Understanding Android Financial Malware Attacks: Taxonomy, Characterization, and Challenges

Andi Fitriah Abdul Kadir, Natalia Stakhanova and Ali A. Ghorbani

Canadian Institute for Cybersecurity (CIC),
University of New Brunswick, New Brunswick, Canada
E-mail: andi.fitriah; natalia.stakhanova; ghorbani@unb.ca

Received 18 February 2018; Accepted 12 April 2018;
Publication 14 June 2018

Abstract

With the increased number of financial-related malware, the security community today has turned their attention to the Android financial malware. However, what constitutes Android financial malware is still ambiguous. A comprehensive understanding of the existing Android financial malware attacks supported by a unified terminology is necessarily required for the deployment of reliable defence mechanisms against these attacks. Thus, in this paper, we address this issue and devise a taxonomy of Android financial malware attacks. By devising the proposed taxonomy, we intend to: give researchers a better understanding of these attacks; explore the Android financial malware characteristics; and provide a foundation for organizing research efforts within this specific field. In order to evaluate the proposed taxonomy, we gathered a large collection of Android financial malware samples representing 32 families, which are selected based on the main characteristics defined in the taxonomy. We discuss the characterization of these families in terms of malware installation, activation and attacks, and derive a set of research question: how does the malware spread to the Android users?,

Journal of Cyber Security and Mobility, Vol. 7_3, 1–52. *River Publishers*
doi: 10.13052/jcsm2245-1439.732

how does the malware activate itself on the phone?, and what happens after the malware has reached the Android system? Evaluation and characterization of this taxonomic model towards Android financial malware implies the possibility for introducing an automatic malware categorization, which can effectively save the time of malware analysts to correlate various symptoms of malicious behavior; this combination provides a systematic overview of malware capabilities, which can help analyst in the malware-triage process for prioritizing which malware to be scrutinized. Also, we identified a number of challenges related to Android financial malware, which can create opportunity for future research.

Keywords: Adware, Android malware, banking, behavioral analysis, financial malware, malware characterization, taxonomy, ransomware, scareware, SMS malware.

1 Introduction

Mobile malware such as viruses, trojan horses, and worms have emerged as the fastest growing threat in the digital world. This malware exhibits malicious behavior targeting mobile phones without the user's consent by adding malicious code into a smartphone's software system. Mobile malware has various ways of infecting smartphones' systems and propagating themselves. Some malware can infect systems by being bundled with other programs or attached as macros to files. Some can exploit the vulnerability of the systems through several mediums such as mobile network services, Internet access, bluetooth, Global Positioning System (GPS), etc. Most mobile malware aims at mobile pick pocketing, i.e., stealing off money or other valuables via Short Messaging Services (SMS) and Multimedia Messaging Service (MMS), or the ability to charge premium bills via SMS or calls. Apart from that, malware is used to steal information, send SMS spam, and install other malicious applications.

Today, the mobile platforms face a range of security challenges. The widespread adoption of mobile platforms coupled with the growth of malware, and lack of understanding of the malware (especially financial malware) is one of the primary concerns. The other challenge relates to the lack of effective security solutions, and the last, but not least, is the high cost of attack recovery. The first challenge has opened up new avenues for old attacks. Mobile phones are a rich source of sensitive information, traditionally not available to stationary computers (e.g., location information,

user's activities, financial information). This creates an opportunity for new context-aware mobile malware to access and exfiltrate information typically not monitored by traditional detection systems. Secondly, the growth of malware, especially financial malware presents a major challenge as well. Due to its popularity, Android mobile operating system (OS) has become the most targeted platform surpassing Apple iOS, Windows Mobile, Blackberry, and Symbian [6]. With the ubiquitous shift to financial gain, Android financial malware has emerged as the fastest growing threat of all attacks targeting the mobile platform or individual users. The 2017 Symantec Financial Threats Review reported that mobile financial threats is the third most common threat category, behind SMS-premium-rate malware and ransomware [12].

Although Android malware detection systems are being actively developed, research efforts focused on Android financial malware are still isolated. Our concern is the lack of understanding of mobile financial malware. Without knowing what constitutes mobile financial malware, the detection systems are not capable of providing an accurate recognition of an advanced and sophisticated mobile financial malware. A simple illustration to that is the labelling of malware family *Zitmo*. *Zitmo* was initially analyzed by Zhou & Jiang [57] in 2008 and labelled as a banking malware. However, a quick scan of one of its family samples by VirusTotal platform shows the disparity in labelling (Table 1). Based on the VirusTotal results, none of the labels indicate banking nature, even though some anti-viruses even use a technical malware naming convention such as *McAfee/Artemis!048C4A526C99*. The detection results show that most of the current detection systems (20 out of 32) emphasize the Android malware threats from a high-level perspective by analyzing malware types and providing a general label (e.g. Trojan). The problem is that the existing systems are not accurately detecting financial malware. The existing signatures are only suitable for recognition of generic malware types rather than indicating its capabilities. The inconsistent labelling between different anti-virus products leads to confusion, hence affecting the mitigation and response strategy of mobile malware, which in turn leads to an increased recovery cost.

We believe that by having a solid understanding of the financial malware attacks followed by a unified terminology can help in the deployment of reliable defence mechanisms for financial malware attacks. To address this problem, we propose a comprehensive taxonomy for the Android financial malware attacks. We believe that such taxonomy would provide a good foundation for an effective detection system.

Table 1 Example of VirusTotal analysis for Banking Malware *Zitmo* (md5 hash value: 048c4a526c999539a122e39a95b7f0a1)

No	Anti-virus	Result
1	AVG	Android/Deng.FVQ
2	Ad-Aware	Android.Trojan.Zitmo.E
3	AhnLab-V3	Android-Spyware/Rehail6.d55d
4	Alibaba	A.H.Pri.Dvci
5	Antiy-AVL	Trojan[Spy:HEUR]/AndroidOS.Mekir.2
6	Arcabit	Android.Trojan.Zitmo.E
7	Avast	Android:Morcut-G [Trj]
8	Avira (no cloud)	ANDROID/Agent.EW.Gen
9	Baidu-International	Trojan.AndroidOS.Mekir.b
10	BitDefender	Android.Trojan.Zitmo.E
11	CAT-QuickHeal	Android.Mekir.A
12	Cyren	AndroidOS/GenB1.048C4A52!Olympus
13	DrWeb	Android.Spy.176.origin
14	ESET-NOD32	a variant of Android/Morcut.A
15	Emsisoft	Android.Trojan.Zitmo.E (B)
16	F-Secure	Trojan:Android/Fakeinst.NG
17	Fortinet	Android/Mekir.D!tr
18	GData	Android.Trojan.Zitnio.E
19	Ikarus	Trojan.AndroidOS.Morcut
20	Jiangmin	TrojanSpy.AndroidOS.lbq
21	K7GW	Trojan (004c7e8c1)
22	Kaspersky	HEUR:Trojan-Spy.AndroidOS.Mekir.b
23	McAfee	Artermis!048C4A526C99
24	McAfee-GW-Edition	Artemis'Trojan
25	eScan	Android.Trojan.Zitmo.E
26	NANO-Antivirus	Trojan.Android.Mekir.dubdof
27	Qihoo-360	Trojan.Android.Gen
28	Rising	APK:Trojan.Generic(AndrCity)!17.1762 [F]
29	Sophos	Andr/Spy-AEC
30	VIPRE	Trojan.AndroidOS.Generic.A
31	Zillya	Trojan.Morcut..57
32	Zoner	Trojan.AndroidOS.Morcut

Our contribution. The contribution of our work is three-fold:

1. This research provides a comprehensive guideline in understanding the threat landscape of the Android financial malware. The behavioral analysis of the Android financial malware based on the proposed taxonomy can give researchers a better understanding of the Android financial malware attacks and their individual categories. For each category, we provide its

definition, distinctive features and representative examples derived from both industry and academia.
2. This research is helpful in providing a foundation for organizing research efforts in the field of Android financial malware. It outlines the fundamental principles necessary for the effective mobile malware detection system including the challenges faced by Android malware researchers. This is the first attempt to organize the existing research efforts in this area that we hope will be extended by other researchers in the future.
3. To foster more research in this area, we release the accumulated dataset to the research community[1]. The dataset is equipped with an analysis behavior of each malware family in terms of malware installation, activation, and attacks. A key to building an effective solution for Android financial malware detection is to have a comprehensive and up-to-date dataset. Our accumulated dataset combines samples from several resources such as malware security blogs, security web-services, anti-malware vendors, and other researchers.

The rest of the paper is organized as follows: Section 2 describes the related work and then followed by the methodology of the study in Section 3. Sections 4 and 5 discuss the analytical analysis and taxonomy of Android financial malware, respectively. Next, Section 6 presents the evaluation of the proposed taxonomy and followed by the challenges faced by researchers in conducting research in Section 7. Finally, Section 8 concludes the paper with some remarks about the outcome of the work.

2 Related Work

Mobile malware was almost non-existent before the official release of the Android platform in 2008. A few studies [23, 33, 39] that were conducted at that time focused on other platforms such as Blackberry and Symbian. In fact, the first computer worm that infected mobile phones was targeting Symbian OS. With the rapid development of mobile platforms and the increase in the number of mobile threats, the number of studies in the field of mobile malware, specifically Android malware, has been steadily increasing.

With the rapid advancement of Android devices, researchers focused their attention on Android malware. A broad overview of mobile malware characteristics were offered by Alzahrani et al. [19] and Zhou et al. [57]. The work by Zhou et al. was one of the early studies in this domain that aimed to give researchers an understanding of mobile malware through

[1] http://www.unb.ca/cic/datasets/index.html

systematic characterization of the Android malware from various aspects. At that time one of the main concerns was a timely detection of Android malware and one of the first attempts to provide that was offered by Bose et al. [22]. The work presented a behavioral detection framework based on logical ordering of application actions. This study was quickly followed by a series of more advanced detection approaches focused on developing detection and mitigation techniques in various areas, e.g., mobile botnet detection [24, 34, 43, 52, 54], mobile ransomware [20, 30, 41, 49, 53] detection of privacy violations (TaintDroid [26], MockDroid [21], VetDroid [55]), and security policy violations [45, 48].

In 2015, Sufatrio et al. [51] presented a survey and taxonomy of existing studies that focused on securing Android devices. The survey highlighted the limitations of existing works and current challenges of Android security, which aimed to help identify the potential research directions for protecting Android devices. Similarly, another survey by Faruki et al. [28] discussed the issues, malware growth, and stealth techniques used by malware authors to evade detection. With the focus of the work on general Android malware, financial malware was not even mentioned. In this research, we focus on the taxonomy of Android financial malware attacks, its challenges, and characteristics.

Apart from that, there exists only a few studies on financial malware, which are related to our work. In 2010, Riccardi et al. [47] presented work-in-progress research aimed at creating a system for mitigating financial botnets. The architecture promoted information sharing among law enforcement authorities, ISPs and financial institutions. Later in 2015, a work by Tajalizadehkhoob et al. [50] explored the incentives and strategies of attackers by analyzing the instructions sent to machines infected with Zeus malware between 2009 to 2013. They highlighted that on average, code similarity is well over 90% across all Zeus versions. This suggests heavy code reuse, selling, or perhaps stealing among hackers. Another study looked at the life cycle of Zeus botnet, its attack behavior, topology and technology based on two versions 1.2.7.19 and 2.0.8.9 [36].

Shifting from the traditional domain to the mobile-based malware, we found that the generic mobile malware has quickly evolved becoming more focused on extracting profits. Although this already became a real concern for industry [27, 35], there exists only a few studies of Android financial malware on the academic side. The first one was presented by Jung et al. [37] which tested some of the major Android-based banking apps to verify whether a money transfer could be made to an unintended recipient through a repackaging attack. The experimental results showed that this repackaging

attack is possible without having to illegally obtain any of the sender's personal information, such as the senders public key certificate, the password to their bank account, or their security card. In 2015, Rasthofer et al. [51] analyzed the behavior of Android banking malware family called *BadAccents*. They described in detail the techniques this malware family used and confronted them with current state-of-the-art static and dynamic code-analysis techniques for Android applications. Additionally, several authors investigated the holistic security of mobile money applications including mobile banking, mobile wallets, and mobile payment apps. Reaves et al. [46] performed a comprehensive analysis of branchless banking applications. They discovered vulnerabilities using the Common Weakness Enumeration (CWE) classification system and showed that six of the seven applications fail to preserve the integrity of their transactions. Similarly, Darwish and Husain [25] presented an intensive security analysis of mobile banking and mobile payment on Android platform. They found 80% of the selected applications were not following the best security practices, which is defined in the AndroBugs report [14]. On the other hand, de Almeida [18] and Harris et al. [32] presented the policy implications of the insecurity of mobile money.

