceware Operators Exploit Covid-19*. [Online]. Available: https://www.lookout.com/blog/commercial-surveillanceware-operators-latest-to-take-advantage-of-covid-19

[754] C. Osborne. (Jul. 2022). *How to Find and Remove Spyware From Your Phone*. ZDNET. [Online]. Available: https://www.zdnet.com/article/how-to-find-and-remove-spyware-from-your-phone/

[755] L. Franceschi-Bicchierai. (Aug. 2013). *Android to Spyphone: How Hackers Can Spy on Your Smartphone*. Sydney Morning Herald. [Online]. Available: https://www.smh.com.au/technology/android-to-spyphone-how-hackers-can-spy-on-your-smartphone-20130802-2r3ah.html

[756] SCLTR. Team. (Apr. 2020). *Fake Android Zoom Video Meeting Apps Harbor Malware/Adware Components—Sonicwall*. [Online]. Available: https://securitynews.sonicwall.com/xmlpost/fake-android-zoom-video-meeting-apps-harbor-malware-adware-components/

[757] M. Kan. (May 2022). *Hackers Exploit Community Meetings to Spread Malware Via Fake Zoom Invites*. PCMAG. [Online]. Available: https://www.pcmag.com/news/hackers-exploit-community-meetings-to-spread-malware-via-fake-zoom-invites

[758] D. Palmer. (May 2020). *Hackers Target Remote Workers With Fake Zoom Downloader*. ZDNET. [Online]. Available: https://www.zdnet.com/article/hackers-target-remote-workers-with-fake-zoom-downloader/

[759] BushidoToken. (Apr. 2020). *Xploitspy: New Android Spyware Designed By Ethical-ish Hackers*. [Online]. Available: https://blog.bushidotoken.net/2020/04/xploitspy-new-android-spyware-designed.html

[760] H. N. Duc. (Apr. 2020). *Xploitspy is an Android Monitoring/Spying Tool*. [Online]. Available: https://hakin9.org/xploitspy-is-an-android-monitoring-spying-tool/

[761] L. O'Donnell. (Jun. 2020). *Android 'Actionspy' Malware Targets Turkic Minority Group*. [Online]. Available: https://threatpost.com/android-actionspy-malware-targets-turkic-minority-group/156507/

[762] G. Donnelly. (2020). *Social Network for Programmers and Developers*. [Online]. Available: https://morioh.com/p/0dd5df862508

[763] E. Xu and J. C. Chen. (Jun. 2020). *Phishing Attacks From Earth Empusa Reveal Actionspy*. Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/research/20/f/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa.html

[764] G. Chahal. (Jan. 2022). *Donot Hackers Attack Organizations & Individuals With Windows & Android Malware*. Cyber Security New. [Online]. Available: https://cybersecuritynews.com/donot-hackers/

[765] cybleinc. (Aug. 2021). *Bahamut Threat Group Targeting Users Through Phishing Campaign*. Cyble. [Online]. Available: https://blog.cyble.com/2021/08/10/bahamut-threat-group-targeting-users-through-phishing-campaign/

[766] SCLTR. Team. (Nov. 2020). *Android Spyware Bahamut Spreads Disguised As Voice of Islam App—Sonicwall*. [Online]. Available: https://securitynews.sonicwall.com/xmlpost/android-spyware-bahamut-spreads-disguised-as-voice-of-islam-app/

[767] O. Asoltanei. (Jun. 2020). *Bitterapt Revisited: The Untold Evolution of an Android Espionage Tool*. Bitdefender Labs. [Online]. Available: https://www.bitdefender.com/blog/labs/bitterapt-revisited-the-untold-evolution-of-an-android-espionage-tool/

[768] A. Kumar and J. Albrecht. (Dec. 2020). *New Spyware Used By Sextortionists | Ios/android Blackmail | Lookout*. [Online]. Available: https://www.lookout.com/blog/lookout-discovers-new-spyware-goontact-used-by-sextortionists-for-blackmail

[769] P. Ducklin. (Mar. 2020). *Android Malware Uses Coronavirus for Sextortion and Ransomware Combo*. Naked Security. [Online]. Available: https://nakedsecurity.sophos.com/2020/03/18/android-malware-uses-coronavirus-for-sextortion-ransomware-combo/

