EC2: Ensemble Clustering and Classification for Predicting Android Malware Families

Tanmoy Chakraborty, Fabio Pierazzi and V.S. Subrahmanian

Abstract—As the most widely used mobile platform, Android is also the biggest target for mobile malware. Given the increasing number of Android malware variants, detecting malware families is crucial so that security analysts can identify situations where signatures of a known malware family can be adapted as opposed to manually inspecting behavior of all samples. We present EC2 (Ensemble Clustering and Classification), a novel algorithm for discovering Android malware families of varying sizes – ranging from very large to very small families (even if previously unseen). We present a performance comparison of several traditional classification and clustering algorithms for Android malware family identification on DREBIN, the largest public Android malware dataset with labeled families. We use the output of both supervised classifiers and unsupervised clustering to design EC2. Experimental results on both the DREBIN and the more recent Koodous malware datasets show that EC2 accurately detects both small and large families, outperforming several comparative baselines. Furthermore, we show how to automatically characterize and explain unique behaviors of specific malware families, such as FakeInstaller, MobileTx, Geinimi. In short, EC2 presents an early warning system for emerging new malware families, as well as a robust predictor of the family (when it is not new) to which a new malware sample belongs, and the design of novel strategies for data-driven understanding of malware behaviors.

Index Terms—Android, malware, ensemble, classification, clustering.

1 INTRODUCTION

With over 1.4 billion active phones worldwide [1] and over 290,000 phones sold in Q1 2016 alone with an 84.1% market share [2], Android dominates the mobile market. But this success has a dark side - more than 97% of mobile malware target Android devices [3] in order to steal money or private data. Examples include illegally sending SMSs to premium-rate numbers, stealing calendars, emails, texts, contact lists, social network accounts, documents and banking credentials. To elude detection, malicious developers use obfuscation techniques (e.g., polymorphism and metamorphism) [19] to automatically generate multiple variants of the same malware, thus creating a new family [17] of malware samples having the same purpose but slightly different characteristics (e.g., different file hash, names of functions and variables). In fact, almost 9,000 new Android malware samples were found daily in 2016, an increase of 40% over 2015 [8].

Given the increasing number of new malware samples, manual investigation is impractical and might lead to significant delays in the release of detection signatures for anti-malware tools. The only viable way to manage such huge volumes of malware is to design novel algorithms that can automatically group similar samples into families. This has several major benefits – (i) if a sample belongs to a known family, the same removal techniques can be re-used; (ii) security analysts can focus their manual investigation on the few new samples that do not belong to any known family, thus optimizing their limited time and resources; (iii) understanding the characteristics of each family helps to detect more robust signatures for anti-malware tools.

Most literature on mobile malware analysis [11], [14], [21], [48], [58] is focused on detection (i.e., distinguishing malware from benign software). Several efforts [28], [29], [30], [55], [56], [58], [59] have been proposed in the context of detecting Android malware families. Some of these works consider outdated datasets (e.g., [30], [59]) and/or do not characterize malware families through feature explanation (e.g., [28]), mostly because they use features that are low level and hard to interpret, such as API call sequences. However, the major limitation of all existing works [28], [29], [30], [55], [56], [58], [59] is that they focus only on large families (e.g., size > 10) for which training data is available, and ignore small families which represent the novel malware variants on which security analysts should focus their attention.

We propose EC2, the first algorithm that effectively classifies a malware sample into both large and small families (even if previously unseen). We begin by presenting a thorough performance comparison on the classification of Android malware families by using DREBIN [4], [14], the largest publicly available Android malware dataset with labeled families. Several state-of-the-art classification and clustering algorithms are evaluated for the task of family classification by considering different combinations of static

1. It is important to observe that in some cases the concept of “malware family” may be fuzzy, as a security analyst may consider that a sample belongs to more than one family. For this reason, all results in this paper refer to the publicly available and labeled DREBIN [4] and Koodous [9] datasets.
and dynamic features. We then design EC2 as an ensemble that combines the best of classification and clustering, and evaluate its performance both on DREBIN [4] and on the more recent Koodous academic dataset [9], outperforming several comparative baselines [30], [42], [52], [60].

The paper makes five major contributions.

(i) We thoroughly assess performance of several state-of-the-art supervised classification and unsupervised clustering algorithms for Android malware family identification. The best supervised classifier (Random Forest) has accuracy\(^2\) of 0.93 for large families (size \(\geq 10\)), which decreases to 0.73 for small families (size \(< 10\)) due to lack of training data. In contrast, the best unsupervised clustering method (DBSCAN) achieves accuracy of 0.91 for small families and 0.86 for large families (see Table 5).

(ii) While past research has looked at clustering and classification separately for traditional (mostly PC) malware, EC2 combines the results of both clustering and classification to overcome the drawbacks of each. EC2 delivers significant performance across all malware families (including families with just one sample), achieving an overall accuracy of 0.97, and outperforming several comparative baselines on DREBIN.

(iii) Unlike all related works [28], [29], [30], [55], [56], [58], [59], EC2 is the first algorithm that can classify malware samples into small or even \textit{previously unseen} Android malware families. Given the huge number of malware released in the wild everyday [8], the capability of detecting small and previously unseen malware families is critical for prioritizing manual inspection of new threats. We show how we identify samples belonging to very small malware families - in fact showing 0.43 Precision and 0.31 Recall for detecting families of size just 1.

(iv) We show how to characterize different malware families by extracting family-specific features that distinguish one family from others. We chose to use the DREBIN dataset as each sample is labeled with a ground truth family to which the sample belongs [4]; our analysis reveals that the most important features for malware family classification are: re-using signatures for signing malware variants, requesting network permissions, requesting permissions to read/send SMS messages (used to send texts to premium-rate numbers) and use of encryption (often used for string decryption or repacking of malicious code to avoid static analysis). We also show that some malware families are better identified through static features, while others require dynamic analysis (e.g., because they adopt string decryption at runtime of C2C server URLs and C2C commands to avoid trivial detection via static code analysis). We observe that more recent malware families may show different behaviors trends [55] as obfuscation strategies become more sophisticated and adapt to anti-virus strategies; however, the approach we propose for family characterization is general and can also be applied to more recent malware samples.

(v) To show that EC2 is equally efficient in detecting recently released malware samples, we use Koodous, a dataset (Dec 2015 to May 2016) of recent Android malware samples. Here too, EC2 outperforms other baselines with an overall F-Score of 0.74.

The rest of the paper is organized as follows. Section 2 presents a thorough literature review on malware detection and classification. Section 3 presents the DREBIN dataset. Section 4 describes static and dynamic features for malware samples. Section 5 shows how classification and clustering leads to our new EC2 algorithm. A detailed evaluation of the classification and clustering algorithms are separately presented in Section 6 and Section 8 respectively. Section 7 shows how to use classification to automatically characterize malware families. Finally, Section 9 compares EC2 with several existing baselines, including the best classification and clustering algorithms and shows that EC2 outperforms all. Section 10 presents conclusions and directions for future works.

2 Related work

We identify and discuss three main areas of related work: (i) malware spread and characterization, (ii) malware analysis and detection, (iii) prediction of malware families.

Malware spread and characterization. Some broadly related works predict malware spread [40], [62], evaluate infection rates and risk indicators [57], characterize of malware on different third-party Android markets [45] etc. However, these works do not propose ways to detect/classify malware into families.

Malware analysis and detection. Several efforts [14], [15], [41], [44], [54], [61] focus on malware detection, i.e., given a new sample, predict whether it is benign or malicious. Koller et al. [41] propose an n-gram approach based on the bytes of malware binaries. Baldangombo et al. [15] propose an ensemble classifier relying on static features from Windows malware. Siddiqui et al. [54] compare some supervised classifiers using static features and achieve best performance with decision trees. Ye et al. [61] combine file content and file relations for malware detection. While these works focus on PC malware, malware detection for mobile devices [53] has gained much recent attention. Some works [22], [36], [46], [51] study the effectiveness of existing antivirus solutions against obfuscation techniques applied to malware, whereas our main focus in this paper is related to family prediction algorithms. Some papers [35], [50] proposed distillation and re-training on adversarially crafted samples to increase classifier robustness against obfuscation; but this approach has been later shown to be not effective [23] through a quantitative evaluation. Other works like DREBIN [14], Crowdroid [21], DroidAPIMiner [11] perform malware detection through static features of Android applications, whereas TaintDroid [32] and DroidScope [58] use dynamic features extracted from execution traces. Droid-SIFT [63] performs semantics-aware classification based on control flows. MARVIN [44] proposes a binary classification method to discriminate between benign and malware applications using both static and dynamic features. MaMaDroid [49] builds behavioral models from dynamic logs through HMM to distinguish between benign and malicious applications. Unlike malware detection, our paper focuses on the problem of identifying malware families. Moreover unlike most past work we present a thorough analysis

2. We report accuracy in terms of Macro F-Score (MaF*), formally defined in Section 8.
of several supervised classification and unsupervised clustering methods with different combinations of static and dynamic features.

**Prediction of malware families.** Several efforts ([17], [38], [52], [60]) consider the problem of malware classification, i.e., given a set of malware samples, identify which samples are variants of the same malware family. Ye et al. [60] propose an ensemble based on k-medoids and hierarchical clustering. Bayer et al. [17] propose a scalable method combining hierarchical clustering and locality-sensitive hashing on malware execution traces. Rieck et al. [52] propose a supervised SVM-based approach that clusters dynamic features from execution traces. All these works are focused on traditional PC malware, whereas our focus is on Android [53], an ecosystem that differs from traditional PC malware in terms of application, sandboxing, resource access, and system calls (more details in Section 4.1). Some recent work tackles the problem of Android malware classification. [16] proposes a very preliminary model checking approach to classify malware samples from just 2 families (OpFake, DroidKungFu) with 100 samples each. We consider 156 families including 47 singleton families with about 5000 samples. Dendroid [56] proposes a text-mining based method to find similarities in malware families by extracting code chunks and deriving static features from them. DroidLegacy [30] proposes an approach to detect malicious code modules, but their focus is explicitly on piggybacked and repackaged applications. However, these works [30], [56] have some major shortcomings – they evaluate their approach only on the outdated MalGenome dataset [6], [64] (which is only a small subset of DREBIN, consisting of about 20% of the DREBIN dataset samples), and results obtained with their approach are hard to interpret for a human security analyst, whereas we automatically identify specific characteristics that distinguish malware families and which are easy to interpret. Moreover, past works do not consider small families, which is one of the major strengths of EC2. In [30] the authors remove all families with ≤ 10 samples, while in [56] the authors remove all singletons (i.e., families with just one sample) from the analysis. There are other works related to mobile malware classification. DroidMiner [59] analyzes fine-grained behaviors of Android malware applications. DroidScribe [28] considers only dynamic features and classifies Android malware into families to provide a baseline against proposals that focus on static features. DroidSieve [55] considers only static features – in particular, it proposes a set of features that are resilient to modern obfuscations techniques. Prescience [29] builds on DroidSieve and studies periodic retraining of classifiers over time to adapt to novel obfuscation techniques. However, in this paper we also consider small and previously unseen families which are not the main focus of [28], [29], [55], [59], [63]; in particular, our major contribution is the EC2 algorithm which is very efficient in detecting both very small (including new malware families) and large families. Andronio et al. [12] propose a method for discriminating between goodware, scareware and ransomware by generalizing three key insights of common behaviors in mobile ransomware: threatening text, device locking, and encryption. Aresu et al. [13] propose an approach that by extracting features from HTTP traffic is focused on classification of mobile botnets variants (e.g., Zitmo). However, these works are not generic since they are targeted to specific objectives (identify which malware is scareware/ransomware, and identify variants of mobile botnets samples), whereas we propose a generic approach that can be applied to any malware family and is also able to detect singleton families.