Overall, none of these studies offer a comprehensive understanding of Android financial malware necessary for building effective defences against financial mobile malware. In this paper, we fill this gap and propose a taxonomy that will facilitate the Android financial malware detection. Since the majority of mobile malware targets Android platforms, in this work, we only focus on this platform. However, the attack and defence mechanisms we discuss are applicable to all types of mobile platforms. This has been proven true by Mylonas et al. [44] in their study on the feasibilty of malware attacks in various smartphone platforms such as Windows Mobile, Blackberry, Apple iOS, and Android. The study presented a comparative evaluation of different smartphone platforms by analyzing their protection against simple malicious applications. The study also showed that all examined platforms can become the target of privacy attacks especially on data theft e.g., harvesting data from the device without the users consent.

3 Methodology

The aim of this study is to provide a comprehensive guideline in understanding the threat landscape of the Android financial malware, which can be used as a research foundation for the effective mobile malware detection system. In seeking to understand the threat landscape, we addressed the following

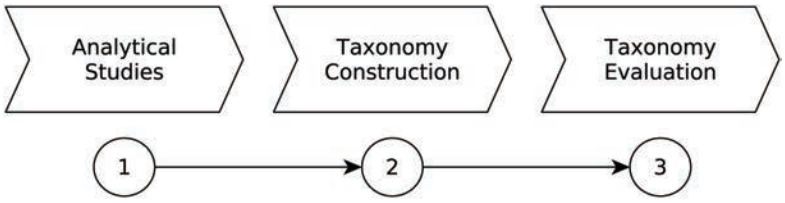

Figure 1 Overview of the research phases.

research questions: (a) Can the current detection system detects Android financial malware?, (b) how does Android financial malware different from the general malware?, and (c) What are the unique characteristics of Android financial malware? To answer these questions, the study is carried out in three stages, as shown in Figure 1. Following are the description of each stage:

1. **Analytical studies:** this stage is to conduct a critical analysis of the current detection systems towards Android financial malware. The goal is to examine the detection ratio of current detection tools towards Android financial malware (Section 4: Analytical Studies).
2. **Taxonomy construction:** this stage presents the proposed taxonomy of Android financial malware, which aim to improve the understanding and knowledge of the current systems (Section 5: Proposed Taxonomy).
3. **Taxonomy evaluation:** this stage evaluates the proposed taxonomy presented in Stage 2. An evaluation of this taxonomic model towards Android financial malware implies the possibility for introducing an automatic malware categorization, which can effectively save the time of malware analysts to correlate various symptoms of malicious behavior (Section 6: Characterization).

3.1 Dataset

We gathered a large collection of Android financial malware samples representing 32 malware families. Our accumulated dataset combines samples from the Android Genome Malware project [57], malware security blogs [42], as well as samples provided by anti-malware vendors and security researchers [31, 38]. Only unique samples (based on their hash value) were retained in the dataset. Overall, our dataset includes 1758 unique samples spanning a period of 2010 (the first appearance of Android malware) to 2015. To ensure correct labeling of samples, we inspected our dataset with VirusTotal malware analyzer [2]. VirusTotal aggregates 63 antivirus products and online scan engines for analyzing suspicious files and URLs, and for detecting the types of

Table 2 The breakdown of Android financial malware by categories

Category	Total Number of Families	Total Samples
Adware	4	151
Banking Malware	10	973
Ransomware	7	408
SMS Malware	5	82
Scareware	6	144
Total number of samples		1758

malware including viruses, worms, and trojans. We generated a python script to scan all samples in our dataset; out of 63 engines available on VirusTotal, we only selected the labelling provided by F-secure and Kaspersky as they were able to successfully label the largest number of samples. Finally, we run another script to correlate the results between F-secure and Kaspersky for creating unique samples of malware family[2]. Table 2 shows the total number of malware collected.

4 Analytical Analysis

In this section, we present an analysis of the financial malware that we have in our dataset. The objective is to evaluate the current detection systems towards Android financial malware. We inspect the dataset by scanning it with VirusTotal as it aggregates 63 different AVs.

Table 3 presents an example of one category which is the banking malware that are labelled by AVG. We chose to follow AVG simply to analyze consistency of labelling by the same provider. Besides, AVG mobile app is one of the popular mobile apps in the market, and exceeded 100 million of downloads on Google Play by May 2017 and is increasing every day [13]. To check the accuracy of malware detection, we chose to analyze the highest number of samples in our dataset, which is banking malware. Out of 973 banking malware samples, around 3% (49 samples) are not detected or in other words seen as legitimate apps by the AVG. We labelled these 49 samples as Undetected (Table 3). Similarly, in order to check the accuracy of malware labeling, we also implemented the same process but for all other categories that we have in our dataset. We first scanned all the 1758 samples with AVG engine and then calculated the frequency of each label provided by AVG for each malware family (we labelled them as *most frequent label*. The results for all five categories of Android financial malware are listed in Table 4.

[2]The uniqueness was judged by different hash values.

Table 3 An example of Android banking malware family detected by AVG engine

Family	Malwarelabel Given by AVG	Total
Bankbot	AVG#Android ctl2	2
	AVG#Android dc	2
	AVG#Android/Deng	95
	AVG#Android/G2M	9
	AVG#Android/Generic	23
	AVG#Android/Zitmo	2
	Undetected	3
Binv	AVG#Android/Rl.EBN	1
	AVG#Android dc	1
Citmo	AVG#Android/Citmo	3
Fakebank	AVG#Android/SpyBanker	1
	AVG#Android/SpyBanker	8
	AVG#Android ctl2	4
	AVG#Android dc	1
	AVG#Android/Deng	96
	AVG#Android/FakeBank	44
	AVG#Android/G2M	4
	AVG#Android/G2P	1
	Undetected	2
Sandroid	AVG#Android/Generic	12
	AVG#Android/Deng	29
	AVG#Android/G2P	1
	Undetected	19
SMSspy	AVG#Android/Deng	43
	AVG#Android/G2M	2
	AVG#Android/G2P	85
	AVG#Android/SMSAgent	1
	AVG#Android/Deng	21
	AVG#Android/Generic	1
	AVG#Android/Spitmo	131
	AVG#Android/Zitmo	38
Wroba	AVG#Android ctl2	1
	AVG#Android/Deng	104
	AVG#Android/G2M	3
	AVG#Android/SMSAgent	13
	Undetected 1	13
Zitmo	AVG#Kamel	5
	AVG#Android ctl2	3
	AVG#Android dc	1
	AVG#Android/Agent.C	2
	AVG#Android/Deng	66
	AVG#Android/G2M	10
	AVG#Android/Zitmo	43
	Undetected	12
ZertSecurity	AVG#Android/Deng	2
	AVG#Android/G2M	2
Total 973		

Table 4 Comparison of malware family detection

No.	Family Name	Year	Total	AVG Engine Most Frequent Label
1	Adware-Kemoge	2015	100	Android/Deng
2	Adware-Mobidash	2015	25	Android/G2P
3	Adware-Selfmite	2014	2	Android/Deng
4	Adware-Shuanet	2015	24	Android/G2P
5	Banking Malware-Bankbot	2015	136	Android/Deng
6	Banking Malware-Binv	2014	2	Android/Rl
7	Banking Malware-Citmo	2012	3	Android/Citmo
8	Banking Malware-FakeBank	2014	151	Android/Deng
9	Banking Malware-Sandroid	2014	61	Android/Deng
10	Banking Malware-SMSspy	2013	131	Android/G2P
11	Banking Malware-Spitmo	2011	191	Android/Spitmo
12	Banking Malware-Wroba	2014	152	Android/Deng
13	Banking Malware-ZertSecurity	2013	4	Android/G2M
14	Banking Malware-Zitmo	2010	142	Android/Deng
15	Ransomware-FakeDefender	2013	44	Android/Deng
16	Ransomware-Koler	2014	74	Android/Deng
17	Ransomware-Pletor	2014	16	Android/Deng
18	Ransomware-RansomBO	2014	100	Android/Deng
19	Ransomware-ScarePakage	2014	2	Android/G2M
20	Ransomware-SimpleLocker	2014	72	Android/Rl
21	Ransomware-Svpeng	2014	100	Android/Deng
22	Scareware-Avpass	2013	25	Android/G3P
23	Scareware-FakeAV	2013	25	Android/G2P
24	Scareware-FakeFlash	2013	12	Android/G2M
25	Scareware-FakeJobOffer	2013	7	Android/Fakejoboffer
26	Scareware-FakePlayer	2010	25	Android/G2M
27	Scareware-Penetho	2012	50	Android/G3P
28	SMS Malware-Gazon	2015	1	Android_dc
29	SMS Malware-GGTracker	2011	11	Android/G2P
30	SMS Malware-Plankton	2011	20	Android/AirPush
31	SMS Malware-Uxipp	2011	25	Android/G2M
32	SMS Malware-YZHCsms	2012	25	Android/G2M

Overall, the first result indicates that the AVG is able to detect the malicious apps with 98% detection, however the AV is not capable of detecting the category of Andoid financial malware in our dataset. As can be seen in Table 3, none of the labels indicate the banking nature. The second result demonstrates an inconsistent labelling of malware family: about 40% (12 out of 32 families) are detected as *Android Deng* family. This non-standardization leads to confusion and inaccuracy. As such, we propose a taxonomy (Section 5) to unify terminology in the field of malware research.

5 Proposed Taxonomy

Since 2014, most of the security reports [9, 11, 35] have referred to Android financial malware as banking fraud. However, the modern Android financial malware ranges from keyloggers to spyware to ransomware and botnets. For example, an advanced Android malware called *Zitmo (Zeus in the mobile)* is not only capable of stealing financial information but also launching a banking malware attack. Similarly, *Svpeng* banking malware has ransomware in its arsenal. The lack of a unified vocabulary and inconsistent understanding of Android financial malware amongst security researchers led us to define the term for Android financial malware.

We refer an *Android financial malware as a specialized malicious software (malware) designed to direct financial profit to the fraudsters with or without the user's knowledge and consent.* This includes any reselling of victim's data, or direct transactions between the victim and the cybercriminal. As visualized in Figure 2, typically, the Android financial malware uses one of the following avenues to gain financial profit:

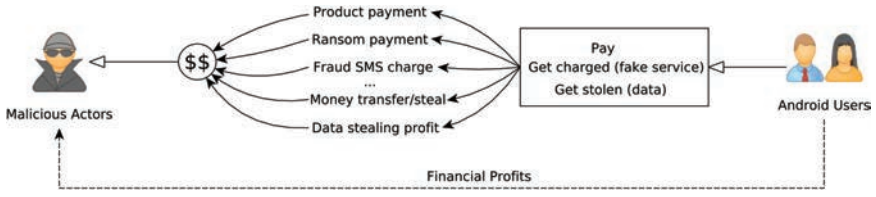

Figure 2 Android financial malware.

- Product payment: to persuade a user to buy fake apps or fake services.
- Ransom payment: to regain control over the mobile devices by locking the mobile screen or encrypting the personal data stored on the mobile devices.
- Fraud SMS charge: to exploit the mobile service (phone billing system) to subscribe a user to a premium-rate SMS service without the user's consent.
- Money transfer: to steal the login credentials for online banking and credit card information by replacing the authentication fields of Android apps (e.g. mobile banking apps) on the infected mobile devices.
- Data theft: to gather sensitive information by stealing personal data (banking information, social insurance number).

5.1 Android Financial Malware Classification

Although the majority of the existing studies in the field attempt to provide some classification, they often contradict each other in defining various attack types related to Android financial malware, resorting to inconsistent terminology and vague descriptions of any given attack types. For example, a report by Kaspersky refers to *trojan SMS, trojan banker,* and *ransomware* as the Android financial malware [11]. Sophos classifies mobile money making schemes into *premium-rate SMS, banking malware, ransomware, pay-per-click fraud, social media spam,* and *fake security software* [9]. On the other hand, several existing studies resort to a generic term to categorize all types of financial malware. For instance, IBM refers the attack types of financial malware as *fraudulent transactions* [35].