[770] E. Montalbano. (Dec. 2020). *Sextortionist Campaign Targets Ios, Android Users With New Spyware*. [Online]. Available: https://threatpost.com/sextortionist-campaign-targets-ios-android-users-with-new-spyware/162321/

[771] SCLTRTeam. (May 2020). *Fake Aarogya Setu Android Apps Harbor Spyware Capabilities—Sonicwall*. [Online]. Available: https://securitynews.sonicwall.com/xmlpost/fake-aarogya-setu-android-apps-harbor-spyware-capabilities/

[772] R. Majumdar. (May 2020). *Fake Aarogya Setu Apps Carrying Spyware Spotted*. Mint. [Online]. Available: https://www.livemint.com/technology/tech-news/fake-aarogya-setu-apps-carrying-spyware-spotted-11590650596973.html

[773] T. Seals. (Oct. 2020). *Gravityrat Comes Back to Earth With Android, Macos Spyware*. [Online]. Available: https://threatpost.com/gravityrat-back-android-macos-spyware/160299/

[774] cybleinc. (Nov. 2021). *Gravity Rat Malware Returns As a Chat Application*. Cyble. [Online]. Available: https://blog.cyble.com/2021/11/11/gravity-rat-malware-returns-as-a-chat-application/

[775] S. Gatlan. (Oct. 2020). *Windows Gravityrat Malware Now Also Targets Android, Macos*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/windows-gravityrat-malware-now-also-targets-android-macos/

[776] P. Paganini. (Oct. 2020). *Gravityrat Malware Also Targets Android and Macos*. Security Affairs. [Online]. Available: https://securityaffairs.co/wordpress/109744/malware/gravityrat-malware-android-macos.html

[777] L. Stefanko. (May 2020). *Insidious Android Malware Gives Up All Malicious Features but One to Gain Stealth*. WeLiveSecurity. [Online]. Available: https://www.welivesecurity.com/2020/05/22/insidious-android-malware-gives-up-all-malicious-features-but-one-gain-stealth/

[778] (Dec. 2020). *Fortiguard*. FortiGuard. [Online]. Available: https://www.fortiguard.com/encyclopedia/virus/8279818

[779] L. Stefanko. (Jul. 2020). *Welcome Chat As a Secure Messaging App? Nothing Could Be Further From the Truth*. WeLiveSecurity. [Online]. Available: https://www.welivesecurity.com/2020/07/14/welcome-chat-secure-messaging-app-nothing-further-truth/

[780] I. Ilascu. (Jul. 2020). *Android Chat App Uses Public Code to Spy, Exposes User Data*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/android-chat-app-uses-public-code-to-spy-exposes-user-data/

[781] B. Botezatu. (May 2016). *Mandrake—Owning Android Devices Since 2016*. Bitdefender Labs. [Online]. Available: https://www.bitdefender.com/blog/labs/mandrake-owning-android-devices-since-2016/

[782] I. Arghire. (May 2020). *'Mandrake' Android Spyware Remained Undetected for 4 Years | Securityweek.com*. [Online]. Available: https://www.securityweek.com/mandrake-android-spyware-remained-undetected-4-years

[783] D. Palmer. (May 2020). *This Powerful Android Malware Stayed Hidden for Years, Infecting Tens of Thousands of Smartphones*. ZDNET. [Online]. Available: https://www.zdnet.com/article/this-powerful-android-malware-stayed-hidden-years-infected-tens-of-thousands-of-smartphones/

[784] A. Kivva and I. Golovin. (Mar. 2020). *Cookiethief: A Cookie-stealing Trojan for Android*. [Online]. Available: https://securelist.com/cookiethief/96332/

[785] C. Osborne. (Mar. 2020). *Cookiethief Android Malware Uses Proxies to Hijack Your Facebook Account*. ZDNET. [Online]. Available: https://www.zdnet.com/article/android-malware-tweaks-expose-devices-to-browser-app-cookie-theft/

[786] P. Paganini. (Mar. 2020). *Cookiethief, the Android Malware That Hijacks Facebook Accounts*. Security Affairs. [Online]. Available: https://securityaffairs.co/wordpress/99569/malware/cookiethief-android-malware.html