As a final remark, it is important to observe that in some cases the concept of “malware family” may be fuzzy, as a security analyst may consider that a sample belongs to more than one family. For example, consider the Petya ransomware and its more recent variant NotPetya [10], which antivirus vendors eventually decided to consider as two distinct families due to their differences in propagation and operativity. Nevertheless, the detection of small and/or previously unseen families can also be helpful in the detection of very different variants of a known family which may represent an entirely new strain. For the sake of fairness, all results in this paper refer to the publicly available and labeled DREBIN [4] and Koodous [9] academic datasets.

### 3 DREBIN Dataset

We first analyze the DREBIN dataset [4] as it represents the largest public, labeled mobile malware dataset, as of 2016. All DREBIN samples (even ones in the same family) are characterized by different hash values, indicating that some obfuscation technique [19] has been applied in order to prevent easy detection of variants. As described in Section 4.3.1, we execute the malware samples in a controlled environment to extract dynamic features. We only kept dynamic logs for samples executed for 120 seconds without failures. In particular, the final dataset used in this paper consists of 4,845 malware samples: Figure 1(a) reports the distribution of malware family sizes, and Figure 1(b) reports the top 15 malware families by size, among which: FakeInstaller, that simulates an installer of Android applications but in reality sends SMSs to a premium-rate service; DroidKungFu that tries to perform privilege escalation and steals sensitive data from the device; Opfake that is another malware family sending SMSs to premium-rate numbers.

The size of Android malware families follows a heavy-tailed skewed distribution (cf. Figure 1(a)): 112 of 156 families have under 10 samples. This suggests that supervised classification algorithms might not work well due to lack of training samples for small families. Hence, we leverage unsupervised clustering approaches and propose a novel ensemble method that leverages both classification and clustering.

### 4 Feature extraction

We first present some fundamentals about the Android environment, and then describe how we design and extract static and dynamic features from the samples.

#### 4.1 Android Fundamentals

Android applications (or apk files) are jar-like compressed files. Android users can install applications from both official (Google Play Store) and third-party marketplaces. The components of each Android application must be declared in the Manifest file which is a header in each apk. The main apk components are:
Activities model the screens and windows that constitute the user interface of an application.

Services are background processes that remain active even when the application is out-of-focus (e.g., playing music), and may be used for malicious acts (e.g., aggressive advertisement from Adware).

Content Providers are used to define and regulate data sharing between applications.

Broadcast Receivers are used to monitor system-level events (such as \texttt{BOOT_COMPLETED}, commonly monitored by malware to trigger malicious behavior on phone startup [14]).

Intents are messaging objects that can be used for interactions and communication between components. They are used to invoke actions, e.g., start another activity, start a service, or deliver a broadcast message that can be captured by broadcast receivers.

Each Android application runs in an isolated environment that is separated from other applications, and by default it can only write on a separate memory space and cannot access phone resources (e.g., Camera). To perform more advanced interactions, Android relies on a fine-grained permissions system for which an application has to explicitly request the user, at installation time, for permission to access specific software (e.g., access call log) and/or hardware (e.g., camera, vibration) resources. This guarantees transparency about the data that can be accessed by the application (e.g., access and modify Calendar or Contact List), although it is often overlooked by users since the number of permissions may be high. Moreover, it is not trivial to determine what an application actually does with a permission (e.g., when/where an app exactly uses \texttt{READ_SMS} permission to read text messages inbox). A full set of standard permissions is available in Android documentation\(^3\), but program developers can also define a set of custom permissions depending on their needs (e.g., to communicate with other applications of the same developer).

### 4.2 Static Features

Several static features have been proposed in the literature (e.g., [14], [44], [55], [63]). We wanted to develop easy to extract and explainable static features by leveraging those proposed in [14]. Despite [14] extracts static features both from the Manifest and from the source code (e.g., API calls), we decided to consider only features from the Android Manifest\(^4\) for three main reasons: (i) features from the code may introduce overly detailed and noisy information [31], [36], whereas the Android Manifest already has rich information about an application and its structure; (ii) the use of encryption or reflection [46] may easily introduce much noise in the code, whereas the Android Manifest must be declared in plaintext and also contains many specifications about requested permissions and interfaces; (iii) finally, we consider features that are easy to interpret, so that we can automatically extract meaningful characteristics that distinguish malware families (cf. Section 7 and supplementary materials).

Depending on their meaning, our static features fall into three main groups: \texttt{author}, \texttt{structure} and \texttt{permissions}. Table 1 reports the complete list of static features, where the leftmost column reports feature groups.

**Author**. Malware of the same family may be developed by the same author. Developer information is usually published by marketplaces (e.g., Google Play). However, the DREBIN dataset also contains applications that have been removed from the store or that have been retrieved from third-party marketplaces. We assume that if two applications are digitally signed with the same certificate, then they have been developed by the same author. This feature has not been considered by [14], but in some other related research (e.g., [55]). Section 7 shows that some families (e.g.,

**Structure**

4. Our static feature set corresponds to the features proposed in [14] related to the Android Manifest with some modifications: unlike [14], we also consider the \texttt{filesize} and \texttt{author} of an app (which have also been considered in [55]); unlike [14], we only consider the \texttt{number} of application components (e.g., Activities, Services), instead of their specific class names (e.g., \texttt{HomepageActivity.class})—this is because names can be very easily obfuscated, whereas number of components may not be modified arbitrarily by the malware developer without raising suspiscionousness in malware detectors. We also observe that all static features in [14] are binary, whereas we also have continuous static features: \texttt{author}, \texttt{filesize}, number of components, and number of permissions.

<p>| Table 1: Static features derived from the analysis of code and Manifest in the malware samples in DREBIN. |</p>
<table>
<thead>
<tr>
<th>Group</th>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author</td>
<td>author</td>
<td>Derived from SHA256 hash that digitally signs the Android sample</td>
</tr>
<tr>
<td>Structure</td>
<td>filesize</td>
<td>The size of the file in bytes</td>
</tr>
<tr>
<td></td>
<td>n_activities</td>
<td>Num. Activities</td>
</tr>
<tr>
<td></td>
<td>n_intents</td>
<td>Num. Filtered Intents</td>
</tr>
<tr>
<td></td>
<td>n_providers</td>
<td>Num. Content Providers</td>
</tr>
<tr>
<td></td>
<td>n_providers</td>
<td>Num. Services</td>
</tr>
<tr>
<td></td>
<td>n_receivers</td>
<td>Num. Broadcast Receivers</td>
</tr>
</tbody>
</table>

\(^3\) https://developer.android.com/guide/topics/security/permissions.html
MobileTx and Opfake) have many samples developed by the same author — while the author feature is insignificant for others (e.g., Geinimi, FakeInstaller, JiFake) as the malware developers were more careful.

**Application components.** Applications sharing similar structure may be variants of the same family. We describe app structure via the number of components found in the Manifest: filesize, n_activities, n_intents, n_providers, n_receivers, n_services. As an example, the feature n_activities is very significant to discriminate the family Opfake (cf. supplementary materials), and also for discriminating the various families in the multiclass classification task (cf. Figure 8). Unlike the feature set presented in [14], we choose not to consider the names of the Android components, but rather their counts because component names can be altered very easily (as they are just the names of Java classes defined by the application developer). On the other hand, the number and organization of components is harder to change significantly without also improving chances of detection of a sample as malware.

**Permissions.** The Android permissions system provides a rich source of features as malware from the same family may need the same permissions that may help distinguish them from other families. For example, MobileTx is one of the few families requiring the RESTART_PACKAGES permission, that is used to kill antivirus and application monitoring systems. Sometimes, even the absence of a certain permission requested by the malware can be useful to discriminate its family. For instance, FakeInstaller does not need the ACCESS_NETWORK_STATE permission — this absence is a strong indicator that a sample belongs to this family. A predefined set of standard permissions label some features dangerous as they provide access to sensitive resources such as call logs or contact lists. Our feature set includes binary vectors as in [14], containing possible standard software and hardware permissions from the Android official documentation. We also count the number of customized permissions that can be defined by programmers. As a final remark, although permission-related features are very important, they may not be sufficient by themselves for detecting/classifying some types of Android malware (e.g., in case of privilege escalation attacks [20]); hence it is fundamental to consider the other kinds of features presented in this section as well.

We extract static features with official Android SDK tools and Androguard, a Python library for extracting metadata from apk files and their Manifest. We have 190 static features in all (Author: 1, Application components: 6, Permissions: 183).

### 4.3 Dynamic Features

Since static features alone may not be enough because of obfuscation techniques [19], we run malware samples in a sandbox in order to find common behaviors exhibited by families [52]. We first describe generation of dynamic logs, then design and motivate extraction of dynamic features.

#### 4.3.1 Generation of Malware Dynamic Logs

We installed and configured the official Android emulator, a fully-functional Android system that runs applications with a graphical user interface. We also used inetsim, a tool that simulates many network services, and also provides realistic data in response to malware requests (e.g., if a malware tries to download an executable file from an external website). This allows us to log the most relevant malware Internet requests of the malware, despite absence of real Internet connectivity. To run the malware samples, we use DroidBox 4.1.10, an open-source sandbox especially tailored for dynamic malware analysis of Android applications. DroidBox can install and execute apk applications in the Android emulator. For each malware sample in DREBIN/Koodous, we execute the malware for 120 seconds and log all its activities through DroidBox, which include: file system activities (read/write), network activity (sendnet/recevnet), usage of cryptographic primitives, dynamic loading of classes, start of new services (background processes), generation of system events. We did not use simulated user input because: (i) a random input simulator would prevent deterministic code execution, which is important for malware classification; (ii) designing a deterministic input simulator to be run on all applications would be a huge challenge as many malware applications crash often.