This lack of unified vocabulary emphasizes the need for comprehensive understanding of the existing Android financial malware. A unified terminology is a necessary foundation for the advanced development of an effective defense mechanism against these type of attacks. In this research, we address this problem and propose a taxonomy for Android financial malware as given in Figure 3. The defined taxonomy and classification are based on the smartphone's functionality and techniques the cybercriminals are using to gain the financial profit. There are three elements of mobile devices which can be exploited by the cybercriminals:

1. Mobile service - the mobile services such as SMS, MMS, and Bluetooth can be exploited as a platform to spread the malware attacks. Due to its popular monetization, we focus only on SMS and refer to this type of exploitation as *SMS malware*.

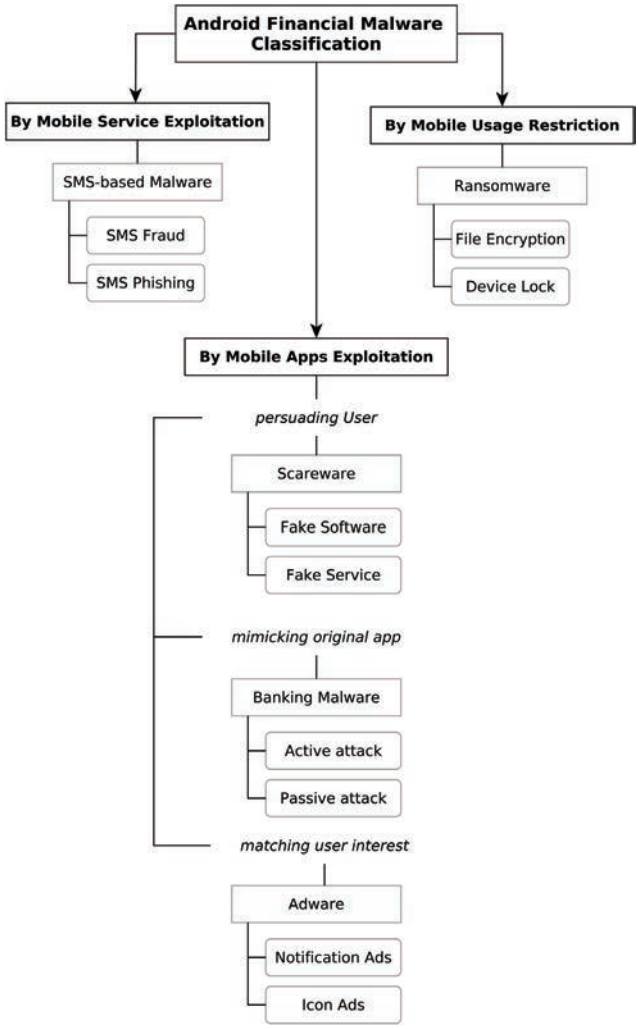

Figure 3 Proposed taxonomy of Android financial malware attack types.

2. Mobile usage - the mobile usage can be restricted by blocking the user to access the mobile device or some files stored in the mobile device; user has to pay ransom in order to regain control over the mobile device. This exploitation is known as *ransomware*, which can be divided into two types: encryption-based and device-locking.
3. Mobile apps - the mobile apps typically serve as a vehicle for rapid distribution of malware. There are three different ways of exploiting apps:

- *by persuading user to download the infected apps*: when the cybercriminals make money from the malicious apps by threatening victims to download the apps or convincing them to pay some amount of money for the fake service. We refer to this technique as *scareware*.
- *by mimicking original apps*: typically popular apps such as Uber, WhatsApp, Facebook including the banking apps are used for attacks. In this research, we only focus on the financial apps, i.e. banking apps. We name this category *banking malware*.
- *by matching user interest with the apps*: when the cybercriminals exploit the app advertisement by posing a threat to user personal information and interfere in user activity. The malware displays the related ads based on the user's interest. We call this category *adware*.

In the remainder of this section we provide details on each of the categories in the given classification, which cover various forms of financial malware including SMS malware, ransomware, banking malware, scareware, and adware.

5.1.1 Mobile service exploitation (SMS malware)

SMS Malware is a financial malware that uses the SMS service as its medium of operation to intercept SMS payload for conducting attacks. Depending on how the cybercriminals gain profit through SMS service abuse, we distinguish two types of SMS malware: SMS fraud and SMS Phishing.

1. **SMS fraud.** SMS fraud refers to the exploitation of phone billing service which is called mobile premium service (sms premium-rate). This service is favoured by many legitimate service providers due to its ease of use as a mobile payment mechanism. For instance, the users can order a variety of mobile content (e.g. ringtones, wallpapers, donation), receive the ordered content, and the fee will be charged to the phone bill directly. Once the transaction is completed, the aggregator (middleman) who maintains the technical service pays the service fee to the service providers. To subscribe or receive an advertised content, a user typically has to send an SMS to a given number. Figure 4 illustrates how an attacker exploits the premium-rate service by subscribing a victim to a vast numbers of premium service providers silently. In this SMS fraud, the attacker sets up its own service provider and receives money from the aggregator based on the number of subscriptions. Depending on country, some services require an acknowledgement from a user before

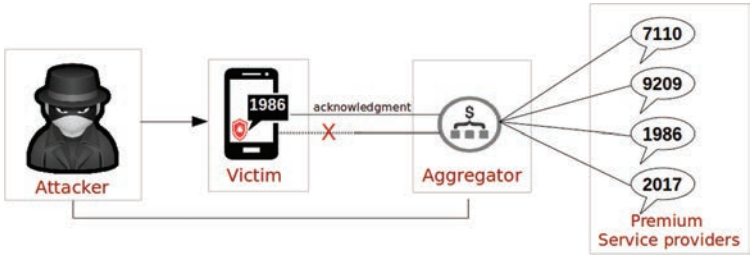

Figure 4 Premium-rate SMS fraud attack.

the charge is processed, as part of the service providers procedure. However, the attackers have exploited this mechanism by intercepting the acknowledgement messages from an infected mobile device without the user's consent. As a result, the fraud is continuous and rarely caught after the first occurrence [29].

2. **SMS Phishing.** Traditionally, SMS Phishing or SMiShing refers to a form of phishing that use the social engineering technique as a method of information retrieval to acquire user's sensitive information. For instance, a fraudster sends victim an SMS message asking for the sensitive information including credentials via a Web link or a telephone number. In the context of Android financial malware, we refer SMS Phishing as a method of malware distribution that spreads through SMS messages and persuades user to perform several actions, as depicted in Figure 5.

There are two ways of distributing malware via SMS messages: spoofing and malicious apps. SMS Phishing via spoofing refers to the manipulation of the sender's information by changing the originating mobile number with different international codes or networks for the purpose of impersonating another person, company, and product. This technique leverages free SMS services that allow to freely spoof SMS messages. Such services are created mainly for users that do not own a mobile phone but need to send an SMS from a number that they have provided to the receiver in advance. However, the attackers are making use of this service as a medium of propagating malware. *MozarBot* is an example of SMS spoofing technique employed by the Android botnet. This SMS malware is impersonating the legitimate organization in Denmark i.e. Post Denmark. By clicking on the shortened URL in the spoof message, a victim downloads the infected Android installation application file (.apk) for *MozarBot.*

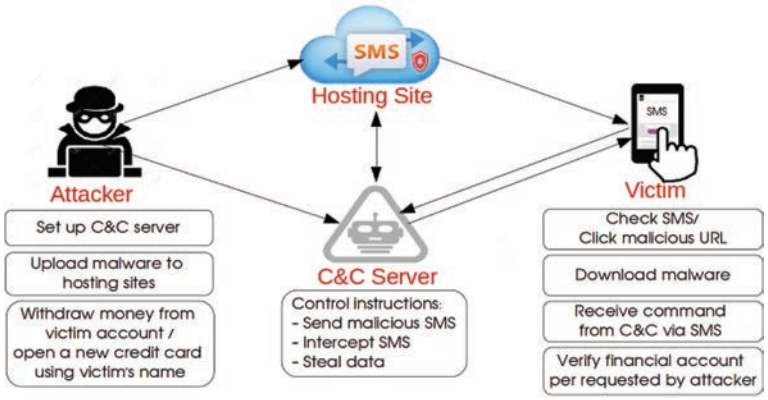

Figure 5 SMS Phishing scam.

SMS Phishing via malicious apps consists of several processes: the attackers first upload malware to their hosting sites to be linked with the SMS. They use the C&C server for controlling their attack instructions i.e. send malicious SMS, intercept SMS, and steal data. Once the victim received the SMS and visited the malicious URL, the malware is installed on the victim's device without the victim's knowledge [1]. After installation, the malware shows typical phishing behavior requesting device administrator privileges and remaining in the background to perform a series of malicious actions. Typically, these actions include the following: (1) intercept and capture all incoming and outgoing SMS messages (2) receive command and control (C&C) commands via SMS e.g. sends an SMS text message to every contact in the victim's phone book (3) steal sensitive information (e.g financial data) by intercepting SMS messages based on pre-defined keywords, such as *Pay, Check, Bank, Balance, Validation*. All obtained information is relayed to a remote C&C server. As a result, the attacker is able to withdraw money from the victim's account or open a new credit card by using the victim's personal information. *Nickyspy* is an example of malware that spreads through SMS Phishing via drive-by download without the victim's knowledge. The SMS message contains the request link for an important update allegedly sent by the user's service provider. Once clicked, the link downloads the malware and executes the loader, which crashes the device and installs the actual malware components while rebooting [1].

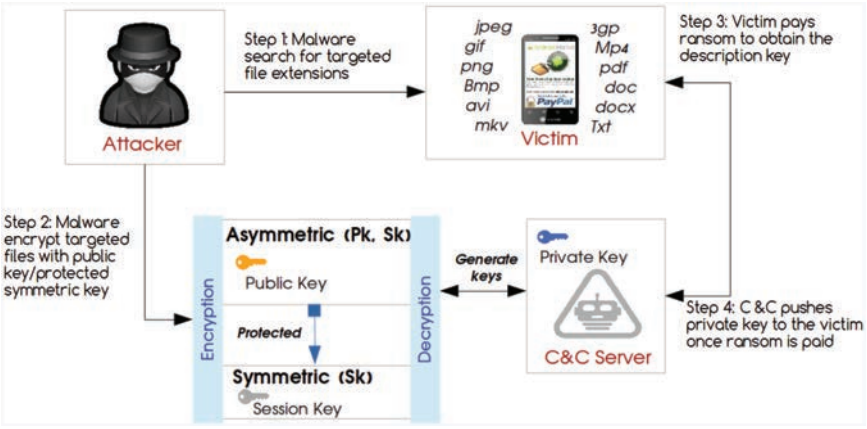

Figure 6 Encryption-based ransomware with dual encryption.

5.1.2 Mobile usage restriction (Ransomware)

Android ransomware is inspired by the desktop ransomware, which restricts usage of the infected device and demands a ransom from the infected user in order to regain control over the device or personal data. There are two variants of Android ransomware that are common today:

1. **Encryption-based ransomware** - this type of ransomware employs an encryption technique to encrypt documents and to secure the communication between the malware and its C&C server. Also, this ransomware holds a key necessary to decrypt data to the original unencrypted form. Since the security restrictions built into the Android OS prevent the malware from encrypting files stored on the device's internal memory, it encrypts data stored on external SD memory cards that typically contain personal data such as text files, pictures, and videos. The cybercriminals combine both symmetric and asymmetric encryption. Since symmetric encryption is efficient in terms of performance, the victim's files are encrypted using symmetric encryption and a session key. This session key is also encrypted by public key. Such use of asymmetric encryption is convenient as it enables the malware operator to protect only one private key that is needed for the decryption regardless of the number of victims. The malware has different ways of storing the decryption keys. Some malware families fetch the decryption key online through C&C server once ransom is paid. An older malware stores a key inside the malware code (e.g., SimpleLocker). But most frequently the ransomware's private

key is embedded into the malware or fetched from the C&C server (e.g., RansomBO). After the encryption, the symmetric key is often stored on the affected device. Figure 6 presents an example of an encryption-based ransomware with dual encryption that combines assymmetric and symmetric encryption. There are four steps of encryption-based ransomware: (1) File search: the malware look up for specific file extension such as jpeg, jpg, png, bmp, gif, pdf, doc, docx, txt, avi, mkv, 3gp, mp4 (2) File encryption: the malware encrypt the targeted files via asymmetric and symmetric encryption methods. (3) Ransom Payment: In order to decrypt the files, the victim has to pay for the ransom. Once the ransom is paid, the victim receives the decryption key online via C&C server. (4) File decryption: C&C server fetches the private key to the victim once ransom is paid.