[787] J. Steinberg. (Aug. 2016). *Spynote Trojan—New Threat to Android*. Best Security Search. [Online]. Available: https://bestsecuritysearch.com/spynote-trojan-virus-new-threat-android-users/

[788] *Android/Trojan.Spy.Spynote.Dcnp*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.malwarebytes.com/blog/detections/android-trojan-spy-spynote-dcnp

[789] J. Wallen. (Aug. 2016). *Spynote Malware: One More Reason to Never Sideload Android Apps*. TechRepublic. [Online]. Available: https://www.techrepublic.com/article/spynote-malware-one-more-reason-to-never-sideload-android-apps/

[790] V. Chebyshev. (Mar. 2020). *Monitorminor: Vicious Stalkerware?* [Online]. Available: https://securelist.com/monitorminor-vicious-stalkerware/95575/

[791] P. Shoshin. (Mar. 2020). *Monitorminor: Spying on Android*. [Online]. Available: https://www.kaspersky.com/blog/monitorminor-stalkerware/34060/

[792] S. Hakak, W. Z. Khan, M. Imran, K. R. Choo, and M. Shoaib, "Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies," *IEEE Access*, vol. 8, pp. 124134–124144, 2020.

[793] T. Bao and J. Lu. (Apr. 2020). *Coronavirus Update App Leads to Project Spy Android and Ios Spyware*. Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/research/20/d/coronavirus-update-app-leads-to-project-spy-android-and-ios-spyware.html

[794] Deloitte. (Apr. 2020). *Organizations Invest Substantial Resources in Addressing Attacks*. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/COVID-19/gx-deloitte-global-cyber-covid-19-executive-briefing-issue-4-release-date-4.29.2020.pdf

[795] A. Spadafora. (May 2022). *Dangerous Predator Spyware Hits Android Phones—What to Do*. Tom's Guide. [Online]. Available: https://www.tomsguide.com/news/this-dangerous-android-malware-spies-on-your-every-move-what-to-do

[796] C. Cimpanu. (Sep. 2020). *New 'Alien' Malware Can Steal Passwords From 226 Android Apps*. ZDNET. [Online]. Available: https://www.zdnet.com/article/new-alien-malware-can-steal-passwords-from-226-android-apps/

[797] A. N. Desai. (2022). *'Alien' Spyware is Loading Predator Malware on Android Devices, Warns Google*. [Online]. Available: https://www.neowin.net/news/alien-spyware-is-loading-predator-malware-on-android-devices-warns-google/

[798] Z. Dong, F. Yarochkin, and S. Du. (Jul. 2021). *Strongpity APT Group Deploys Android Malware for the First Time*. Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/research/21/g/strongpity-apt-group-deploys-android-malware-for-the-first-time.html

[799] (Jul. 2021). *Strongpity APT Group Hacked an Official GOV Website to Deliver Android Malware*. Cyber Security News. [Online]. Available: https://cybersecuritynews.com/strongpity-apt-group/

[800] C. Cimpanu. (Sep. 2020). *Google Removes Android App That Was Used to SPY on Belarusian Protesters*. ZDNET. [Online]. Available: https://www.zdnet.com/article/google-removes-android-app-that-was-used-to-spy-on-belarusian-protesters/

[801] P. Paganini. (Sep. 2020). *Is the Belarusian Government Behind the Surveillance Android App Banned By Google*. Security Affairs. [Online]. Available: https://securityaffairs.co/wordpress/107869/malware/surveillance-app-belarusian-government.html

[802] J. Fingas. (Sep. 2020). *'Iranian Hackers' Android Malware Spies on Dissidents By Stealing 2fa Codes*. Engadget. [Online]. Available: https://www.engadget.com/iran-rampant-kitten-android-2fa-malware-212913812.html

[803] P. Paganini. (Sep. 2020). *Rampant Kitten's Arsenal Includes Android Malware That Bypasses 2FA*. Security Affairs. [Online]. Available: https://securityaffairs.co/wordpress/108467/malware/rampant-kitten-android-malware.html