![Fig. 2: Example of (a) write-log and (b) SMS activity log generated by DroidBox.](image-url)

**Fig. 2:** Example of (a) write-log and (b) SMS activity log generated by DroidBox.

Figure 2(a) shows a sample Droidbox log of a filesystem **write** operation, where about 1.9s after starting the execution of the malware, some data is written in /data/com.app/stats.log. The “data” field in Figure 2(a) contains the data written by the application in hexadecimal format. Figure 2(b) shows another sample log related to SMS sending activity. Many malware try to deceptively send SMSs to premium-rate numbers owned by the malware developer in order to get money from the user. Sometimes, SMSs are also used to spread the malware by sending a text to users from a contact list to deceive them into clicking a malicious URL. Details of the dynamic log generation process can be found in the supplementary materials.

#### 4.3.2 Dynamic Feature Extraction

Our goal is to design features that capture similarities in malware behaviors in order to classify samples into families. Dynamic logs allow us to even design very low-level features, such as read operations on specific data from files

---

7. [https://github.com/androguard](https://github.com/androguard)
9. [http://www.inetsim.org](http://www.inetsim.org)
10. [https://github.com/pjlantz/droidbox](https://github.com/pjlantz/droidbox)
TABLE 2: Dynamic features derived from the execution of the Android malware samples using bag of words.

<table>
<thead>
<tr>
<th>Group</th>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RW</td>
<td>read [[&lt;basepath&gt;] [&lt;filename&gt;]]</td>
<td>N-gram counts about read operations on the Android filesystem. The basepath is just the name of the first folder after the root</td>
</tr>
<tr>
<td></td>
<td>write [[&lt;basepath&gt;] [&lt;filename&gt;]]</td>
<td>N-gram counts about write operations on the Android filesystem. The basepath is just the name of the first folder after the root</td>
</tr>
<tr>
<td>System</td>
<td>start [&lt;service-name=]</td>
<td>N-gram counts about started background processes (i.e., services)</td>
</tr>
<tr>
<td></td>
<td>load [[&lt;classpath&gt;] [&lt;classname&gt;]]</td>
<td>N-gram counts about Dex Android classes loaded during execution</td>
</tr>
<tr>
<td></td>
<td>receive [[&lt;path&gt;]=&lt;name&gt;]</td>
<td>N-gram counts about operations performed during execution</td>
</tr>
<tr>
<td>Network</td>
<td>sendnet [[&lt;protocol&gt;] [&lt;port&gt;]]</td>
<td>N-gram counts about outgoing network activity</td>
</tr>
<tr>
<td></td>
<td>request [[&lt;protocol&gt;] [&lt;port&gt;]]</td>
<td>N-gram counts about incoming network activity</td>
</tr>
<tr>
<td>SMS</td>
<td>sendsms [[&lt;phonenumber&gt;]=&lt;message&gt;]</td>
<td>N-gram counts about SMS sent by the application</td>
</tr>
</tbody>
</table>

and folders at particular timestamps. However, past work shows that overly detailed dynamic features rarely improve malware classification [28], [31] as they inject noise. We therefore leverage an n-gram representation commonly used in malware analysis and classification (e.g., [18], [31], [33], [52]). Using n-grams, we count the following operations captured by the sandbox: RW (read and write operations), System (e.g., start of a new background process), Network (Internet requests), SMS (texts sent by the device). For each dynamic log operation, we extract several possible sets of words to limit the impact of possible obfuscation strategies adopted by the attacker (e.g., changing the filename of a written file). For this purpose, we consider a bag of word approach in which we extract n-gram counts. In particular, we have experimentally verified that considering n-grams with n > 3 does not yield any performance improvement (because the level of details increases and features become too specific, as discussed in [28], [31]), so we consider unigrams, bigrams and trigrams. Each word is a feature, where the value is represented by the number of occurrences of that keyword in the logs [52]. The idea is that similar malware execute similar types of operations.

To clarify how the bag of words for dynamic features are extracted, consider an example based on the write log of Figure 2(a). Since we consider up to 3-grams, we can extract the following four words from this log: (i) write, (ii) write /data/; (iii) write /data/stats.log, (iv) write /data/stats.log. The first word corresponds just to the name of the executed operation. In the second word, we extract only the basepath /data/ instead of the fullpath /data/com.app/ (i.e., the first folder name in the path, in addition to the root folder) because most Android folders are dependent on Application names (e.g., com.app in the example) or process ids, but the basepaths are unique [31]. We do not include the content written – we verified that it is not useful for malware classification, as many malware read files in different sequences (e.g., a 256 byte file read 1 or 2 bytes at a time), and also use encryption strategies to hide the real read/written content. Note that feature values represent number of occurrences of a word in the dynamic log of the malware sample.

We can then define a generalized version of a write operation feature set as follows:

\[
\text{write \left[ \left[ \text{< basepath >} \right]\left[ \text{<filename> } \right] \right]}
\]

where items between squared brackets are optional (hence, if one considers all the possible combinations she can obtain four words).

Table 2 reports the full list of dynamic feature types extracted with the bag of words approach. The rationale behind the design of these features is to capture similarities in malware behaviors by counting the number of high-level actions of each sample [31]. Section 7 shows that dynamic features are effective in characterizing different malware families (cf. supplementary materials): for example, Opfake loads a malicious apk in memory at runtime through the dexclass loading function; MobileTx sends SMS to premium-rate numbers; Geinimi starts a fake background process called GoogleKeyboard that collects user information that are then sent outside.

Note that since we always consider 1-gram counts consisting of just the operation (e.g., write, read), our approach also captures the total number of dynamic operations of each kind executed by a malware.

By executing DREBIN malware samples, we collect 6,875 dynamic features corresponding to the set of possible words of Table 2. We then drop all the features that have value 0 (i.e., never occurred) for all malware samples except one. In other words, we drop all n-grams executed by just a single malware sample in the dataset – as they do not contribute to the malware classification task; thus we are left with 2,048 dynamic features.

5 DISCOVERING ANDROID MALWARE FAMILIES

5.1 Supervised Classification

We consider six standard supervised classifiers – Decision Tree (DT), K-Nearest Neighbors (K-NN), Logistic Regression (LR), Naive Bayes (NB), Support Vector Machine (SVM), and Random Forest (RF). We perform hyper-parameter optimization in order to find the parameters that generate the best results. For instance, we use CART with Gini gain criteria for DT; K-NN method with K = 5; multinomial logistic regression and SVM with linear kernel. Section 6 shows that Random Forest turns out to be the best classifier in general, but fails to capture small families. This motivated us to run unsupervised clustering algorithms with the hope that interdependency between malware samples captured via clustering might help in detecting small families.

5.2 Unsupervised Clustering

We consider five well known clustering methods previously used in malware analysis: [17], [26]: DBSCAN, Hierarchical with complete linkage and Euclidean distance, Affinity, K-Means and MeanShift. The value of K in K-Means was determined by the Silhouette Method. Other parameters were systematically tuned to get the best performance.

Section 8 shows that DBSCAN turns out to be the best clustering algorithm. Although it accurately captures small families, its overall performance is significantly worse than
the best classification algorithm. This further motivates us to combine both the results of classification and clustering in a systematic way to improve the overall performance as well as to detect small families.

5.3 EC2: Combining Classification and Clustering

Section 6 will show that while classification methods perform well on families with at least 10 samples, they fail to predict small families effectively. On the other hand, clustering methods efficiently capture small families. To get the best of both worlds, we propose EC2 (Ensemble Clustering and Classification) which combines the results of classification and clustering in a systematic way (see Algorithm 1).

In the initial steps, EC2 uses an unsupervised clustering method $A_{uc}$ to cluster all the samples (Step 1). In parallel, it trains a supervised classifier $A_{sc}$ on training set $TR$ (Step 2) and measures the membership probability of each test sample for each family (Step 4). If a test sample achieves a maximum membership probability greater than a certain threshold $\delta_1$, it is assigned to the corresponding family (Step 8); otherwise it is marked as “unlabeled” (Step 10). In Section 9.2, we vary the value of $\delta_1$, and observe that the highest accuracy is obtained with $\delta_1 = 0.6$. For each such unlabeled sample $s$, EC2 first checks the cluster $C_s$ where it is assigned by $A_{uc}$ (Step 13). If more than $\delta_2$ fraction of the constituent members in $C_s$ have already been labeled with a single family $f$, then $s$ is labeled with $f$ (Step 15); otherwise $s$ is labeled with a new family $C_s$. Note that in this step if there is a tie in the size of the classes inside the cluster $C_s$, we by randomly assign the sample into one of the majority classes\(^\text{11}\). Moreover, Step 17 enables us to create a completely new family which may not be present in the training set, allowing us to identify completely unobserved families.

**Illustrative Example:** Figure 3 shows an example of EC2 in action. Suppose there are six samples $O_1, \cdots, O_6$. A classification algorithm $A_{sc}$ classifies the samples with a probability distribution as shown in Figure 3(a). If $\delta_1 = 0.7$, then samples $O_1$ and $O_3$ are assigned to class $C_1$ because the membership probability of both these samples is above 0.7 (Figure 3(b)). No other samples are assigned to a class due to the lack of high confidence. Therefore, we run a clustering algorithm $A_{uc}$ that may group them into three clusters $G_1, G_2, G_3$ (Figure 3(c)). For the unassigned samples we use the clustering results as follows. For instance, in the case of $O_2$ we see that it belongs to cluster $G_1$, and there are two other samples $O_1$ and $O_3$ which also belong to $G_1$. Now, out of 3 samples in $G_1$, two are already labeled as $C_1$ from the classification result, i.e., more than $\delta_2$ (which is set as 0.6) fraction of samples in $G_1$ are labeled as $C_1$. Therefore, $O_2$ is also assigned to $C_1$. However for $O_5$ and $O_6$ which belong to $G_2$ and there is no other member labeled earlier, we assign them separately in a class $G_2$. Similarly $O_4$ is assigned to a singleton class $G_3$.

**Time Complexity:** Assume that there are $n$ malware samples and $f$ families in the test set. Once we obtain the results of the classification and clustering algorithms,

\(^\text{11}\) Note that if $\delta_2$ is greater than 0.5, there is no possibility that a tie is encountered.