2. **Device-locking ransomware** - this ransomware aims to block the access to the compromised device by locking the device's screen. Starting with an Android 4.2, Android's lock screen supports a variety of different unlock methods as well as widgets. There are five different options of lock mechanism that have been developed by Android: *slide, face unlock, pattern, PIN, password.* But any user selected lock mechanism will be replaced by random PIN number set by malware. This type of ransomware is irreversible, even if a user pays the ransom, the device

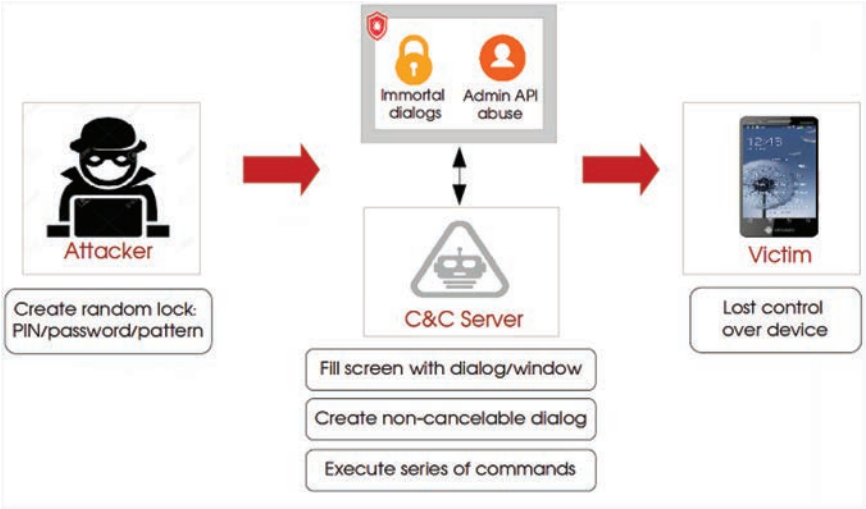

Figure 7 Device-locking ransomware.

cannot be unlocked because the attackers do not keep track of these random PIN numbers. Without device administrator privileges or without some other form of security management solution installed, users have no effective way of regaining access to their device. The only practical way to unlock is to reset to factory defaults which would delete all the data. The attackers maintain the communication although the user has no ability to access the device (Figure 7). Typically, the attackers maintain communication with an infected locked device through the C&C server. If a C&C communication channel is established, the malware can execute commands and take over control of the infected device. Some examples of commands in ransomware, include: a) send an SMS message to phone contacts, b) steal received SMS messages and harvest contacts, c) enable or disable mobile data and Wi-Fi, and d) track user's GPS location.

5.1.3 Mobile apps exploitation (Banking Malware, Scareware, Adware)

1. **Banking Malware.**
   Android banking malware refers to the specialized malware designed to gain access to the user's online banking accounts by mimicking the original banking applications or banking web interface. Based on its behavior, the Android banking malware can be categorized into two groups:
   - **Active banking malware** is designed to steal account credentials by removing the two-factor authentication system. A popular approach involves Transaction Authentication Number (TAN) theft. TAN is used by online banking services as a form of single use one-time passwords to authorize financial transactions. When the bank receives a request from the user (either via mobile or desktop), it generates the TAN and sends it via SMS to the bank customer's device. This process is intercepted by the banking Trojan malware that extracts the TAN and sends it back to the bank to gaining access to bank account to complete one time the illegal banking transaction (e.g. funds withdrawal). The users awaiting for the TAN typically think that their request is not delivered and therefore request another TAN number. The visual representation of the process is shown in Figure 8.
   - **Passive banking malware.** In contrast to the active banking malware, the passive malware is designed to monitor the use of mobile

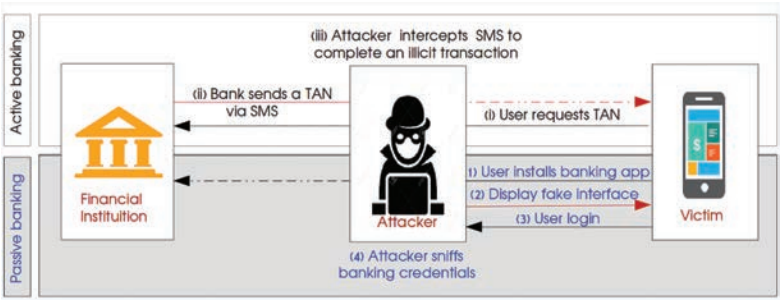

Figure 8 Active vs Passive banking malware attacks.

banking apps. This type of banking Trojan disguises itself as legitimate apps (i.e. Google Play Store apps) and once installed, it will run as a service in the background tomonitor events on the host device. This enables it to capture incoming SMS, monitor installed apps, and communicate with a remote server. The malware then searches for the existence of any targeted banking apps on the victim's mobile. If any results found, it will remove and download a malicious version to replace the original apps. This malicious version displays a fake user interface asking for user to input their credential information. The attackers then can sniff the banking credentials for illegal banking transaction. They can also capture other useful data that generate revenue for them (e.g. credit card number). Figure 8 shows the difference between active and passive banking malware attacks.

2. **Scareware**. Android scareware is a malicious software that poses as legitimate apps and falsely claims to detect a variety of threats on the affected mobile device (i.e. battery issues, malware threats). Similar to ransomware, the scareware exploits human emotions (cause panic, shock, anxiety) to manipulate users. Typically, users are first offered to download apps or to buy the fake services, which are claimed from a trusted source (e.g. live wallpapers, photo editors, radio apps, fake anti-virus, gaming apps). But instead of getting money as a ransom, in scareware attack, the cybercriminals receive money as a product payment for the malicious apps. Some scareware masks itself as a legitimate apps, which makes it looks legitimate and difficult for the detection system such as Google Bouncer[3] to identify it as scareware.

[3]http://googlemobile.blogspot.ca/2012/02/android-and-security.html

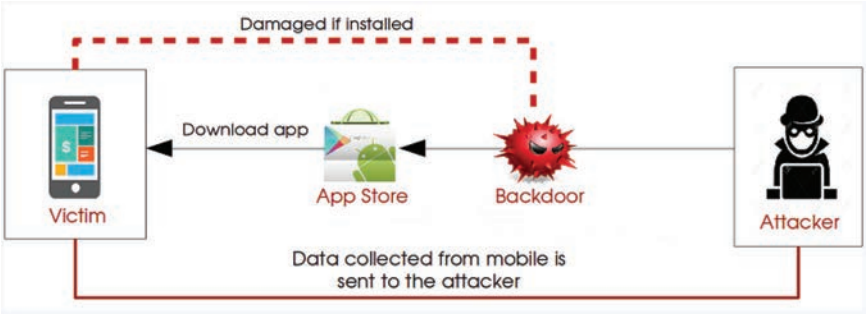

Figure 9 Android scareware attacks.

Figure 9 shows how the attack of typical scareware works. Once the victim downloads the malware, some form of notifications continue to pop-up on the device, falsely alerting the victim that the mobile device is infected and requires a security solution and protection. The damage effects of scareware usually fall into one of two categories:

- to deceive victims into paying for fake security service. For instance, paying for the threats cleanup of non-existent infections on the device. Typically, the scanning process to find the false threats is free, but the cleanup process is not. If victims pay for the cleanup service, the app remains indefinitely to perform fake updates by using a Java-based pseudo-random-number generator (PRNG) that consequently leave the device vulnerable to real malware threats.
- to deceive victims into downloading and installing malware. For example, downloading and installing fake anti-virus (fake AV) to protect the device. Usually, after downloading and installing fake AV, the victim receives a fake progress bar with the infection result of a range of different malware randomly (e.g. Malware Tapsnake). The scareware also opens a backdoor to give attackers remote access to the device. This access remains on the device even afterthe malware app is removed, which leads to more attacks: sign up the victim to a premium-rate SMS, install an advanced Mobile Remote Access Trojan (mRAT) to steal the victim's personal data (banking credentials and other sensitive information), take pictures and relaying them to the attacker's server. The attack process becomes more attacker-friendly as the victim believes that the malware is an AV app, which causes victims to grant the malicious apps with all the permissions and access that it requests.

3. **Adware.** Android adware refers to the advertising material (i.e., ads) that typically hide inside the legitimate apps. e.g., *Candy Crush, Google, Facebook, Twitter* which have been infected by malware (available on the third-party market). Similar to scareware, adware also prompts victim to install another app in order to launch its attack. However, once installed, the adware continuously pops up ads through a third-party library even if the victim tries to force-close the apps. This is because the ad library that used by the malware repeats a series of steps to keep the ads running: (a) runs code with a number of processes, (b) creates a file then locks it (each process creates another file), (c) monitors the lock status of files (if any file is unlocked, another process is generated again). The damage effects of adware typically fall into one of three categories (Figure 10):
    - to display advertising content based on the user's interest (which links to a malicious site). This behavior is considered unwanted if the victim is unaware of the presence of the module of the advertising materials displayed. There are two ways of displaying ads: (1) notification ads: the ads deliver alerts to the mobile's notification bar when the user swipes the notification bar from the top of the screen. The notification ads technology has been used by mobile marketing firms and app developers (e.g., Facebook and Groupon) to send updates and deal alerts to their customers, but this platform has been exploited by the attackers. (2) icon ads: the ads are inserted onto a mobile's homescreen or desktop shortcuts and usually launch a search engine or a web service which links to a malicious site when the user touches the icon (e.g. redirect homepages to malicious site).
    - to harvest sensitive details from the device such as the International Mobile Equipment Identity (IMEI) number, location, contacts, and sensitive information (e.g., credit card information, banking information) which can link to the banking malware attacks.
    - to root an infected device for the admin privilege escalation, which makes it difficult to remove the adware. The mobile apps typically have no access to files created by other applications, but the root privilege granted by the attacker bypasses this safeguard and expose the infected devices to fraud and identity theft.

Unlike normal adware, the financial adware aims on multiple platforms in generating revenue; instead of using the JavaScript code to click on advertisements, the financial adware inserts its code into a Google-owned mobile advertising platform (i.e. Admob) to stimulate the automatic ad clicking

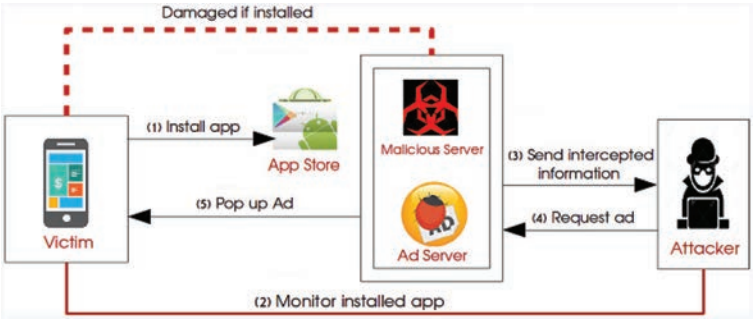

Figure 10 Android adware attacks.

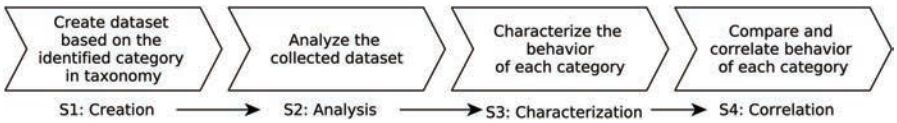

Figure 11 Stages of taxonomy evaluation.

and pop ups in other apps' download links in the Google Store in order to earn more stream for the revenue.

6 Taxonomy Evaluation

In this section, we present the taxonomy evaluation of the Android financial malware. Figure 11 depicts the major phases of the evaluation process: a) Stage 1: Dataset creation, which is to create a dataset based on the identified category in the taxonomy. b) Stage 2: Analysis, which is to analyze the collected dataset in Stage 1 c) Stage 3: Characterization, which is to characterize the behavior of each malware category d) Stage 4: Correlation, which is to compare and correlate the behavior of each malware category.