[804] L. Finkelsteen. (Sep. 2020). *Rampant Kitten—An Iranian Espionage Campaign*. Check Point Research. [Online]. Available: https://research.checkpoint.com/2020/rampant-kitten-an-iranian-espionage-campaign/

[805] S. Desai. (2020). *Detailed Analysis of Tiktok Spyware | Zscaler Blog*. Zscaler. [Online]. Available: https://www.zscaler.com/blogs/security-research/tiktok-spyware

[806] L. O'Donnell. (May 2020). *Wolfrat Android Malware Targets Whatsapp, Facebook Messenger*. [Online]. Available: https://threatpost.com/wolfrat-android-malware-whatsapp-facebook-messenger/155809/

[807] C. Osborne. (May 2020). *Wolfrat Targets Whatsapp, Facebook Messenger App Users on Android Devices*. ZDNet. [Online]. Available: https://www.zdnet.com/article/wolfrat-targets-users-of-whatsapp-facebook-messenger-apps-on-android-devices/

[808] (May 2020). *Android Users Beware: Wolfrat Malware May Be Coming for You*. Dazeinfo. [Online]. Available: https://dazeinfo.com/2020/05/29/android-users-beware-wolfrat-malware-may-be-coming-for-you/

[809] S. Barbhuiya, P. Kilpatrick, and D. S. Nikolopoulos, "DroidLight: Lightweight anomaly-based intrusion detection system for smartphone devices," in *Proc. 21st Int. Conf. Distrib. Comput. Netw.*, Jan. 2020, pp. 1–10.

[810] E. V. Radar. (2018). *Android/Ksapp.G | Eset Virusradar*. [Online]. Available: https://www.virusradar.com/en/Android_Ksapp.G/description

[811] *Trojan: Android/Updtkiller.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_updtkiller.shtml

[812] (May 2011). *Security Alert: Fee-deduction Malware on Android Devices Spotted in the Wild*. [Online]. Available: https://www.prnewswire.com/news-releases/security-alert-fee-deduction-malware-on-android-devices-spotted-in-the-wild-122822179.html

[813] *Trojan: Android/Basebridge.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_basebridge.shtml

[814] MS Intelligence. (Sep. 2017). *Trojan: Androidos/Basebridge.B Threat Description—Microsoft Security Intelligence*. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:AndroidOS/BaseBridge.B

[815] MS Intelligence. (Feb. 2022). *Trojan: Androidos/Iconosys.B!Mtb*. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:AndroidOS/Iconosys.B!MTB&threatId=-2147155461

[816] *Trojan: Android/Iconosys.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_iconosys.shtml

[817] S. Malik and K. Khatter, "System call analysis of Android malware families," *Indian J. Sci. Technol.*, vol. 9, no. 21, pp. 1–13, Jun. 2016.

[818] J. Clark. (Dec. 2010). *Geinimi Trojan Targets Android Devices*. ZDNET. [Online]. Available: https://www.zdnet.com/article/geinimi-trojan-targets-android-devices/

[819] *Trojan: Android/Geinimi Description | F-Secure Labs*. [Online]. Mar. 10, 2024. Available: https://www.f-secure.com/v-descs/trojan_android_geinimi.shtml

[820] A. Basic. (Jul. 2020). *Android Malware 101: Top Variants, How to Detect and Remove It | Cyberarrow*. [Online]. Available: https://www.cyberarrow.io/blog/2020/07/19/android-malware-101-top-variants-how-to-detect-and-remove-it/

[821] V. Beal. (Aug. 2011). *What is Droiddream?* Webopedia. [Online]. Available: https://www.webopedia.com/definitions/droiddream/

[822] *Trojan: Android/Droiddream.A Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_droiddream_a.shtml

[823] (Jul. 2019). *Android Malware Analysis—Droiddream*. Medium. [Online]. Available: https://nikhilh20.medium.com/android-malware-analysis-droiddream-d06fc0d87bd2

[824] J. DeRuvo. (Mar. 2011). *Android Malware Apps Get Official Attention*. Android Community. [Online]. Available: https://androidcommunity.com/android-malware-apps-get-official-attention-20110304/