---

**Algorithm 1: EC2 algorithm**

```
Input: Training set $TR$, test set $TS$, thresholds: $\delta_1$ and $\delta_2$, Classification alg: $A_{sc}$, Clustering alg: $A_{uc}$
Output: Labeled families of $TS$
1. Run $A_{uc}$ on $TR + TS$ and obtain set of clusters $C$;
2. Train $A_{sc}$ on $TR$;
3. for each $s \in TS$ do
4. $MP[s, f] \leftarrow$ Membership probability of $s$ in family $f$ obtained from $A_{sc}$;
5. $mp^* \leftarrow \max_{f} MP[s, f]$;
6. $f^* \leftarrow \arg\max f MP[s, f]$;
7. if $mp^* \geq \delta_1$ then
8. $L[s] \leftarrow f^*$; \hspace{1cm} \triangleright$ Assigning family label of $s$
9. else
10. \hspace{1cm} Push($UnlabeledS$, s) \hspace{1cm} \triangleright$ Push $s$ into UnlabeledS
11. while $UnlabeledS$ is not empty do
12. $s \leftarrow$ Pop($UnlabeledS$);
13. $C_s \leftarrow$ Cluster of $s$ (where $C_s \in C$);
14. if More than $\delta_2$ fraction of the samples in $C_s$ are labeled with a family $f$ then
15. $L[s] \leftarrow f$;
16. else
17. $L[s] \leftarrow C_s$;
18. return $L$;
```

---

Fig. 3: An illustrative example EC2. Six samples $O_1, \cdots, O_6$ are finally grouped into three clusters $C_1, G_2, G_3$.

---

6 Performance of Supervised Classifiers

In this section, we provide the performance of the classifiers. We start with the metrics used to evaluate the performance of the classifiers, followed by a comparative evaluation.
6.1 Evaluation Metrics

As the size distribution of malware families is highly skewed (cf. Figure 1(a)), we examine the performance of the classifiers at Macro (Ma) and Micro (Mi) levels. At each level, we consider Precision (P), Recall (R), F-Score (F) and Area under the ROC curve (AUC). At macro (resp. macro) level, Precision, Recall and F-Score are denoted as MiP, MiR and MiF (resp. MaP, MaR and MaF) respectively. Each of such metrics ranges from 0 (no match) to 1 (exactly similar).

We recall how Micro and Macro statistics are computed for evaluating multi-class classifiers. Given a classifier and a malware family \(i\), we let \(TP_i\), \(FP_i\), and \(FN_i\) indicate True Positive, False Positive and False Negative samples, respectively. Then, for \(n\) different families, Micro Precision (MiP) and Macro Precision (MaP) are:

\[
MiP = \frac{\sum_{i=1}^{n} TP_i}{\sum_{i=1}^{n} TP_i + FP_i} \quad (2)
\]

\[
MaP = \frac{\sum_{i=1}^{n} TP_i}{\sum_{i=1}^{n} TP_i + FP_i} \quad (3)
\]

We also observe that micro statistics suppress the results of small clusters over those of large clusters.

6.2 Performance Analysis

We observe that Random Forest (RF) achieves the highest overall classification accuracy after 5-fold cross-validation\(^{12}\) (see Supplementary Materials for the performance of the other classifiers). RF yields a MaF=0.65 and MaAUC=0.83, and MiF=0.93 and MiAUC=0.97 averaged over 50 iterations for all families (including the ones with less than 10 samples). Small families lead to lower values for macro statistics because these are difficult to predict due to the lack of training data. Performance of small families will be separately discussed in Section 6.4. For now, we consider only families with size \(\geq 10\) (44 families, 4,545 samples).

**Composite Performance:** Figure 4(c) shows performance of all classifiers on families of size \(\geq 10\) considering both static and dynamic features. For better visualization we adopt the setup used in [25] – for each evaluation metric (such as MiF, MaF, MiAUC, MaAUC), we separately scale the scores of the methods so that the best performing method has a score of 1. The composite performance of a method is the sum of the four normalized scores. If a method outperforms all other methods, then its composite performance is 4 (See Supplementary Materials for the actual performance value of the classifiers).

Figure 4(a) shows the composite performance of all the classifiers for different feature sets. Considering both static and dynamic features, Random Forest outperforms all others (with composite performance of 4), followed by DT (3.92), K-NN (2.24), SVM (2.15), NB (1.99) and LR (1.94). The superior performance of DT corroborates the results in [15], [41] for separating malware from benign applications and might be due to the categorical features such as author, structure and permissions. As described in [24], K-NN and DT are extremely useful when the features are categorical and/or a mixture of continuous and categorical. This might also explain the poor performance of SVM. Figure 4(b) presents the relative performance of the classifiers by individually considering dynamic features and both static and dynamic features together w.r.t. the performance with only static features (which were used in most previous mobile malware classification research [30], [34], [56]).

Figure 4(b) reports that for all classifiers the relative performance exceeds one in most cases, showing that dynamic features improve classification accuracy compared to static ones. Although the relative performance of K-NN, LR, NB and SVM is higher with only dynamic features, among all classifiers the best absolute performance is achieved by Random Forest with both static and dynamic features (Figure 4(c)). Moreover, Section 7 will show that adopting both kinds of features is also extremely useful in distinguishing characteristics of each malware family. Therefore, unless otherwise mentioned, we will present results that include both static and dynamic features and that refer to the best classifier (RF).

**Family-wise Performance:** To understand the detailed results of the classifier, Figure 5 shows the family-wise accuracy of Random Forest, the best classifier. We consider all the detected (resp. ground-truth) families, sort them by descending order of size, and plot the Precision (resp. Recall) for the families with at least 10 samples in Figure 5(a) (resp. Figure 5(b)). We observe high Precision irrespective of family size, whereas Recall drops slightly for smaller families. The small performance drop at bin 5 for both Precision and Recall is caused by two malware families, Boxer and SMSreg, that have some hard-to-detect variants.

6.3 Prediction of Unknown Families

Thus far, out of total 4,845 samples we have considered 4,545 samples belonging to 44 large families (families with at least 10 samples). However, there are 300 other malware samples present in a total of 112 small families. In this experiment, we treat these 300 malware samples as “unknown malware samples”. In particular, out of 4,545 samples (with size greater than 10) we randomly choose 4,245 samples for our training set (set I). Two test suites are prepared for this experiment: (i) Set II: the remaining 300 samples from large families out of 4,545 sample set, (ii) Set III: 300 unknown malware samples (belonging to 112 small families) whose representatives are absent in the training set. The classifiers are trained on Set I to predict samples in Set II and Set III. The experiment is repeated 50 times to see how the classifier performs especially for Set III. We wish to show that a standard classifier should identify the family of a sample with high confidence if the malware belongs to one of the given families. However, if it does not belong to a known family, the classifier should assign it to a known family with low confidence.

We use Random Forest with all (static and dynamic) features to estimate the probability of each test sample belonging to different families. Figure 6(a) shows that Random Forest with the proposed feature set is very confident in labeling Set II (the maximum probability is greater than 0.80 for the great majority of test samples; and MaF and MiF
Fig. 4: Performance for families having \( \geq 10 \) samples averaged over 50 iterations with 5-fold cross-validation on the DREBIN dataset. (a) Composite performance of the classifiers; (b) relative improvement (in terms of Micro AUC) of the classifiers with respect to their performance with only static features (the horizontal dotted red line indicates that both the performance are equal); (c) absolute values of the metrics for all the classifiers considering static and dynamic features together.

Fig. 5: Family-wise accuracy (mean values of (a) Macro Precision (MaP) and (b) Macro Recall (MaR) and their variance) of Random Forest (RF) with static and dynamic features on the DREBIN dataset. The families are grouped in bins and sorted by descending order of their size. The results are obtained with 5-fold cross-validation and averaged over 50 iterations. The small drop in bin 5 is caused by Boxer and SMSreg families, that have variants harder to detect.

Fig. 6: Family membership probability of test samples (300 samples each from (a) known (Set II) and (b) unknown families (Set III)) obtained from Random Forest with static and dynamic features on the DREBIN dataset. For better visualization, we plot top 10 most probable families per test sample and sort families based on descending order of membership probability.

are 0.96 and 0.91); whereas in Figure 6(b) it is extremely erratic in predicting the labels of Set III. As we have seen in Section 5.3, this behavior of the classifier has been leveraged to design the **EC2** algorithm.

### 6.4 Performance for Small Families

Thus far, we have primarily considered 44 families with size \( \geq 10 \). However, there are 109 families that have size \( \geq 2 \), and each of the remaining 47 families has only one sample (singleton families).

We now consider all the families of size \( \geq 2 \) and adopt a 2-fold cross validation using stratified sampling so that at least one sample per family is present in the training set. The experiment is repeated 50 times and the average accuracy is reported. We separately measure class-wise performance. Figure 7 shows the performance of Random Forest for families of size less than \( x \) (where \( 5 \leq x \leq 50 \)) with large families (having size \( \geq 10 \)).

We compare this performance with the performance obtained earlier in Figure 4 for families with at least 10 malware samples. Figure 7 shows that the performance of the classifier drops significantly if we consider only small families in the test set - not surprising due to the small size of the training set. Moreover, although Section 6.3 shows that for samples belonging to unknown families Random Forest is erratic in assigning them into known families, it is not possible for a classifier to identify completely unknown families. This means that singleton families cannot be identified by classifiers. However, because of the huge daily growth in malware variants, it is critical to identify malware families as soon as an application has been detected as malware. This motivates us to study unsupervised clustering algorithms, as presented in Section 8.

### 7 Characterizing Some Malware Families

A security analyst needs both an accurate predictor and to understand which features discriminate between different
malware families. These findings are useful in engineering robust signatures for detection of new malware variants.

Figure 8 reports the top 25 features by decreasing classification weight for the Random Forest multi-class classifier, with static features in yellow and dynamic features in blue (see Table 1 and Table 2 for detailed features description). We see that static features are more important than dynamic ones, probably because Android applications have a rich set of information in their Manifest (i.e., XML-header), making it more challenging for malware authors to create hugely different variants. Figure 8 shows that the most relevant static features are about custom permissions, that can be used for interactions and data sharing between applications with the same author/signature. filesize is also relevant, suggesting that variants of the same malware often share similar size distributions. Another important feature is author, because malware authors might reuse the same signature to publish many variants of their malicious applications on multiple markets. The most important dynamic features include the number of write operations on the filesystem and read cpuinfo, i.e. the number of read operations of CPU characteristics (to learn details of the device hardware to determine possible exploits). The receiver for BOOT_COMPLETED signal is also a top feature – it is often used by malware developers to determine when the device is turned on in order to trigger malicious behavior [14].