6.1 Stage 1: Dataset Creation

To create a dataset which is based on the identified category in the taxonomy, we followed the same procedure of data collection and labeling in Section 3.1. Additionally, we generated another shell script for categorizing the samples into second-level category (adware notification, adware icon, banking active attack, banking passive attack, scareware fake software, scareware fake service, ransomware lock, ransomware encrypt, sms fraud, and sms phishing)

as shown in Table 5. The script is based on the hash value of all 32 families that are generated in Section 3.1. The malware categorization in Table 5 demonstrates a systematic overview of malware information, which is useful for malware analyst during the malware triage process.

Table 5 Android financial malware dataset based on taxonomy categorization

No	Family Name	Category	Second-Level Category	Year of Discovery	No. Samples
1	Avpass	Scareware	Fake Software	2013	25
2	Bankbot	Banking	Active Attack	2015	136
3	Binv	Banking	Active Attack	2014	2
4	Citmo	Banking	Active Attack	2012	3
5	FakeAV	Scareware	Fake Software	2013	25
6	FakeBank	Banking	Passive Attack	2014	151
7	FakeDefender	Ransomware	Device-Locking	2013	44
8	FakeFlash	Scareware	Fake Software	2013	12
9	FakeJobOffer	Scareware	Fake Service App	2013	7
10	FakePlayer	Scareware	Fake Software	2012	25
11	Gazon	SMS-based	Phishing	2015	1
12	GGTracker	SMS-based	Fraud	2011	11
13	Kemoge	Adware	Notification Ads	2015	100
14	Koler	Ransomware	Device-Locking	2014	74
15	Mobidash	Adware	Icon Ads	2015	25
16	Penetho	Scareware	Fake Software	2012	50
17	Plankton	SMS-based	Phishing	2011	20
18	Pletor	Ransomware	Device-Locking	2014	16
19	RansomBO	Ransomware	Encryption-Based	2014	100
20	Sandroid	Banking	Active Attack	2014	61
21	ScarePakage	Ransomware	Device-Locking	2014	2
22	Selfmite	Adware	Icon Ads	2014	2
23	Shuanet	Adware	Notification Ads	2015	24
24	SimpleLocker	Ransomware	Encryption-Based	2014	72
25	SMSspy	Banking	Active Attack	2013	131
26	Spitmo	Banking	Active Attack	2011	191
27	Svpeng	Ransomware	Device-Locking	2014	100
28	Uxipp	SMS-based	Fraud	2011	25
29	Wroba	Banking	Passive Attack	2014	152
30	YZHCsms	SMS-based	Fraud	2012	25
31	ZertSecurity	Banking	Active Attack	2013	4
32	Zitmo	Banking	Active Attack	2010	142
Total number of samples					1758

6.2 Stage 2: Analysis

After categorizing the malware family into a specific category based on the proposed taxonomy, we then analyzed each category in our dataset. Our focus is to understand the following research questions: (1) How does the malware spread to the Android users? (2) How does the malware activate itself on the phone? (3) What happens after the malware has reached the Android system? To answer these questions, we analyzed the malware samples in our dataset and compiled the following main characteristics of each Android financial malware categories: malware installation (Table 7), malware activation (Table 9), and malware attacks (Table 10)[4]. The summary of these characteristics is provided in Table 6. The analysis information is based on the malware reports compiled from several Antivirus vendors such as Fortinet [5], Kaspersky [3], Avast [4], and other security blog [7, 8].

6.3 Stage 3: Characterization

Malware Installation. In order to evaluate the Android financial malware, we first need to understand how malware lands on a phone and gets activated. By inspecting the malware samples in our collection, we categorized the ways Android malware are to be installed:

1. Repackaging: is a common technique used by the attackers to plagiarize or stealing the legitimate applications in creating the malicious ones. Due to its openness, the attackers can easily change the code and sign the applications with a self-signed certificate. To check the presence of repackaging in our dataset, we employed FSquaDRA (Fast Detection of Repackaged Applications) [56]. FSquaDRA uses a pairwise application comparison to compute similarity between apps, which is based on a variety of metrics such as Euclidean, Block, Jaccard, Cosine, and to name a few. We used the Block metric in our analysis as it gave us more results of similarity with the higher scores. In total, among the 1 758 malware samples, FSquaDRA detected 56 525 pairs of similar apps. Following the defined repackaging threshold of 0.7 similarity score, we found 17 480 pairs (30.92%) were repackaged. We also calculated the average of the similarity for each category: 40.56% ransomware, 32.50% SMS malware, 26.98% Banking, 26.93% scareware, and 0% adware. We then looked deeper into the adware results and found that the highest

[4]Note: The number shown on these tables is the average of malware family per category (%).

Table 6 Analysis of Android financial malware dataset

		Repackaging	Update Attack	Social Engineering	Boot	SMS	Network	Call	USB	Package	Battery	System	Botnet Functionality	Information Theft	Spam/ Phishing	Privilege Escalation	Functionality Exploitation	Geographic location
Category	Types Category	Malware Installation						Malware Activation							Malware Attacks			
SMS-based	SMS Fraud	√	√	√	√	√		√		√	√		√	√			√	
	SMS Phishing	√	√	√	√		√	√		√		√	√	√	√			√
Ransomware	Encryption-based	√		√	√	√	√	√		√	√	√	√		√		√	√
	Device-locking	√		√	√	√		√		√		√	√	√	√		√	√
Scareware	Fake Software	√	√	√	√	√	√	√		√	√	√	√	√	√	√	√	√
	Fake Service Apps	√		√	√		√	√				√	√				√	
Banking	Active Attak	√	√	√	√	√		√		√			√	√	√		√	√
malware	Passive Attack	√		√	√								√	√	√		√	√
Adware	Notification Ads		√	√	√			√	√	√		√				√		√
	Icon Ads			√	√			√					√	√	√			√

similarity score for one of the adware families named Shuanet is 0.655 (with only 1 pair), which is below the threshold. This indicates that the adware samples in our dataset are unique.

2. Update Attack: similar to the repackaging method, update attack technique also exploits the legitimate apps but specifically on the update component. For instance, instead of repackaging the whole application with malicious payload, it includes an update component that is activated at runtime. Once the program is installed on the user's mobile phone, it hijacks the Android update screen and notifies user that a new update is available. To quantify the update attack technique in our samples, a dynamic analysis is required (which is not the scope of this paper). As such, we manually inspect the malware family with the previous studies [10, 38, 57]. Overall we found approximately 31% (10 out of 32 families) that reported using the update attack technique in delivering the malware: 60% (3 families) from SMS malware category (*GGTracker*, *Plankton, YZHCsms*.), 50% (2 families) from adware category (*Kemoge*, *Shuanet*), 33% (2 families) from scareware category (*FakeAV, AVpass*), and 30% (3 families) from banking malware category (*Bankbot, Spitmo*, *Zitmo*).
3. Social Engineering: a method that requires user's participation to succeed without exploiting the browser. With social engineering, the attackers convince the user to download the malicious payloads, which may happen when checking an e-mail message, visiting a website or by clicking on a deceptive pop-up window. Social engineering can be done through various mediums such as SMS, fake application, email, and drive-by download. An example is the banking trojan called *Spitmo* family. This trojan asks the user to install a new updated app that can better protect banking activities. If the user installs the app, the trojan steals the banking credentials and send them to a remote server. By applying the similar approach when analyzing the update attack method, we found that all malware categories are using social engineering as a medium of malware delivery: 100% (all family) of scare-ware (*FakeAV, FakeFlash, FakeJobOffer, FakePlayer, Penetho*) 80% (8 families) of banking malware (*Bankbot, Binv, Fakebank, Sandroid, SMSspy, Spitmo*, *Wroba, Zitmo*) 60% (3 families) of SMS malware (*GGTracker, Plankton*, *YZHCsms*), and 44% (3 families) of ransomware (*Koler, Pletor, SVpeng*).

Malware Activation. This section further discusses the malware activation once they are installed on the phone. Android applications are typically

Table 7 Analysis of Android financial malware installation

Category	Types	Malware Installation (%)		
		Repackaging	Update Attack	Social Engineering
SMS-based	SMS Fraud	15	40	40
	SMS Phishing	18	20	20
Ransomware	Encryption-based	12	0	14
	Device-locking	28	0	29
Scareware	Fake Software	26	33	86
	Fake Service Apps	2	0	14
Banking malware	Active Attack	25	30	60
	Passive Attack	2	0	20
Adware	Notification Ads	0	50	50
	Icon Ads	0	0	50

divided into two categories: pre-installed and user-installed. Pre-installed applications include the original equipment manufacturer (OEM) or the mobile carrier-provided applications such as the calendar, email, browser and contact managers. User-installed applications refer to the applications that the user has installed (including the malicious applications) either through an app market such as Google Play or direct download or manually with adb install. Zhou & Jiang [57] claimed in their paper that the Android malware can launch its payloads by registering for the system events. Thus, we further investigate the system events of Android in order to examine the malware activation in our dataset; we reverse engineered the samples and generated a shell script to check the Android system events, which is based on the set of features including system boot, phone, package, system, SMS/MMS, USB storage, power battery, and network. Table 8 shows the list of these features with its abbreviation and action description[5].

The result in Table 9 and Table 11 demonstrate that most of the Android financial malware is executed with the system boot (BOOT). This is not surprising as this particular event will be triggered once the system finishes its booting process. In our dataset, 84% (27 malware families out of 32) listened to this event to bootstrap the background service.

[5]https://developer.android.com/reference/android/content/Intent.html

Table 8 Android system events

No.	Event Name (Abbreviation)	Events	Action Description
1	System Boot (BOOT)	BOOT_COMPLETED	Sent at boot by all devices. Upon receipt of this event, the user is unlocked
2	Phone (CALL)	PHONE_STATE	Indicates that the call state on the device has changed
		NEW_OUTGOING_CALL	Indicates that an outgoing call is about to be placed
3	Package (PKG)	PACKAGE_ADDED	A new application package has been installed on the device
		PACKAGE_REMOVED	An existing application package has been removed from the device
		PACKAGE_CHANGED	An existing application package has been changed (e.g. enabled or disabled)
		PACKAGE_REPLACED	A new version of an application package has been installed, replacing an existing version that was previously installed.
4	System (SYS)	USER_PRESENT	Sent when the user is present after device wakes up (e.g when the keyguard is gone)
		INPUT_METHOD_ CHANGED	An input method has been changed
		SIM_FULL	The SIM storage for SMS messages is full
5	SMS/MMS (SMS)	SMS_RECEIVED	A new text-based SMS message has been received by the device
		WAP_PUSH_RECEIVED	A new WAP PUSH message has been received by the device
6	USB storage (USB)	UMS_CONNECTED	The device has entered USB Mass Storage mode
		UMS_DISCONNECTED	The device has exited USB Mass Storage mode
7	Power Battery (BATT)	ACTION_POWER_ CONNECTED	External power has been connected to the device
		ACTION_POWER_ DISCONNECTED	External power has been removed from the device
		BATTERY_LOW	Indicates low battery condition on the device
		BATTERY_OKAY	Indicates the battery is now okay after being low
		BATTERY_CHANGED_ ACTION	Contains the charging state, level, and other information about the battery
8	Network (NET)	CONNECTIVITY_ CHANGE	A change in network connectivity has occurred. A default connection has either been established or lost.

Table 9 Analysis of Android financial malware activation

Category	Types	Malware Activation (%)							
		BOOT	SMS	NET	CALL	USB	**PKG**	**BATT**	**SYS**
SMS-based	SMS Fraud	60	40	0	60	0	20	20	0
	SMS Phishing	20	0	20	20	0	40	0	20
Ransomware	Encryption-based	43	14	14	57	0	29	14	14
	Device-locking	57	29	0	29	0	14	0	14
Scareware	Fake Software	67	50	50	83	0	67	17	67
	Fake Service Apps	17	0	17	17	0	0	0	17
Banking malware	Active Attack	70	30	0	50	0	10	0	0
	Passive Attack	20	0	0	0	0	0	0	0
Adware	Notification Ads	25	0	0	50	50	25	0	25
	Icon Ads	25	0	0	25	0	0	0	0

For instance, system boot event is triggered with the shell command *am broadcast -a android.intent.action.BOOT_COMPLETED*. This is followed by 78% (25 malware families) with the phone event (CALL): both of ransomware (6 families) and scareware (6 families) have 19% samples and only 9% of adware samples (3 families) registered to this event. We narrowed down the percentage into per category and found that scareware (fake software cattegory) has the highest number of CALL event with 83% of average, followed by SMS fraud (60%), and encryption-based ransomware (57%). The phone events indicate that the call state on the device has changed and an outgoing call is about to be placed. The package event is the third mostly used event, particularly in scareware. This event consists of four types where the application package can be added, removed, changed, and replaced. For instance, Penetho (scareware fake software) is a hacktool for Android devices that can be used to crack the WIFI password of the router but at the same time able to delete, destroy and steal data.