[825] (Jul. 2014). *Android/Gappusin.A!Tr*. FortiGuard. [Online]. Available: https://www.fortiguard.com/encyclopedia/mobile/6286936/android-gappusin-a-tr

[826] EV Radar. (Feb. 2012). *Android/Gappusin.A | Eset Virusradar*. [Online]. Available: https://www.virusradar.com/en/Android_Gappusin.A/description

[827] EV Radar. (2011). *Android/Spy.Imlog.G | Eset Virusradar*. [Online]. Available: https://www.virusradar.com/en/Android_Spy.ImLog.G/description

[828] M. Corporation. (2017). *Trojanspy: Androidos/Ewall.A Threat Description—Microsoft Security Intelligence*. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy%3AAndroidOS%2FEwall.A

[829] *Trojan: Android/Faketimer Description | F-Secure Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.f-secure.com/v-descs/trojan_android_faketimer.shtml

[830] M-Corporation. (2012). *Trojanspy: Androidos/Faketimer.A Threat Description—Microsoft Security Intelligence*. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy:AndroidOS/FakeTimer.A

[831] SCLTR Team. (Jan. 2019). *The Android Zazdi Botnet Uses FCM to Communicate With Its Infected Bots—Sonicwall*. [Online]. Available: https://securitynews.sonicwall.com/xmlpost/the-android-zazdi-botnet-uses-fcm-to-communicate-with-its-infected-bots/

[832] F. Khan, J. Ahamed, S. Kadry, and L. K. Ramasamy, "Detecting malicious URLs using binary classification through AdaBoost algorithm," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 10, no. 1, p. 997, Feb. 2020.

[833] K. Threats. (2016). *Kaspersky Threats—Fakeapp*. [Online]. Available: https://threats.kaspersky.com/en/threat/Trojan.AndroidOS.Fakeapp/

[834] *Android/fakeapp | Malwarebytes Labs*. Accessed: Mar. 10, 2024. [Online]. Available: https://www.malwarebytes.com/blog/detections/android-fakeapp

[835] M. Spreitzenbarth and F. Freiling, "Android malware on the rise," Friedrich-Alexander Univ. Erlangen-Nürnberg, Erlangen, Germany, Tech. Rep. FAU-CS-TR-2012-05, 2012.

[836] (2012). *Android/Steek.A!Tr*. FortiGuard. [Online]. Available: https://fortiguard.fortinet.com/encyclopedia/virus/3458224

[837] VirusTotal. *Virustotal—Facebook_OTP*. Accessed: Mar. 10, 2024. [Online]. Available: https://rb.gy/5fygw

[838] C. Zheng and T. Luo. (Nov. 2016). *Pluginphantom: New Android Trojan Abuses*. Unit 42. [Online]. Available: https://unit42.paloaltonetworks.com/unit42-pluginphantom-new-android-trojan-abuses-droidplugin-framework/

[839] C. Cimpanu. (Nov. 2016). *Pluginphantom Android Malware Uses Novel Approach to Hide Malicious Behavior*. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/pluginphantom-android-malware-uses-novel-approach-to-hide-malicious-behavior/

[840] E. Kovacs. (Nov. 2016). *'Pluginphantom' Android Trojan Uses Plugins to Evade Detection*. [Online]. Available: https://www.securityweek.com/pluginphantom-android-trojan-uses-plugins-evade-detection

[841] NJCCIC. (2022). *Pluginphantom Njccic Threat Profile*. [Online]. Available: https://www.cyber.nj.gov/threat-center/threat-profiles/android-malware-variants/pluginphantom

[842] QAATR Team. (Apr. 2019). *Stealjob: New Android Malware Used By Donot Apt Group*. [Online]. Available: https://ti.qianxin.com/blog/articles/stealjob-new-android-malware-used-by-donot-apt-group-en/

[843] MalBot. (Jan. 2019). *Rogue Mobile App*. Malware Analysis, News Indicators. [Online]. Available: https://malware.news/t/rogue-mobile-app/26837

[844] M-Corporation. (2017). *Trojanspy: Androidos/Adrd.A Threat Description—Microsoft Security Intelligence*. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy

[845] (2011). *Analysis Report on Android Trojan Hongtoutou (adrd)*. [Online]. Available: https://www.antiy.net/media/reports/android_adrd_analysis.pdf

[846] CR Team. (Mar. 2017). *Operation Electric Powder—Who is Targeting Israel Electric Company?* [Online]. Available: https://www.clearskysec.com/iec/

[847] Accessed: Mar. 10, 2024. [Online]. Available: https://ibotpeaches.github.io/Apktool/

[848] A. Thakkar and R. Lohiya, "Attack classification using feature selection techniques: A comparative study," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 1, pp. 1249–1266, Jan. 2021.