Malware family characterization: Apart from the overall discriminative features obtained from the multi-class classification, it is interesting to identify the specific features that characterize and distinguish each malware family from the rest. To this end, we design the following experimental setup – for each of the 44 large malware families, we learn the best binary classifier (Random Forest) to distinguish each family from the rest, such that there exist 44 set of classification rules that separate the behavior of one malware family from all others. In this way, for each family we can sort the features by decreasing weight learned by the classifier, thus ranking the features that are more relevant for classification.

Figure 9 shows relevant examples of the top 3 features for families of different sizes. Each row in Figure 9 corresponds to a different family. Each histogram reports feature values on the X-axis, and the percent of malware samples having that feature value on the Y-axis. We report results about the following families:

- FakeInstaller pretends to be an app that installs (or uninstalls) other apps from the system, whereas its primary purpose is to send premium-rate SMS without user consent.
- MobileTx is a Trojan that both steals information and also tries to send premium-rate SMS.
- Geinimi is a Trojan that opens a backdoor to send information from the device to a remote server.

Though some of these families share similar gs (e.g., sending premium-rate SMS), each of them is characterized differently through the top 3 features shown in Figure 9.

FakeInstaller. (discovered in May 2012 [5]) The top 3 features in FakeInstaller are static (see first row of Figure 9). The first feature is related to a permission accessing the network state (i.e., whether a connection is available or not on the device at a given time). This feature is important for discriminating FakeInstaller as it is one of the few malware families that does not require it (i.e., where permission ACCESS_NETWORK_STATE is set to 0, as can be observed in Figure 9). The filesize of FakeInstaller samples is usually lower than the other families. Moreover, the recvaction DATA_SMS_RECEIVED is used to monitor whenever an SMS is received, and is probably used by FakeInstaller to remove evidences of its texts sent to premium-rate number and to abort or delete incoming SMS.

MobileTx. (discovered in May 2012 [5]) The second row of Figure 9 reports the top 3 distinguishing features of the MobileTx family, an SMS-fraud malware. The most important feature involves sendsms activity to the following phone number: 1065-71090-88877. This turns out to correspond to a premium-rate number used to steal money from the victim [37]. We discovered 68 premium numbers used by DREBIN samples. Some of these texts also have predetermined text content which is captured by our dynamic analysis. Moreover, all variants of MobileTx require the RESTART_PACKAGES permission that allows the malware to kill all processes including monitors and antivirus software installed in the device. The histogram in Figure 9 shows that some other malware families (blue bar) also require this permission for the same purpose, but it is not common. Finally, all 21 variants of MobileTx have the same author=443 (that is the anonymized integer for the SHA256 signature), and hence this feature also helps identify this family.

Geinimi. (discovered in Dec 2010 [5]) Geinimi variants steal information such as fine location, device IDs (e.g., IMEI, IMSI) and the list of installed apps. Its top 3 distinguishing feature value distributions are shown in the last

13. The average F-score for the binary classification is even higher than multi-class classification, and is reported in supplementary materials.
14. See supplementary materials for top 5 features and explanations of three other families.
Fig. 9: Feature value comparison between malware families present in the DREBIN dataset. In particular, we report the histogram of the top-3 feature values for the following malware families (number of samples within parenthesis): FakeInstaller (883), MobileTx (21), Geinimi (13). (More families in the supplementary materials). Each row corresponds to a family, and the feature value is compared against all other malware families in the dataset.

row of Figure 9. The first feature is associated with the registration of AdServiceReceiver, a component used to monitor system events on which to trigger malicious behavior (e.g., to send stolen data to remove server). The crypto operations identified in the top 3 features use the DES algorithm to decrypt URLs of the CnC servers and GET commands which are encrypted to avoid static code analysis, but the malware authors recycled decryption keys and hence we detected them during dynamic analysis. The permission MOUNT_UNMOUNT_FILESYSTEMS is used to access data in SD card slots, as some variants of Geinimi use SD cards to store and load repackaged malicious applications downloaded from the CnC servers. The servicestart GoogleKeyboard represents the launch of a background process named GoogleKeyboard (to avoid user detection by looking at the phone task manager) that performs malicious actions, steals information periodically and sends it to the CnC whose URLs are decrypted at runtime.

Finally, some families are better distinguished using static features (e.g., FakeInstaller), whereas others are better distinguished through dynamic features (e.g., MobileTx). These statistics can be used by security analysts to define new signatures for malware classification as they automatically reveal some internals of the code obfuscation techniques adopted for a certain malware family.

8 PERFORMANCE OF CLUSTERING ALGORITHMS

In this section, we start by explaining the metrics used to evaluate clustering algorithms followed by a detailed performance evaluation.

8.1 Evaluation Metrics

We compare the detected clusters with the original families in terms of 5 well-known metrics: Micro F-Score (MiF*), Macro F-Score (MaF*), Normalized Mutual Information (NMI) [27], Adjusted Rand Index (ARI) [39] and Purity (PU) [47]. For MiF*, MaF*, NMI and PU (resp. ARI), the value ranges between 0 (resp. -1) and 1 where 0 (resp. -1) refers to no match with the ground-truth and 1 refers to a perfect match. Note, the definitions of Micro and Macro F-Scores for clustering are slightly different from the ones for the classification. They are defined as follows.

Given $N$ samples and a detected cluster $i$ with size $n_i$, True Positive ($TP_i$) denotes the number of pairs (out of $n_i C_2$) in which both samples belong to the same ground-truth family; if not, they are counted as False Positive ($FP_i$). Similarly, True Negative ($TN_i$) counts the number of pairs that are outside cluster $i$, and that belong to different detected clusters $j$ and $k$ ($i,j,k$ are mutually different), for which both samples belong to different ground-truth families. Once $TP_i, TP_j, TN_i$ are computed for all detected clusters $i$, the calculation of MiF* and MaF* is the same as MiF and MaF (see Section 6.1).

8.2 Performance Analysis

We consider all malware samples in 156 families. Since clustering methods may produce different outputs depending upon the parameter settings and the initial seed selection, we run each clustering method 50 times, and the average performance is reported. Figure 10 shows the composite performance (as discussed in Section 6.2) of all the clustering methods (see Supplementary Materials for the actual performance values). Among all, K-Means performs the best. Figure 10(b) shows the relative performance of the 5 clustering methods using both static and dynamic features as compared to static features alone. Unlike classification, dynamic features alone do not improve performance. In 3 out of 5 cases, the combination of static and dynamic
features leads to an improvement over using static features alone. This suggests that static features are more important than dynamic features in clustering malware. Figure 10(c) shows the number of clusters generated by each method using both static and dynamic features. Figure 10(d) summarizes the accuracy of different methods using both static and dynamic features. Overall, the performance of K-Means averaged over all the evaluation metrics is 0.41, followed by DBSCAN (0.39), Affinity clustering (0.37), Hierarchical (0.29) and MeanShift (0.26). This is in sharp contrast with the results reported in [17] where hierarchical clustering yielded the best results for PC malware. A closer inspection of Figure 10 reveals that DBSCAN dominates others in terms of Micro and Macro F-Score values. The reason might be that DBSCAN correctly identifies True Positives for each cluster/family which information theoretic metrics (such as NMI, ARI) often ignore as pointed in [43]. Moreover, the latter metrics do not penalize clusters with large cardinality and tend to prefer a small number of large clusters (which K-Means produces as shown in Figure 12(a) later). Moreover, K-Means does not capture small families. We now discuss how the clustering methods detect small families.

**Family-wise Performance:** Figure 11(a) shows that irrespective of the size of the clusters detected, DBSCAN achieves better Precision than K-Means. Moreover, Figure 11(b) shows that the DBSCAN’s recall is almost double that of K-Means. These results emphasize the fact that DBSCAN accurately captures the skewed size distribution of Android malware families.

**Performance for Small Families:** Figure 12(a) shows the cumulative distribution of the cluster size obtained from different methods as well as that obtained from the ground-truth families. DBSCAN produces the distribution which is closest to ground-truth in terms of Chi-square correlation (0.95). To identify which method best detects small families, we measure the performance for those clusters/families having size less than \( x \) (10 ≤ \( x \) ≤ 50). Figures 12(b) and 12(c) show that DBSCAN is the best. Interestingly, all clustering methods seem to be quite consistent in the small zones. These results highlight the necessity of adopting clustering methods for identifying small malware families.

**Singleton Families:** For singleton families, DBSCAN and K-Means seem to be the best and the worst methods respectively. The Precision (Recall) of the clustering methods for detecting only singleton families are: DBSCAN: 0.33 (0.13), Hierarchical: 0.22 (0.07), Affinity: 0.06 (0.11), MeanShift: 0.02 (0.05) and K-Means: 0.002 (0.004). The detection of singleton families is very important and hugely challenging (due to lack of training data) because these identify potentially new types of malware that may need new anti-malware signatures.

**8.3 Feature Importance**

We identify the most important features in clustering by measuring the percentage decrease in accuracy (in terms of MaP*) when each feature is dropped. Figure 13 reports results for DBSCAN, where the most important feature groups are D:System, S:Author and S:Permissions. Recall...
from Figure 10(b) that combining static and dynamic features performs well, but dynamic features alone perform worse than static features. This differs from the classification results shown in Figure 4(b) where dynamic features are extremely important. Thus both types of features are important.

Fig. 13: Average performance (MaF∗) decrease per group of static (S) and dynamic (D) features (DBSCAN) on the DREBIN dataset.

To better understand the results in Figure 13, let us look at the top 5 static and dynamic features in Table 3, along with their overall ranking (obtained by sorting for decreasing performance loss). Most of the top 5 dynamic features are related to dexclass operations, that correspond to the loading of particular Android classes during execution. Further inspection reveals that the first dynamic feature corresponds to a class loaded by 10 samples (out of 17) of the FakePlayer malware family, which is a Trojan that tries to send premium-rate SMSs. Table 3 suggests that very specific dynamic features (such as dexclass <class-name>) are used by DBSCAN to discriminate clusters. Therefore, samples with very similar features are grouped into reasonably small clusters, which are not allowed to grow further, resulting in high Precision and low Recall. The most relevant static features are related to Android permissions, such as those to access GPS location, Internet, send SMS or write to external storage. The author is fifth in terms of importance, meaning that it plays a significant role in unsupervised clustering approaches to grouping malware.