The SMS_RECEIVED is ranked forth with 11 malware families interested in intercepting or responding incoming SMS messages. This is reasonable as many malware intercept or respond to incoming SMS messages. For example, all samples of YZHCsms listens to the SMS_RECEIVED event and

Table 10 Analysis of Android financial malware attacks

Category	Types	Malware Attacks (%)					
		Botnet	Theft	Spam	Privilege Escalation	Exploit	Location
SMS-based	SMS Fraud	40	60	0	0	40	0
	SMS Phishing	40	20	40	0	0	40
Ransomware	Encryption-based	14	0	29	0	29	29
	Device-locking	29	14	29	0	29	14
Scareware	Fake Software	67	33	33	67	50	50
	Fake Service Apps	17	0	0	0	17	0
Banking malware	Active Attack	60	40	40	0	60	30
	Passive Attack	20	10	10	0	20	10
Adware	Notification Ads	0	0	0	25	0	50
	Icon Ads	25	25	50	0	0	50

intercepts or removes all SMS messages from particular originating numbers, i.e. “12345678911”. We also found that certain financial malware registers for a variety of events. For instance, Pletor registered all events except for USB storage. This is reasonable as the nature of Pletor is more sophisticated than other malware families. There are two variants of Pletor: the first uses the Tor network for communicating with its owners; the second uses more standard HTTP and SMS channels. Also, when the modifications demand encrypting money from the user, they display the victim’s image the contents using the smartphone’s front camera. Moreover, the fake software scareware and the encryption-based ransomware employed almost all of the events except for the USB. A work by Zhou & Jiang [57] highlighted that most of the Android malware in their dataset registered BOOT and SMS event. Our analysis of recent and more advanced mobile malware shows that in addition to the BOOT and SMS, events also register to CALL and PKG. We believe the registration of a large number of events is expected to allow the malware to quickly launch the carried payloads, which indicates the characteristic of financial malware.

Table 11 Malware characterization based on malware installation and activation

Malware Family	Category	Malware Activation								Malware Installation		
		BOOT	SMS	NET	CALL	USB	PKG	BATT	SYS	Repackaging	Update Attack	Social Engineering
Kemoge	Adware				√	√					√	√
MobiDash		√			√							√
Selfmite												√
Shuanet		√			√	√	√		√		√	√
Bankbot	Banking	√			√					√	√	√
Binv			√		√					√		√
Citmo		√	√		√							
FakeBank		√								√		√
Sandroid		√								√		√
SMSspy		√								√		√
Spitmo		√			√		√			√	√	√
Wroba		√								√		√
ZertSecurity		√	√	√								
Zitmo		√								√	√	√
FakeDefender	Ransomware	√	√		√				√	√		
Koler		√			√		√		√	√		√
Pletor		√	√	√	√		√	√	√	√		√
RansomBO		√								√		
ScarePakage		√	√		√							
SimpleLocker		√			√		√			√		
Svpeng		√			√					√		√

(*Continued*)

Table 11 Continued

Malware Family	Category	Malware Activation								Malware Installation		
		BOOT	SMS	NET	CALL	USB	PKG	BATT	SYS	Repackaging	Update Attack	Social Engineering
Avpass	Scareware	√	√	√	√		√		√	√	√	√
FakeAV		√	√		√		√		√	√	√	√
FakeFlash				√	√		√	√	√	√		√
FakeJobOffer		√		√	√				√	√		√
FakePlayer		√	√		√				√	√		√
Penetho		√		√	√					√		√
Gazon	SMS-based			√			√		√			
GGTracker		√	√		√			√		√	√	√
Plankton		√			√		√			√	√	√
Uxipp		√			√					√		
YZHCsms		√	√		√		√			√	√	√
Total number of families		27	11	6	24	2	12	3	9	24	10	24

Malware Attacks. This section presents the type of attacks for each category in Android financial malware: adware, banking malware, ransomware, scareware, and sms malware. To investigate the attack types, we reviewed security reports from multiple sources including Fortinet [5], Kaspersky [3], Avast [4], and other security blog [7, 8]. Based on the reviewed, we described the following attack types of Android financial malware in our dataset:

1. Information theft (A1): the malware is harvesting various information on the infected phones, including SMS messages, phone numbers as well as user banking accounts including the transaction authentication number (TAN). TAN is used by online banking services as a form of single use one-time password to authorize financial transactions. TANs provide additional security because they act as a form of two-factor authentication. TANs theft is a known attack targeting mobile banking services.
2. Spam and/or Phishing (A2): in mobile malware, the spam and/or Phishing scams are sent over the Short Message Service (SMS) with a shortened URLs to the phone contact list.
3. Botnet functionality (A3): a mobile bot is a type of malware that runs automatically once installed on a mobile device to gain complete access to the device and its contents as well as providing control to the botnet creator. It starts communicating with and receiving instructions from one or more command and control servers. Mobile botnets take advantage of unpatched exploits to provide hackers with root permissions over the compromised mobile device, enabling hackers to send e-mail or text messages, make phone calls, access contacts and photos, and more.
4. Privilege escalation (A4): the malware is capable of taking over the device by exploiting and preserving the device administrator privileges. Once the mobile device has been taken over by the cybercriminals, typically, the malware is capable of doing the following actions: locking users out of their device, taking a photo from the device's camera, answering and dropping phone calls, and searching for banking applications on the device.
5. Geographic location attack (A5): the malware targets a specific user based on the geographical location and country.
6. Functionality exploitation (A6): this type of attack exploits the smartphones' functionality, as follows: (a) download/install malicous software, (b) check and uninstall AVs, (c) modify contents (SD card), (d) use the video camera, (e) infect a connected Windows PC, (f) inject malicious code, (g) make silent calls in background

To further analyze the malware attacks and their characteristics, we looked deeper into the six categories (A1 to A6) of attack types for each malware category according to our taxonomy. Table 12 shows the summary of the attack types based on the malware category and family along with the total percentage for each type of attack. According to the result, information theft exhibits the highest percentage out of other categories (botnet functionality, spam/phishing, privilege escalation, geographic location, and functionality exploitation). About 66% of the malware family steal and harvest the information from the victim where most of them are from banking malware and scareware category. This is followed by the geographic location attack with 56% in total. It is interesting to note that Android banking malware tends to be focused on specific geographical areas. For instance, 80% of the banking malware families (8 out of 10 families) are targeting a specific country such as Brazil, Korea, Iran, Spain, German, Russia, and others. Overall, we noticed that ransomware targets more than 10 countries worldwide if compared to other categories. Adware on the other hand is more universal and targeted all users worldwide (Table 13). In addition, we also looked into the profit target behind malware infection. We categorized the types of financial charges caused by malware in our dataset into the following profitable categories:

1. SMS charge: users are billed directly based on the fraud scheme service.i.e premium-rate sms service. The amount charged varies according to the target country as different country has a different type of premium-rate service.
2. Money transfer or steal: users are tricked to pay for the ransom with different payment options such as money pack (7eleven, Walmart, Kmart, CVS pharmacy, RiteAid pharmacy) VISA wallet or credit card. This category also includes the direct money stealing of online banking or fraud banking.
3. Product payment: users paid for fake products or services such as fake job offer service and fake anti-virus. The payment is done through several options such as credit cards, carrier billing, PayPal, and Google Play credit. Some of the malware provides a manual option through the bank deposit.

Additionally, we also checked both the charge amount and the payment options offered by the malware (Table 14). We found that the amount charged varies according to its target country .e.g., from 2 USD to 5000 USD. There are five different currencies that been used by malware such as United States Dollar(USD), Euro, Russian Ruble, Indian Rupee, and Malaysian Ringgit. The payment options are also ranging from credit card, PayPal, Google Play credit, MoneyPak, QIWI VISA to Bank Deposit.

Table 12 Android financial malware attack types

Family	Category	Malware Attack Types												Total Attack (%)
		Al	A2	A3	A4	A5	A6(a)	A6(b)	A6(c)	A6(d)	A6(e)	A6(f)	A6(g)	
Kemoge	Adware						√							8
Mobidash	Adware			√									√	17
Selfmite	Adware	√	√	√			√							33
Shuanet	Adware				√							√		17
Bankbot	Banking	√		√										17
Binv	Banking	√	√	√		√	√							42
Citmo	Banking	√				√								17
FakeBank	Banking	√				√	√				√			33
Sandroid	Banking		√	√		√								25
SMSspy	Banking		√			√								17
Spitmo	Banking	√					√							17
Wroba	Banking	√	√	√		√								33
ZertSecurity	Banking	√				√								17
Zitmo	Banking	√	√	√		√	√							42
FakeDefender	Ransomware			√			√	√	√					33
Koler	Ransomware	√	√			√								25
Pletor	Ransomware			√		√			√	√				33
ScarePakage	Ransomware					√								8
Simplocker	Ransomware	√		√		√	√							33
Svpeng	Ransomware	√		√										17
AVpass	Scareware	√		√	√	√	√	√						50
FakeAV	Scareware	√			√	√		√						33
FakeFlash	Scareware	√	√		√		√					√		42
FakeJobOffer	Scareware	√				√								17
Fake Player	Scareware		√			√	√	√						33

(*Continued*)

Table 12 Continued

Family	Category	Malware Attack Types												Total Attack (%)
		Al	A2	A3	A4	A5	A6(a)	A6(b)	A6(c)	A6(d)	A6(e)	A6(f)	A6(g)	
Penetho	Scareware	√		√	√									25
Gazon	SMS Malware	√		√			√							25
GGTracker	SMS Malware		√			√								17
Plankton	SMS Malware	√	√	√			√							33
Uxipp	SMS Malware	√	√											17
YZHCsms	SMS Malware	√	√			√								25
Total number of family		21	13	15	5	18	13	4	2	1	1	2	1	

Legend:
A1: Steal and harvest information (contacts, text message, bookmark, credit card credentials)
A2: Send spam SMS/phishing/shortened URLs to the contact list
A3: Communicate with botnet
A4: Exploit root (privilege escalation)
A5: Geographic location attack
A6(a): Download/install malicious software A6(b): Check and uninstall Antiviruses
A6(c): Modify contents (SD card)
A6(d): Use the video camera A6(e): Infect a connected window pc
A6(f): Inject malicious code A6(g): Make silent calls in background

Table 13 Malware attacks by geographical location

Category	Family	Target Country
Banking Malware	Binv	Brazil
	Sandroid	MiddleEast
	Wroba	Korea
	FakeBank	Iran
	SMSspy	Spain
	ZertSecurity	German
	Citmo	Russia
	Zitmo	Europe
SMS Malware	YZHCsms	Asian countries
	FakePlayer	Russia, USA, China
Scareware	FakeJobOffer	India
	FakeAV	USA
Ransomware	Koler	Worldwide (30 countries)
	Pletor	Worldwide (13 countries)
	ScarePakage	USA, UK, Germany
	SimpleLocker	Ukraine, USA

Table 14 Example of financial charge

Category	Malware Family	Charge Amount	Payment Option
Money Transfer (Ransom payment)	FakeDefender	99.98 USD	Credit card
	Koler	100–300 USD	• MoneyPak • Prepaid cards
	Pletor	• 15 Euros • 100 rubles • 5000 USD	• QIWI VISA • MoneXy
	ScarePakage	300 USD	MoneyPak
	SimpleLocker	20–200 USD	MoneXy
Product Payment	FakeJobOffer	8150 Rs	Bank Deposit
SMS Charge	YZHCsms	• 3 MYR • 2 USD(per text)	Phone Bill

6.4 Stage 4: Correlation

In particular, we compared and correlated the analysis result of all malware category in order to rank the importance of each category in our dataset. Overall, banking malware ranked first in terms of the total number of malware attacks for all categories, scoring about 80% (8 families out of 10) on both geographical location attacks, and information theft. This is followed by the scareware where AVpass family performed the highest number of total attacks reaching about 50% (information theft, botnet functionality, root exploit, geographic location attack, malicious download, and AV exploit).