[849] G. H. Alshammri, A. K. Samha, E. El-Din Hemdan, M. Amoon, and W. El-Shafai, "An efficient intrusion detection framework in software-defined networking for cybersecurity applications," *Comput., Mater. Continua*, vol. 72, no. 2, pp. 3529–3548, 2022.

**IMAN ALMOMANI** (Senior Member, IEEE) received the bachelor's and master's degrees in computer science from United Arab Emirates and Jordan, in 2000 and 2002, respectively, and the Ph.D. degree in wireless network security from De Montfort University, U.K., in 2007. She was the Associate Director of the Research and Initiatives Centre (RIC), Prince Sultan University (PSU), Riyadh, Saudi Arabia. Before joining PSU, she was an Associate Professor and the Head of the Computer Science Department, The University of Jordan, Amman, Jordan. She is currently a Professor of cybersecurity with The University of Jordan. She is also the Leader of the Security Engineering Laboratory (SEL). Her research interests include the security of wireless networks, mainly wireless mobile ad hoc networks (WMANETs), wireless sensor networks (WSNs), the Internet of Things (IoTs), multimedia networking (VoIP), and android security. She is also interested in cybersecurity maturity models, security intelligence, and AI applications in cybersecurity. She has publications in the above areas in reputable international and local journals and conferences. She is a Senior Member of IEEE WIE. She is on the organizing and technical committees for several regional and international conferences. She also serves as a reviewer and a member of the editorial board for many international journals.

**TALA ALMASHAT** received the bachelor's degree in software engineering in the cybersecurity track from Prince Sultan University (PSU), Riyadh, Saudi Arabia, in 2021. She is currently a Research Engineer with the Security Engineering Laboratory (SEL), PSU. Her research interests include software engineering, application security, digital forensics, malware analysis, machine learning, and artificial intelligence.

**WALID EL-SHAFAI** (Senior Member, IEEE) was born in Alexandria, Egypt. He received the B.Sc. degree (Hons.) in electronics and electrical communication engineering from the Faculty of Electronic Engineering (FEE), Menoufia University, Menouf, Egypt, in 2008, the M.Sc. degree from Egypt–Japan University of Science and Technology (E-JUST), in 2012, and the Ph.D. degree from FEE, Menoufia University, in 2019. Since January 2021, he has been a Postdoctoral Research Fellow with the Security Engineering Laboratory (SEL), Prince Sultan University (PSU), Riyadh, Saudi Arabia. He is currently a Senior Cybersecurity Researcher with SEL and an Assistant Professor with the College of Computer Science and Information Systems. He is also an Associate Professor with the Department of Electronics and Communication Engineering (ECE), FEE, Menoufia University. His research interests include wireless mobile and multimedia communications systems, image and video signal processing, efficient 2D video/3D multi-view video coding, multi-view video plus depth coding, 3D multi-view video coding and transmission, quality of service and experience, digital communication techniques, cognitive radio networks, adaptive filters design, 3D video watermarking, steganography, encryption, error resilience and concealment algorithms for H.264/AVC, H.264/MVC, and H.265/HEVC video codecs standards, cognitive cryptography, medical image processing, speech processing, security algorithms, software-defined networks, the Internet of Things, medical diagnoses applications, FPGA implementations for signal processing algorithms and communication systems, cancellable biometrics and pattern recognition, image and video magnification, artificial intelligence for signal processing algorithms and communication systems, modulation identification and classification, image and video super-resolution and denoising, cybersecurity applications, malware and ransomware detection and analysis, deep learning in signal processing, and communication systems applications. He also serves as a reviewer for several international journals.