TABLE 3: Top 5 features each from static and dynamic set with their overall ranks (OR), sorted by decreasing performance loss of the DBSCAN method for the DREBIN dataset.

<table>
<thead>
<tr>
<th>OR</th>
<th>Static Feature</th>
<th>OR</th>
<th>Dynamic Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>perm:ACCESS_COARSE_LOCATION</td>
<td>1</td>
<td>dexclass org.me.androidapplication1-1.apk</td>
</tr>
<tr>
<td>8</td>
<td>perm:INTERNET</td>
<td>3</td>
<td>dexclass ru.jabox.android.smsbox.lovebox-i.apk</td>
</tr>
<tr>
<td>10</td>
<td>perm:SEND_SMS</td>
<td>4</td>
<td>servicestart PlayerFindService</td>
</tr>
<tr>
<td>11</td>
<td>perm:READ_PHONE_STATE</td>
<td>5</td>
<td>dexclass ru.jabox.android.smsbox.jokebox-i.apk</td>
</tr>
<tr>
<td>12</td>
<td>author</td>
<td>6</td>
<td>dexclass com.agewap.soft1-1.apk</td>
</tr>
</tbody>
</table>

9 PERFORMANCE OF EC2

In this section, we present the performance of EC2. We start by explaining the baseline methods (Section 9.1), followed by a detailed comparative evaluation: Section 9.2 reports results on DREBIN dataset [4], Section 9.3 reports results on the more recent Koodous academic dataset [9].

9.1 Baseline Methods

We consider the following five methods as baselines: (i) best standalone classifier (Random Forest), (ii) RHDL: an SVM based classification of malware behavior [52], (iii) HHC: an ensemble-based hybrid hierarchical clustering [60], (iv) DroidLegacy: an existing algorithm specifically designed for Android malware family classification [30], (v) K2: an ensemble approach where clustering results are used as features for classification [42]. While methods (ii), (iii) and (iv) were applied on malware datasets, method (v) was used for text classification. K2 turned out to be the best baseline.

TABLE 4: Performance of the baseline methods and EC2 on the DREBIN dataset. We consider Random Forest (RF) and different clustering methods separately with δ1 = 0.6 and δ1 = 0.5. The best baseline and the best combination for EC2 are highlighted.

<table>
<thead>
<tr>
<th>Method</th>
<th>MIP</th>
<th>MaF</th>
<th>NMI</th>
<th>ARI</th>
<th>PU</th>
</tr>
</thead>
<tbody>
<tr>
<td>RF (Standalone)</td>
<td>0.63</td>
<td>0.84</td>
<td>0.63</td>
<td>0.13</td>
<td>0.41</td>
</tr>
<tr>
<td>RHDL [52]</td>
<td>0.53</td>
<td>0.81</td>
<td>0.60</td>
<td>0.09</td>
<td>0.41</td>
</tr>
<tr>
<td>HHC [60]</td>
<td>0.68</td>
<td>0.79</td>
<td>0.59</td>
<td>0.08</td>
<td>0.39</td>
</tr>
<tr>
<td>DroidLegacy [30]</td>
<td>0.67</td>
<td>0.82</td>
<td>0.62</td>
<td>0.09</td>
<td>0.35</td>
</tr>
<tr>
<td>K2 [42]</td>
<td>0.72</td>
<td>0.89</td>
<td>0.63</td>
<td>0.11</td>
<td>0.42</td>
</tr>
<tr>
<td>RF+Hierarchical</td>
<td>0.71</td>
<td>0.94</td>
<td>0.69</td>
<td>0.14</td>
<td>0.47</td>
</tr>
<tr>
<td>RF+Affinity</td>
<td>0.69</td>
<td>0.91</td>
<td>0.69</td>
<td>0.69</td>
<td>0.46</td>
</tr>
<tr>
<td>RF+K-Means</td>
<td>0.67</td>
<td>0.90</td>
<td>0.70</td>
<td>0.14</td>
<td>0.47</td>
</tr>
<tr>
<td>RF+MeanShift</td>
<td>0.73</td>
<td>0.93</td>
<td>0.68</td>
<td>0.14</td>
<td>0.46</td>
</tr>
<tr>
<td>RF+DBSCAN</td>
<td>0.76</td>
<td>0.97</td>
<td>0.67</td>
<td>0.14</td>
<td>0.48</td>
</tr>
</tbody>
</table>

9.2 Experimental Results on DREBIN

We consider the entire DREBIN dataset, randomly divide it into 5 folds and predict the families for each fold separately. The following experiment is repeated 50 times and results are averaged.

We assume that each test sample $s_i \in TS$ appears one by one and independently of other test samples. We always use the old and reliable training set $TR$ to classify new test samples $s_t$, instead of augmenting with a newly classified sample. If $s_i$ is classified into one of the existing classes, we keep $s_i$ aside because other representatives of this class are already present in the training set $TS$. If $s_i$ is classified into a completely new class, we use this information in a systematic way. When the next test sample $s_{i+1}$ appears and is classified into a new class by the classifier (trained on $TS$), there are two possibilities – (i) either $s_{i+1}$ belongs to the same class $s_i$ belongs to, or (ii) $s_{i+1}$ forms another new class. We then augment $s_i$ and $s_{i+1}$ into $TS$ and run the clustering algorithm on $TS \cup \{s_i, s_{i+1}\}$. If both of them are clustered together, we assign them same class label; otherwise we keep them separately into two different classes. In this way, we avoid including noise due to old misclassification into the current training set.

We report the results for the best settings of the baseline methods – standalone Random Forest is the first baseline; we use the same configurations proposed in [52] and [60] for RHDL and HHC respectively. For DroidLegacy [30] we extract the Android malware features, run their algorithm using their open-source implementation [7], and report best

15. Augmenting a newly classified sample into the training set might lead to cascading of noise.
results obtained by tuning parameters as recommended in their paper. For K2 we report the results of Random Forest after considering outputs of all the clustering methods as features.

Note that the number of detected clusters and the number of ground-truth families may not be identical (c.f. Figure 3 in which there are 2 classes in the training sample; however we obtain 3 clusters in the final result). Therefore, we compare the performance of EC2 with other baselines using cluster evaluation metrics: MiF*, MaF*, NMI, ARI and PU (see Section 8 for formal definition).

Table 4 shows significant performance gains for EC2 (using Random Forest classifier and different clustering methods with $\delta_1 = 0.6$ and $\delta_2 = 0.5$) and other baselines. The values of the thresholds are selected based on Figure 14 – the performance of Random Forest is best for $\delta_1 = 0.6$ and $\delta_2 = 0.45$. The EC2 algorithm with DBSCAN turns out to be the best in this task – MiF*: 0.76, MaF*: 0.97, NMI: 0.67, ARI: 0.14 and PU: 0.48, which is 6%, 9%, 6%, 27% and 14% higher than the best baseline ($K_2$) respectively. Most importantly, EC2 detects singleton families with average Precision (Recall) of 0.43 (0.31), which is significantly higher than the performance reported in Section 8.2. Interestingly, DroidLegacy which was specifically proposed to classify Android malware families turns out to be even worse than K2 and EC2 when considering all the families. This indicates that ensemble approaches which combine clustering and classification results may be the best choice for classifying malware families.

Finally, we evaluated competing methods separately for small and large families. Table 5 shows that for families with size $\geq 10$, EC2 performs best, even better than Random Forest (standalone). For families with size $< 10$, EC2 performs slightly worse than DBSCAN probably due to some classification noise propagated from the classifier. However, for small families EC2 still outperforms both RF and K2. Although we have shown the performance of EC2 for Android malware prediction, we believe it can also be used in general for other datasets.

### 9.3 Experimental Results on Koodous Dataset

We now present experimental results on the more recent Koodous dataset [9]. Koodous is a community-based platform similar to VirusTotal, but it is entirely focused on static and dynamic analysis of Android malware.

The Koodous academic dataset was generously provided to us by the Koodous administrators and contains 50,000 malware samples spanning from December 2015 to May 2016. This dataset is more recent than DREBIN, but only about 6,700 samples have been labeled with coarse-grained families (namely, categories). We use the labels already provided in this dataset as the ground truth because they have been closely investigated by Koodous administrators. In particular, the dataset contains the following categories (size within the parenthesis): SMS-fraud (3,257), Adware (3,069), Information-Theft (110), Ransomware (95), Fake-Installer (95), Rooting (50), Banker (31).

We use the Koodous dataset because (i) it contains more recent malware (hence it may be interesting to observe how EC2’s performance changes as new obfuscation techniques are encountered), (ii) it contains more coarse-grained families which are more challenging to cluster.

We perform the same feature extraction techniques described in Section 4, and obtain static and dynamic features for the malware samples. We then consider 6,700 labeled malware samples, randomly divide it into 5 folds and predict the families for each fold separately. The following experiment is repeated 50 times and results are averaged.

### 10 Conclusions

This paper makes several major contributions. First, we proposed a systematic analysis of state-of-the-art classification and clustering algorithms applied to the task of grouping
Android malware into families, and by considering different combinations of static and dynamic features. Second, we proposed EC2, the first algorithm used to group malware into families that uses an ensemble of both classification and clustering approaches. Third, we show that the performance of EC2 is high even when considering families of all sizes, achieving an overall Micro and Macro F-Score of 0.76 and 0.97, respectively. Moreover, EC2 also works well on small malware families which can be very hard to identify, yielding to an F-Score of 0.36 for singleton families which is very good, given the lack of training data. Fourth, a detailed analysis of some Android malware families reveals that our approach is also effective in characterizing and explaining behavior of Android malware families. Fifth, we showed that EC2 is equally successful in detecting families of more recent malware samples, and also performs significantly well with obfuscated feature set. Future work might involve how to group malware families into more coarse-grained categories and improve data-driven understanding of malware behaviors. Moreover, since malware authors may employ increasingly sophisticated obfuscation techniques, future work may also address how to design automated feature combination strategies to make it harder for the attacker to evade classification. For instance, instead of using a base set of features, we could replace them for analysis purposes with various linear or non-linear combinations of features.

Acknowledgments

The authors would like to acknowledge the suggestions of the anonymized reviewers. Part of this work was funded by ONR Grants N000141612739, N000141512007, N000141612896, and N000141512742, ARO grant W911NF1410358 and Maryland Procurement Office grant H9823014C0137.