7 Challenges

The study of Android financial malware is dynamic and stimulating. As this is the first study of its type to systematically categorize Android financial malware based on the taxonomy, researchers not only have a new opportunity for research but also a number of challenges. Below are some important challenges in relation to the baseline of Android financial malware field:

1. **Lack of dataset**: The top challenge is a lack of sufficient data. Lack of data is the common problem for all researchers in academia and the study of Android financial malware is no exception. Data is the key for any successful modeling and detection system. In order to ensure that the detection algorithm is reliable, building the malware detection model requires two types of dataset: the training and testing dataset. There exist several public datasets [15, 16, 17] but they are not related to Android financial malware. To tackle this issue, we collect the malware samples from various resources and manually check if the collected samples are financial related malware according to the proposed taxonomy. In addition, the naming convention of malware labelling (i.e. family name) is inconsistent among both academic and industry fields. The inconsistent labelling between different anti-virus vendors and researchers leads to confusion and is time-consuming for reorganization. Researchers have to compare the malware labelling from several anti-virus vendors and follow the majority numbers of the most frequent label of the specific malware family. This technique is completely manual and can lead to errors, hence affecting the accuracy of malware labelling. Therefore, to foster the research in this area, academia and industrial researchers working on Android financial malware field should share the dataset with the research community.
2. **Lack of systematic approach for malware assessment:** There exist a number of metrics developed for malware threat assessment such as vulnerability rating, risk assessment, and incident and impact metrics. But, there is no standard metrics for assessing the malware behavior and evaluating its complexity. Researchers need these metrics to overcome the weaknesses of the current detection system; as the capability of malware is dynamic and becoming more sophisticated, having a standard metrics can help researchers to catch up with the malware trends automatically by defining a formula (i.e. malware complexity scoring formula) which can facilitate researchers for further analysis. In 2016, Maasberg et al. [40] also highlighted this issue giving a set of measures

to quantify malware threats systematically using weights and ratings by focusing on four elements of malware: propagation, characteristics, attribution, impact, and associated dimensions. Although the proposed solution is not fully automated and limited to the zero-day malware (unknown and unidentified malware), it provides a valuable insight into potential capabilities of measuring malware. Significantly, understanding to what degree of sophistication (weight, rating, score) the Android financial malware exhibits can help researchers to provide an accurate and cost-effective mitigation option and strategy.

3. **Hybrid of malware:** The diversity of mobile platforms force malware writers to boost their chances of infection by targeting several attack vectors. The recent samples show that the majority of malware is now hybrid with the banking malware category. For instance, the modern mobile banking malware is not only capable of stealing the banking information, but can also capture SMS messages, record videos of the victim's screen and upload the videos, and even lock the mobile devices and encrypt documents. Moreover, adware and scareware can also be used to compliment banking malware to gain information associated with financial transactions [27]. In that case, it is not easy to classify the malware into a specific category according to the proposed taxonomy. Researchers have to do malware triage and analysis in order to measure the most dominant category between the mix of malware categories. Importantly, the presence of metrics can help to prioritize the most dominant category in an automated way. An accurate dominant malware category acts as an aid to more accurate detection and can help to facilitate the strategy for the mitigation system.
4. **Use of obfuscation:** Today, the use of obfuscation is prevalent in mobile malware. Obfuscation aims to disguise the malware code to make reverse engineering more challenging. An obfuscation refers to the code masking strategy of changing the content of the application (Dalvik Executable .dex files and/or AndroidManifest .xml files) but preserving its original functionality. The obfuscation techniques employed by Android malware typically fall into one of the following categories: loading native libraries, hiding exploits in package assets, using encryption, truncating URLs, injecting malicious bytecode, manipulating the DEX file format to hide methods, and customizing the output of encryption to hide an APK. As such, obfuscation affects the accuracy of malware detection approaches significantly, which also slows down the discovery and detection by security products. Researchers have to consider an effective way to

evaluate the resilience of malware detection technique with regard to the obfuscation behavior in order to combat this issue.

5. **Lack of collaboration with the third-party organizations:** In contrast to non-financially related malware, the financial malware require an interaction with both the victims and the third-party organizations (i.e. financial institutions, SMS centre). For instance, in order to successfully launch their attacks, the banking malware need to monitor the communication between the banking system and the victim. Even after successfully infecting the victim's phone, the cybercriminals still have to collect the victim's banking information (i.e. TAN information) in order to be able to intercept any transactions with the banks. Due to the TAN expiry duration, this theft happens in real time according to the victim's transaction request. As such, in order to combat the financial malware, researchers have to understand how the mobile banking attacks are launched and how the malware is communicated with the bank in real time. This method is significant for the malware response and mitigation strategy. However, due to some policy and privacy issues, a collaboration with this third-party is difficult to establish. As researchers do not have sufficient information and access to the banking systems, the research scope on malware incident response and mitigation strategy is limited. This situation leads researchers to focus more on the analysis and detection part instead of the incident response and mitigation part.
6. **Exploitation of human emotion:** One of the major differences between malware and financial malware is the exploitation of human emotion. Most of the financial malware in accordance with our taxonomy is associated to a psychological game. Psychology plays an important role in almost all aspects of financial malware particularly in ransomware and scareware; from the moment an attack is launched, threat the victims, to the moment the victims pays, or refuses to pay. The malware authors use psychological tactics designed to create a sense of urgency and to exploit human emotions especially anxiety, panic and fear by assigning a warning and deadline. Koler ransomware, for example, presents fake FBI warnings accusing users of viewing of pornography and demands a ransom payment within 48 hours threatening that the recovery keys would be unavailable after that. As a result, if victims got infected with this type of malware, they are willing to pay because they afraid that their activities would be put under a microscope and their reputation would be ruined. In order to increase the capability of malware detection and mitigation, this attribute of human emotion should be taken into account

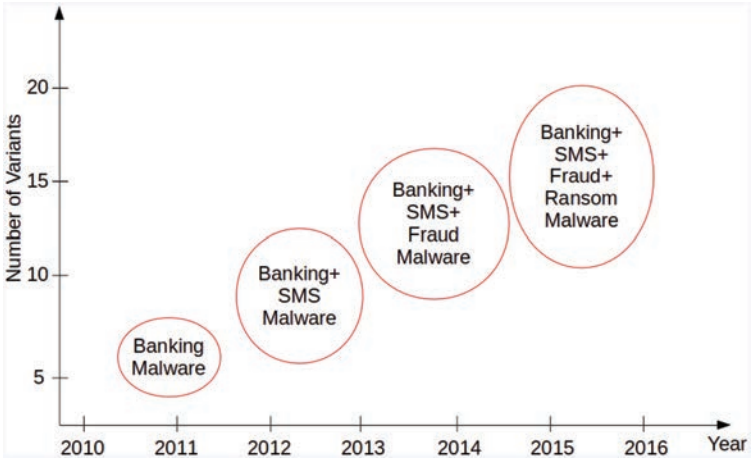

Figure 12 Evolution of Android financial malware (data is based on our dataset).

when developing techniques for Android financial malware detection. In that case, the study of the malware behavior towards human emotion can be conducted in order to measure the malware metrics in accordance with human behavior. This is important to improve understanding and instil awareness of cybersecurity, which can save many people from becoming cyber victims.

7. **Speed of malware evolution:** Android financial malware is evolving quite rapidly. But, the research pace is not accelerating (as much as malware); researchers are still working on developing an intelligent system and methods in order to tackle this issue. Within a short period of time (i.e. 5 years) the evolution shows that the advanced malware capabilities are increasing in accordance with the number of unique variants, as shown in Figure 12.

Researchers can track the speed of evolution with the following four stages:

(a) 1st stage(2010): the introduction period of Android banking malware. The evolution started primarily with the release of the traditional desktop banking malware in the mobile versions. e.g., Zitmo, Spitmo, Citmo.

(b) 2nd stage (2013): these malware families feature simplistic modifications, recompiled the source code with improved infection and distribution strategies, e.g., ZertSecurity, SMSspy, Fake-Bank.

(c) 3rd stage (2014): during this year we saw malware emerging with innovative techniques based on new infection strategies and payloads, e.g., Wroba, Sandroid, Binv.
(d) 4th stage (2015 - onwards): this is the most advanced stage that covers the recently discovered malware such as Bankbot and Svpeng. It is capable of employing advanced techniques for infection and distribution, which are combined with the ransomware technique.

8 Summary

There are many articles, reports, books on the technical of Android malware, but in-depth explorations of Android financial malware are limited. There is a lack of understanding of the financial malware and its behavior. Without knowing what constitutes mobile financial malware, the detection systems are not capable of providing an accurate detection. For this reason, in this work, we defined the Android financial malware and investigated their behavior by exposing all possible schemes that have been used by the cybercriminals to make money off of their victims according to our proposed taxonomy i.e., adware, banking malware, ransomware, scareware, and SMS malware.

By profiling the behavior of Android malware according to the proposed taxonomy, the malware analysis can be done effectively with more emphasis on the financial factors; as the trend of the mobile malware today are focusing more on financial rather than ego motives. Likewise, researchers can gain a deep understanding of each malware category. The understanding of complex characteristics and the unknown behavior of financial malware can be achieved efficiently by classifying the malware into specific groups of financial malware such as banking malware or ransomware.

As this is the first study of its type to systematically categorize Android financial malware based on taxonomy, researchers not only face a number of challenges but also more opportunities for future research. Lack of resources (knowledge, access, dataset) in fact is the common problem for all researchers, but this can also be the motivation for the new research collaboration between the academia and industry. Perhaps, university and financial institutions can work together in building the bridge to connect knowledge and create new knowledge for better schemes of malware detection, response, and mitigation strategy. With the malware sophistication and evolution towards human emotion, researchers can increase the research pace and dig more on the financial malware unique behavior. A standard malware behavioral metrics is needed to overcome the weaknesses of the current detection system.

Through our analysis and experimentation, we identified two necessary factors for the solution to be viable that should be taken into account when developing techniques for Android financial malware detection:

1. **Accurate and precise detection.** There are five categories of Android financial malware according to the proposed taxonomy profile: adware, banking malware, ransomware, scareware, and SMS malware. Due to the hybrid behavior of malware, it is important to define a threshold of each malware category for the malwaremetric. The following are some potential scenarios that should be considered by the researchers in classifying these five categories accurately and precisely:
   - *What if the unknown sample has the same malware behavioral metrics (i.e. malware percentage score)? To which category will it be assigned?*
   - *What if the unknown sample has a high malware behavioral score but is considered as benign according to other malware detection systems such as Virus-Total?*

   Hence, we have to choose the best algorithm and measurement method to evaluate the proposed framework. The focus is not only on the high accuracy with concrete prediction but also the high precision with a probability estimation. Focusing on assessing both the accuracy and precision of the detection system is significantly important for improving the malware profiling.
2. **Thorough evaluation.** Before we can detect the Android financial malware accurately based on the proposed taxonomy, we need to be able to distinguish the uniqueness of such financial malware categories. The malware behavioral metric (i.e. malware scoring formula) plays a key role in handling this issue. The malware scoring formula will be used to set the baseline for how each financial malware category should be evaluated and assessed in order to facilitate the malware detection.

In future work, we plan to design and develop a framework for Android financial malware detection that is capable of analyzing and profiling the Android applications in a comprehensive manner. Introducing and developing a proper measurement to evaluate the complexity of malware would be beneficial for both the research community and malware analyst. The metrics can facilitate malware analysis by scaling any incoming malware samples according to the priority queue. For instance, the samples at the top of the queue would be considered the most concerning and given highest priority for

full analysis. This prioritization offers a guideline for the malware analysts in dealing with huge dataset. Also, it provides an order which facilitates the decision in deciding which malware samples to analyze first.

Acknowledgment

The authors gratefully acknowledge the funding from Ministry of Education Malaysia (MOE) and International Islamic University Malaysia (IIUM).