References


Tanmoy Chakraborty is an Assistant Professor and a Ramanujan Fellow in the Dept of Computer Science & Engineering, Indraprastha Institute of Information Technology Delhi (IIIT-D). Prior to this, he was a postdoctoral researcher at University of Maryland, College Park, USA. He finished his Ph.D as a Google India Ph.D fellow from IIT Kharagpur, India in 2015. His Ph.D thesis was recognized as best thesis by IBM Research India, Xerox research India and Indian National Academy of Engineering (INAE).

His broad research interests include Data Mining, Social Media and Data-driven Cybersecurity. Home page: http://faculty.iiitd.ac.in/~tanmoy/

Fabio Pierazzi is a postdoctoral researcher at the University of Modena and Reggio Emilia, Modena, Italy. In the same institute, he completed the Master’s Degree in Computer Engineering in 2013 and the PhD in Computer Science in 2017. During 2016, he spent 10 months as a visiting research scholar at the Department of Computer Science, University of Maryland, College Park, MD, USA. His research interests focus on security analytics, network security, malware classification, intrusion detection, and all solutions that combine cybersecurity and data mining. Home page: http://weblab.ing.unimo.it/people/fpierazzi

V. S. Subrahmanian is the Dartmouth College Distinguished Professor in Cybersecurity, Technology, and Society. From 1989 to 2017, he was a Professor with the Department of Computer Science, University of Maryland, College Park, having previously served as Director of the University of Maryland Institute for Advanced Computer Studies (UMIACS). He was with the Editorial Boards of numerous ACM and IEEE journals as well as Science, the Board of Directors of the Development Gateway Foundation (set up by the World Bank), SentiMetrix, Inc., and with the Research Advisory Board of Tata Consultancy Services. He has worked extensively at the intersection of databases and artificial intelligence. He has authored over 200 refereed publications, and is a Fellow of both AAAI and AAAS. Home page: https://www.cs.umd.edu/users/ves/
1 Malware Family Distribution

We observe that the size of the malware families present in our dataset follows a skewed distribution. In Figure 1, we plot the non-cumulative size distribution of malware families. We notice that out of 156 families, there are 47 families of size 1, 20 families of size 2, and 112 families of size less than 10.

![Size versus frequency of malware families](image)

Fig. 1: Number of malware family of certain size.

2 Generation of Malware Dynamic Logs

This section provides more comprehensive details on how the dynamic malware logs have been generated.

The DREBIN malware samples have been dumped into a Ubuntu 16.04 server which was completely disconnected from the Internet in order to avoid malware spread risks. On this server, we installed and configured the official Android emulator, which represents a fully-functional Android system that runs application with a graphical user interface. Command-line Linux debug tools such as 

| adb | allows to log system events (e.g., READ and WRITE operations of an application) and provide an interface to the Android emulated device.

Since the malware may not trigger its malicious behavior in the absence of network connectivity, we used a network simulator tool purposely intended for malware analysis: inetsim, that simulates many network services, including HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, DNS, FTP, FTPS, TFTP, IRC, NTP. Moreover, inetsim also provides realistic files in response to malware requests (e.g., if the malware tries to download an .exe file from an external website).

To run the malware samples, we used DroidBox 4.1.1, an open-source sandbox especially tailored for dynamic malware analysis of Android application. DroidBox comes with an Android filesystem and RAM that contain some realistic but fake data (e.g., contacts, SMS, phone logs) and that are used to restore the Android emulator to a consistent state after each malware execution. DroidBox builds upon an emulator running an Android 4.1.2 image, which is the late 2012 edition of Android, and is perfectly aligned with the DREBIN dataset that spans from 2010 to 2012. DroidBox can install and execute .apk applications in the Android emulator. For each malware sample in the DREBIN dataset, we execute the malware for 120 seconds and log all its activities through DroidBox, which include: file system activities (read/write), network activity (sendnet/recvnet), usage of cryptographic primitives, dynamic loading of classes, start of new services (background processes), generation of system events. After the execution of each malware, the emulator is restored to the initial state, so that the execution of the next malware does not pollute the environment. In this paper we consider the 4,845 samples that were executed without crashes during the 120 seconds time span. The execution of the overall dataset spanned over about three weeks.

Figures 2 report an example related to logs generated by execution in DroidBox. Figure 2(a) reports a log of a write operation on the filesystem, where after about 1.9s from starting the execution of the malware on DroidBox, some data is written in /data/com.app/stats.log. The field named “data” in Figure 2(a) contains the data written by the application in hexadecimal format. In Figure 2(b) we report another example of a log related to SMS sending activity.

- T. Chakraborty is with Dept. of Computer Science and Engineering, Indraprastha Institute of Information Technology, Delhi (IIIT-D), India. F. Pierazzi is with the Department of Engineering “Enzo Ferrari”, University of Modena and Reggio Emilia, 41125 Modena, Italy. V.S. Subrahmanian is with Department of Computer Science, Dartmouth College, Hanover, NH 03755, USA.

E-mail: tanmoy@iiitd.ac.in, fabio.pierazzi@unimore.it, vs@umiacs.umd.edu

Manuscript received November, 2016; revised –.

3. https://github.com/pjlantz/droidbox
In this section, we report the detailed raw values of classification performance discussed in Section 6.

### 3.1 All families

Table 1 reports the detailed results of supervised classifiers comparison in which we consider all malware families, including singleton families consisting of only one malware sample. Results are computed with 5-fold cross-validation and averaged over 50 iterations. Table 1 reports results for Decision Tree (DT), K-NearestNeighbor (K-NN), Logistic Regression (LR), Naive Bayes (NB), Support Vector Machines (SVM) and Random Forest (RF). Results in Table 2 refer also to three set of features: only static, only dynamic, and both static and dynamic. Reported results correspond to Micro F-Score (MiF), Macro F-Score (MaF), Micro AUC (MiAUC) and Macro AUC (MaAUC). Formal definitions of these metrics are reported in Section 6.

The purpose of this experiment is to show how supervised classification performance decreases significantly when also considering also small families. As expected, Table 1 shows that the worst performance are associated with Macro statistics, because they are computed as an average of the characteristics of each family. Hence, the low performance on small families and singletons decrease the Macro performance.

### 3.2 Families with at least 10 samples

Table 2 reports the 5-fold results averaged over 50 iterations with all the classifiers considered in the previous sections. In particular, it reports results for Decision Tree (DT), K-NearestNeighbor (K-NN), Logistic Regression (LR), Naive Bayes (NB), Support Vector Machines (SVM) and Random Forest (RF). Results in Table 2 refer also to three set of features: only static, only dynamic, and both static and dynamic. Reported results correspond to Micro F-Score (MiF), Macro F-Score (MaF), Micro AUC (MiAUC) and Macro AUC (MaAUC). Formal definitions of these metrics are reported in Section 6.

As expected, the classifiers performance on families with at least 10 samples are higher to performance obtained when considering all families. This is especially evident in the Macro statistics. Moreover, Table 2 shows that although some of the classifiers achieve better performance with only dynamic features, the best overall classification performance is achieved by RF with both static and dynamic features.

### 3.3 Binary classification

In this section we report a table with the raw binary classification performance. Table 4 reports results for the Random Forest classifier, for different feature combinations. In most cases, performance are even higher than the multiclass classification, although some samples (e.g., Zitmo) are harder to classify correctly due to stronger obfuscation techniques.
TABLE 3: Raw performance on the clustering algorithms on different feature sets (static, dynamic, static+dynamic).

<table>
<thead>
<tr>
<th></th>
<th>Clustering</th>
<th>MiF*</th>
<th>MaF*</th>
<th>NMI</th>
<th>ARI</th>
<th>PU</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DBSCAN</td>
<td>0.17</td>
<td>0.80</td>
<td>0.61</td>
<td>0.10</td>
<td>0.46</td>
</tr>
<tr>
<td>Static</td>
<td>Hierarchical</td>
<td>0.22</td>
<td>0.61</td>
<td>0.71</td>
<td>0.20</td>
<td>0.40</td>
</tr>
<tr>
<td></td>
<td>Affinity</td>
<td>0.11</td>
<td>0.66</td>
<td>0.63</td>
<td>0.10</td>
<td>0.27</td>
</tr>
<tr>
<td></td>
<td>K-Means</td>
<td>0.15</td>
<td>0.68</td>
<td>0.70</td>
<td>0.19</td>
<td>0.48</td>
</tr>
<tr>
<td></td>
<td>MeanShift</td>
<td>0.16</td>
<td>0.72</td>
<td>0.29</td>
<td>0.03</td>
<td>0.10</td>
</tr>
<tr>
<td>Dynamic</td>
<td>DBSCAN</td>
<td>0.15</td>
<td>0.86</td>
<td>0.46</td>
<td>0.03</td>
<td>0.36</td>
</tr>
<tr>
<td></td>
<td>Hierarchical</td>
<td>0.12</td>
<td>0.43</td>
<td>0.66</td>
<td>0.10</td>
<td>0.27</td>
</tr>
<tr>
<td></td>
<td>Affinity</td>
<td>0.11</td>
<td>0.62</td>
<td>0.58</td>
<td>0.07</td>
<td>0.29</td>
</tr>
<tr>
<td></td>
<td>K-Means</td>
<td>0.15</td>
<td>0.67</td>
<td>0.59</td>
<td>0.09</td>
<td>0.42</td>
</tr>
<tr>
<td></td>
<td>MeanShift</td>
<td>0.16</td>
<td>0.80</td>
<td>0.25</td>
<td>0.04</td>
<td>0.09</td>
</tr>
<tr>
<td>Stat.+Dyn.</td>
<td>DBSCAN</td>
<td>0.17</td>
<td>0.90</td>
<td>0.44</td>
<td>0.02</td>
<td>0.44</td>
</tr>
<tr>
<td></td>
<td>Hierarchical</td>
<td>0.10</td>
<td>0.35</td>
<td>0.67</td>
<td>0.10</td>
<td>0.24</td>
</tr>
<tr>
<td></td>
<td>Affinity</td>
<td>0.11</td>
<td>0.57</td>
<td>0.66</td>
<td>0.13</td>
<td>0.36</td>
</tr>
<tr>
<td></td>
<td>K-Means</td>
<td>0.15</td>
<td>0.60</td>
<td>0.68</td>
<td>0.14</td>
<td>0.46</td>
</tr>
<tr>
<td></td>
<td>MeanShift</td>
<td>0.16</td>
<td>0.82</td>
<td>0.22</td>
<td>0.03</td>
<td>0.07</td>
</tr>
</tbody>
</table>

4. The average F-score for the binary classification is even higher than multi-class classification, and is reported in supplementary materials.