References

[1] The rise of android drive-by downloads. Available at: http://0x4d31.blogspot.ca/2012/05/rise-of-android-drive-by-downloads.html accessed April 1, 2018.
[2] Virus total. Available at: https://www.virustotal.com/en/ accessed August 1, 2017.
[3] The first mobile encryptor trojan. Available at: https://securelist.com/blog/mobile/63767/the-first-mobile-encryptor-trojan/ accessed Jan, 2017.
[4] Mobile crypto-ransomware simplocker now on steroids. Available at: https://blog.avast.com/2015/02/10/mobile-crypto-ransomware-simplocker-now-on-steroids/ accessed Jan, 2017.
[5] Mobile ransomware: Status quo. Available at: https://blog.fortinet.com/2014/06/25/mobile-ransomware-status-quo accessed Jan, 2017.
[6] The rising tide of android malware. Available at: http://www.sonicwall.com/whitepaper/2017-sonicwall-annual-threat-report8121810/ accessed Jan, 2017.
[7] Scarepakage android ransomware pretends to be fbi porn warning. Available at: https://www.theguardian.com/technology/2014/jul/17/scarepakage-android-ransomware-porn-fbi accessed Jan, 2017.
[8] Sms trojan yzhcsms found in android market and third party stores. Available at: http://forums.juniper.net/t5/Security-Now/SMS-Trojan-YZHCSMS-Found-in-Android-Market-and-Third-Party/ba-p/132963 accessed Jan,2017.
[9] Security threat trends 2015. Available at: https://www.sophos.com/en-us/threat-center/medialibrary/PDFs/other/sophos-trends-and-predictions-2015.pdf accessed July 11, 2015.
[10] Current android malware. Available at: https://forensics.spreitzenbarth.de/android-malware/ accessed July 11, 2017.

[11] IT threat evolution in q3 2014. Available at: https://securelist.com accessed July 13, 2015.
[12] Financial threats review 2017. Available at: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf accessed July, 2017.
[13] Avg antivirus available for free on google play. Available at: https://urbangeekz.com/2017/05/avg-antivirus-available-for-free-on-google-play/, accessed July 31, 2017.
[14] Androbugs.com. Available at: http://www.androbugs.com/ accessed September 7, 2017.
[15] Android malware. Available at: http://amd.arguslab.org/sharing accessed September 7, 2017.
[16] Android malware dataset. Available at: https://github.com/ashishb/android-malware, accessed September 7, 2017.
[17] Malware sample sources for researchers. Available at: https://zeltser.com/malware-sample-sources/, accessed September 7, 2017.
[18] Almeida, G. M. D. (2012). M-Payments in Brazil: Notes on How a Country's Background May Determine Timing and Design of a Regulatory Model. *Wash. JL Tech. & Arts*, *8*, 347.
[19] Alzahrani, A. J., Stakhanova, N., Ali, H. G., and Ghorbani, A. (2014). Characterizing Evaluation Practicesof Intrusion Detection Methodsfor Smartphones. *Journal of Cyber Security and Mobility*, 3(2), (pp. 89–132).
[20] Andronio, N., Zanero, S., and Maggi, F. (2015). Heldroid: Dissecting and detecting mobile ransomware. In *International Workshop on Recent Advances in Intrusion Detection* 382–404 Springer, Cham.
[21] Beresford, A. R., Rice, A., Skehin, N., and Sohan, R. (2011). Mockdroid: trading privacy for application functionality on smartphones. In *Proceedings of the 12th workshop on mobile computing systems and applications* (pp. 49–54).
[22] Bose, A., Hu, X., Shin, K. G., and Park, T. (2008). Behavioral detection of malware on mobile handsets. In *Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services* (pp. 2259–238).
[23] Chen, T. M., and Peikari, C. (2008). Malicious software in mobile devices. In *Handbook of Research on Wireless Security*, 1:1–10, 2008.
[24] Choi, B., Choi, S. K., and Cho, K. (2013). Detection of mobile botnet using VPN. In *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on* (pp. 142–148). IEEE.

[25] Hesham Darwish and Mohammad Husain. Security analysis of mobile money applications on android. Available at: http://www.cpp.edu/ accessed April, 2017.
[26] Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B. G., Cox, L. P., and Sheth, A. N. (2014). Taint-droid: an information-flow tracking system for realtime privacy monitoring on smartphones. *ACM Transactions on Computer Systems (TOCS)*, 32(2):5.
[27] Erturk, E. (2015). Two trends in mobile security: Financial motives and transitioning from static to dynamic analysis. CoRR, abs/1504.06893.
[28] Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M., and Rajarajan, M. (2015). Android security: a survey of issues, malware penetration, and defenses. *IEEE communications surveys & tutorials*, 17(2), 998–1022.
[29] Garner, P., Mullins, I., Edwards, R., and Coulton, P. (2006). Mobile Terminated SMS Billing—Exploits and Security Analysis. In *Third International Conference on Information Technology: New Generations (ITNG'06)*, (pp. 294–299).
[30] Gharib, A., and Ghorbani, A. (2017). Dna-droid: A real-time android ransomware detection framework. In *International Conference on Network and System Security* (pp. 184–198). Springer, Cham.
[31] Gonzalez, H., Stakhanova, N., and Ghorbani, A. A. (2014). Droidkin: Lightweight detection of android apps similarity. In *International Conference on Security and Privacy in Communication Systems* (pp. 436–453). Springer, Cham.
[32] Harris, A., Goodman, S., and Traynor, P. (2012). Privacy and security concerns associated with mobile money applications in Africa. Wash. *JL Tech. & Arts*, 8, 245.
[33] Hoffman, D. V. (2007). *Blackjacking: security threats to Blackberry devices, PDAs, and cell phones in the enterprise*. John Wiley & Sons.
[34] Hua, J., and Sakurai, K. (2011). A sms-based mobile botnet using flooding algorithm. In Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication, pp. 264–279. Springer, 2011.
[35] IBM. Financial malware explained. Available at: http://cdn.americanbanker.com/pdfs/WGW03086USEN.PDF 2014.
[36] Ibrahim, L. M., and Thanon, K. H. (2015). Analysis and detection of the zeus botnet crimeware. *International Journal of Computer Science and Information Security*, 13(9), 121.

[37] Jin-Hyuk Jung, Ju Young Kim, Hyeong-Chan Lee, and Jeong Hyun Yi (2013).Repackaging attack on android banking applications and its countermeasures. Wireless Personal Communications, (pp. 1421–1437).

[38] Kadir, A. F. A., Stakhanova, N., and Ghorbani, A. A. (2016). An Empirical Analysis of Android Banking Malware. *Protecting Mobile Networks and Devices: Challenges and Solutions*, 209.

[39] Leavitt, N. (2005). Mobile phones: the next frontier for hackers?. *Computer*, 38(4), 20–23.

[40] Maasberg, M., Ko, M., and Beebe, N. L. (2016). Exploring a systematic approach to malware threat assessment. In *System Sciences (HICSS), 2016 49th Hawaii International Conference on* (pp. 5517–5526).

[41] Mercaldo, F., Nardone, V., Santone, A., and Visaggio, C. A. (2016). Ransomware steals your phone. formal methods rescue it. In *International Conference on Formal Techniques for Distributed Objects, Components, and Systems* (pp. 212–221). Springer, Cham.

[42] Mila. Contagio mobile: Mobile malware mini dump. Available at: http://contagiominidump.blogspot.ca/ accessed July 11, 2015.

[43] Mulliner, C., and Seifert, J. P. (2010). Rise of the iBots: Owning a telco network. In *Malicious and Unwanted Software (MALWARE), 2010 5th international conference on* (pp. 71–80).

[44] Mylonas, A., Dritsas, S., Tsoumas, B., and Gritzalis, D. (2011). On the feasibility of malware attacks in smartphone platforms. In *International Conference on E-Business and Telecommunications* (pp. 217–232). Springer, Berlin, Heidelberg.

[45] Nauman, M., and Khan, S. (2011). Design and implementation of a fine-grained resource usage model for the android platform. *Int. Arab J. Inf. Technol.*, 8(4), 440–448.

[46] Reaves, B., Scaife, N., Bates, A. M., Traynor, P., and Butler, K. R. (2015). Mo (bile) Money, Mo (bile) Problems: Analysis of Branchless Banking Applications in the Developing World. In *USENIX Security Symposium* (pp. 17–32).

[47] Marco Riccardi, David Oro, Jesus Luna, Marco Cremonini, and Marc Vilanova. (2010). A framework for financial botnet analysis. In eCrime Researchers Summit (eCrime), pp. 1–7.

[48] Schreckling, D., Posegga, J., and Hausknecht, D. (2012). Constroid: data-centric access control for android. In *Proceedings of the 27th Annual ACM Symposium on Applied Computing* (pp. 1478–1485).

[49] Song, S., Kim, B., and Lee, S. (2016). The effective ransomware prevention technique using process monitoring on android platform. *Mobile Information Systems*, 2016.

[50] Tajalizadehkhoob, S. T., Asghari, H., Gañán, C., and Van Eeten, M. J. G. (2014). Why them? Extracting intelligence about target selection from Zeus financial malware. In *Proceedings of the 13th Annual Workshop on the Economics of Information Security, WEIS 2014, State College (USA), June 23–24, 2014*. WEIS.

[51] Darell JJ Tan, Tong-Wei Chua, Vrizlynn LL Thing, et al. Securing android: a survey, taxonomy, and challenges. ACM Computing Surveys (CSUR), 47(4):58, 2015.

[52] Vural, I., and Venter, H. (2010). Mobile botnet detection using network forensics. In *Future Internet-FIS 2010*, (pp. 57–67). Springer, 2010.

[53] Yang, T., Yang, Y., Qian, K., Lo, D. C. T., Qian, Y., and Tao, L. (2015) Automated detection and analysis for android ransomware. In *2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS)*, (pp. 1338–1343).

[54] Zeng, Y., Shin, K. G., and Hu, X. (2012, April). Design of SMS commanded-and-controlled and P2P-structured mobile botnets. In *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks* (pp. 137–148). ACM.

[55] Yuan Zhang, Min Yang, Bingquan Xu, Zhemin Yang, Guofei Gu, Peng Ning, X Sean Wang, and Binyu Zang (2013). Vetting undesirable behaviors in android apps with permission use analysis. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, (pp. 611–622).

[56] Zhauniarovich, Y., Gadyatskaya, O., Crispo, B., La Spina, F., and Moser, E. (2014). Fsquadra: fast detection of repackaged applications. In *IFIP Annual Conference on Data and Applications Security and Privacy*, (pp. 130–145). Springer, 2014.

[57] Zhou, Y., and Jiang, X. (2012). Dissecting android malware: Characterization and evolution. In *Security and Privacy (SP), 2012 IEEE Symposium on* (pp. 95–109).

Biographies

Andi Fitriah Abdul Kadir is a Ph.D. student and a member of the Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick, Fredericton, Canada. She completed her Master's degree in Computer Science (Network Security) in 2013 at International Islamic University Malaysia (IIUM). Andi Fitriah was the recipient of the IIUM Academic Excellence Award and currently attached with IIUM as an academic trainee. She received several awards from International academic conferences including the Best Poster, Gold Medal, and Best Paper Honorable Mention awards. She works closely with industry focusing on the R&D projects. Her current research focus is computer forensics, network security, malware analysis, and machine learning.

Natalia Stakhanova is an Assistant Professor and the New Brunswick Innovation Research Chair in Cyber Security at the University of New Brunswick, Canada. Her work revolves around building secure systems and includes mobile security, IoT security, software obfuscation & reverse engineering, and malicious software. Working closely with industry on a variety of R&D projects, she developed a number of technologies that resulted

in 3 patents in the field of computer security. Natalia Stakhanova is the recipient of the UNB Merit Award, the McCain Young Scholar Award and the Anita Borg Institute Faculty Award.

Ali A. Ghorbani is currently serves as Director of the Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick, Fredericton, Canada. Dr. Ghorbani is the co-Editor-In- Chief of Computational Intelligence, an international journal. He supervised more than 150 research associates, postdoctoral fellows, and undergraduate & graduate students and authored more than 250 research papers in journals and conference proceedings and has edited 11 volumes. He is the co-inventor of 3 patents in the area of Network Security. His current research focus is cybersecurity, complex adaptive systems, critical infrastructure protection, and web intelligence.