4  CLUSTERING PERFORMANCE

In this section we report the detailed clustering performance results of Section 8. In particular, Table 3 reports the results of the following clustering algorithms: DBSCAN, Hierarchical Clustering (we report the best results achieved with Complete Linkage), Affinity Clustering, K-Means, MeanShift. We report the performance in terms of the following clustering metrics: Micro F-Score (MiF*), Macro F-Score (MaF*), Normalized Mutual Information (NMI), Adjusted Rand Index (ARI), and Purity (PU). Description of these metrics are reported in Section 8.

5  MALWARE FAMILY CHARACTERIZATION

Apart from the overall discriminative features obtained from the multi-class classification, it is interesting to identify the specific features that characterize and distinguish each malware family from the rest. To this end, we design the following experimental setup – for each of the 44 large malware families, we learn the best classifier (Random Forest) to distinguish each family from the rest, such that there exist 44 set of classification rules that separate the families.

In this section we report the detailed clustering performance results of Section 8. In particular, Table 3 reports the results of the following clustering algorithms: DBSCAN, Hierarchical Clustering (we report the best results achieved with Complete Linkage), Affinity Clustering, K-Means, MeanShift. We report the performance in terms of the following clustering metrics: Micro F-Score (MiF*), Macro F-Score (MaF*), Normalized Mutual Information (NMI), Adjusted Rand Index (ARI), and Purity (PU). Description of these metrics are reported in Section 8.

- **FakeInstaller** pretends to be an app that installs (or uninstalls) other apps from the system, whereas instead its primary purpose is to send premium-rate SMS without the user consent.
- **Opfake** is another malware family that sends premium-rate SMS (i.e., to register a premium-rate number and to abort or delete incoming SMS). Moreover, the overall number of permissions required by FakeInstaller is lower than the average for the other malware categories (less than 15 permissions, of only about 5 of which are marked as dangerous).

**Fakelnstaller.** Four of the top 5 features in FakeInstaller are static. The top 5 features distributions are reported in the first row of Figure 3. The first feature is related to a permission accessing the network state (i.e., whether at a certain moment a connection is available or not on the device). This feature is important for discriminating FakeInstaller as it is one of the few malware families that does not require it (i.e., where permission ACCESS_NETWORK_STATE is set to 0, as can be observed in Figure 3). The filesize of FakeInstaller samples is usually lower than the other families. Moreover, the recvstaction DATA_SMS_RECEIVED is used to monitor whenever an SMS is received, and is probably used by FakeInstaller to remove evidences of its texts sent to premium-rate number and to abort or delete incoming SMS. Moreover, the overall number of permissions required by FakeInstaller is lower than the average for the other malware categories (less than 15 permissions, of only about 5 of which are marked as dangerous). This is probably because this type of family is very targeted for SMS fraud.

**Opfake.** Although Opfake shares a similar goal as FakeInstaller (i.e., SMS fraud), in the second row of Figure 3 we see that its top 5 distinguishing features are different. In particular, the most relevant feature to distinguish Opfake is related to the author attribute (each author found in the dataset is mapped to an integer value on the X-axis of Figure 3). This is because the classifier discriminates that the majority of Opfake variants have been signed with the same signature. Out of the 607 samples in Opfake, 496 samples have author=697, 60 samples have author=740, and 40 samples have author=40, and others have different authors. Opfake also modifies the settings.xml file, which is not touched by the majority of other malware families. It also loads an apk in memory, which may be a repacked application that contains the actual malicious code. Finally, a peculiarity of Opfake is that its Activities (i.e., windows shown to the user) are very few – less than 10, whereas most malware have at least 20. Its filesize is also usually smaller than other families.

**GinMaster.** The GinMaster family is another malware family that sends premium-rate SMS, and often tries to perform aggressive advertisement and to install unwanted toolbars.

- **Geinimi** is a Trojan that opens a backdoor to send information from the device to a remote server.

Despite the fact that some of these families share a similar purpose (e.g., sending premium-rate SMS), each of them is characterized differently through the top 5 features shown in Figure 3.

**FakeInstaller.** Four of the top 5 features in FakeInstaller are static. The top 5 features distributions are reported in the first row of Figure 3. The first feature is related to a permission accessing the network state (i.e., whether at a certain moment a connection is available or not on the device). This feature is important for discriminating FakeInstaller as it is one of the few malware families that does not require it (i.e., where permission ACCESS_NETWORK_STATE is set to 0, as can be observed in Figure 3). The filesize of FakeInstaller samples is usually lower than the other families. Moreover, the overall number of permissions required by FakeInstaller is lower than the average for the other malware categories (less than 15 permissions, of only about 5 of which are marked as dangerous). This is probably because this type of family is very targeted for SMS fraud.

**Opfake.** Although Opfake shares a similar goal as FakeInstaller (i.e., SMS fraud), in the second row of Figure 3 we see that its top 5 distinguishing features are different. In particular, the most relevant feature to distinguish Opfake is related to the author attribute (each author found in the dataset is mapped to an integer value on the X-axis of Figure 3). This is because the classifier discriminates that the majority of Opfake variants have been signed with the same signature. Out of the 607 samples in Opfake, 496 samples have author=697, 60 samples have author=740, and 40 samples have author=40, and others have different authors. Opfake also modifies the settings.xml file, which is not touched by the majority of other malware families. It also loads an apk in memory, which may be a repacked application that contains the actual malicious code. Finally, a peculiarity of Opfake is that its Activities (i.e., windows shown to the user) are very few – less than 10, whereas most malware have at least 20. Its filesize is also usually smaller than other families.

**GinMaster.** The GinMaster family is better discriminated through dynamic features, since all its top 5 features shown in Figure 3 are dynamic. The first feature is read cpuinfo, and is probably used to determine the hardware characteristics of the mobile device. This infor-
mation is used by GinMaster to determine if the device is susceptible to rooting exploits that allow the malware to get root privileges on the smartphones. The write operations (up to 20 operations per file) on files such as icons_android.ico, icons_com.svox.pico.ico and installer.xml are probably performed to attempt privilege escalation and get full access on device data. The recvsaction USER_PRESENT allows an app to control status bar, and is usually used only by system applications. The same consideration holds for permissions JiFake to read and write the calendar. The READ_FRAME_BUFFER permissions allows to take screenshots of other applications, whereas CONTROL_LOCATION_UPDATES allows it to modify whether phone location is updated or not. We thus observe that though the primary purpose of JiFake is to send premium-rate SMS, these permissions are involved with an additional behavior of some JiFake variants that try

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mf</td>
<td>MaF</td>
<td>MaAUC</td>
</tr>
<tr>
<td>Fakelnstaller</td>
<td>0.98</td>
<td>0.98</td>
<td>0.98</td>
</tr>
<tr>
<td>DroidKungFu</td>
<td>0.97</td>
<td>0.97</td>
<td>0.97</td>
</tr>
<tr>
<td>Opfake</td>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
</tr>
<tr>
<td>Plankton</td>
<td>0.98</td>
<td>0.98</td>
<td>0.98</td>
</tr>
<tr>
<td>BaseBridge</td>
<td>0.95</td>
<td>0.95</td>
<td>0.95</td>
</tr>
<tr>
<td>GinMaster</td>
<td>0.96</td>
<td>0.96</td>
<td>0.96</td>
</tr>
<tr>
<td>Iconosys</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
<tr>
<td>FakeDoc</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
<tr>
<td>Amd</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
<tr>
<td>DroidDream</td>
<td>1.00</td>
<td>1.00</td>
<td>0.98</td>
</tr>
<tr>
<td>Gloadream</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
<tr>
<td>ExploitLinuxLootor</td>
<td>0.95</td>
<td>0.95</td>
<td>0.98</td>
</tr>
<tr>
<td>Jifake</td>
<td>0.94</td>
<td>0.94</td>
<td>0.96</td>
</tr>
<tr>
<td>Boxer</td>
<td>0.80</td>
<td>0.79</td>
<td>0.79</td>
</tr>
<tr>
<td>MobileTx</td>
<td>1.00</td>
<td>1.00</td>
<td>0.99</td>
</tr>
<tr>
<td>Xsider</td>
<td>0.95</td>
<td>0.95</td>
<td>0.98</td>
</tr>
<tr>
<td>Fakelogo</td>
<td>0.98</td>
<td>0.98</td>
<td>0.98</td>
</tr>
<tr>
<td>Dougalek</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>Fatlkr</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>FakelPlayer</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>Fcober</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>Tystpu</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>SerBG</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>Ster</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>Zizko</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>Penemo</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>Nandrobox</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>Geiniml</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>Faketime</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>Copycat</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>Placms</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>TrojanSMS.Hippo</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>Fakengry</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>Cosha</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>SmsZombie</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>DroidSheep</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>Vloader</td>
<td>0.93</td>
<td>0.93</td>
<td>0.93</td>
</tr>
</tbody>
</table>

**TABLE 4**: Raw performance per-family for binary classification problem for the families with at least 10 samples in the DREBIN dataset (Random Forest classifier). Results are ordered by decreasing family size.
to perform aggressive advertisement (Adware) and install unwanted system toolbars.

**MobileTx.** The fifth row of Figure 3 reports the top 5 distinguishing features of MobileTx family, an SMS-fraud malware. Figure 3 shows that three out of the top 5 features involve `sendsms` activity to premium-rate numbers with pre-determined text content — this is captured by dynamic analysis. For example, in the first feature `1065-71090-88877` turns out to correspond to a premium-rate number used to steal money from the victim. (In the whole DREBIN dataset, we have found 68 premium numbers used among several variants). Moreover, all variants of MobileTx require the `RESTART_PACKAGES` permission, that allows the malware to kill other processes on the Android device, and is probably used to kill process monitors and antivirus software possibly installed in the device. The histogram in Figure 3 shows that some other malware families (blue bar) also require this permission for the same purpose, but it is not common. Finally, all 21 variants of MobileTx have the same `author=443` (that is the anonymized integer for the SHA256 signature), and hence this feature also helps identify this family.

**Geinimi.** The Geinimi malware family usually steals information such as fine location, device IDs (e.g., IMEI, IMSI) and the list of installed apps. Its top 5 distinguishing feature value distributions are shown in the last row of Figure 3. The first feature is associated with the registration of `AdServiceReceiver` that is a component used to monitor system events on which to trigger malicious behavior (e.g., to send stolen data to remove server). The crypto operations identified in the top 5 features use the DES algorithm to decrypt URLs of the CnC servers and GET commands which are encrypted to avoid static code analysis, but the malware authors recycled decryption keys and hence we detected them during dynamic analysis. The permission `MOUNT_UNMOUNT_FILESYSTEMS` is used to access data in SD card slots, as some variants of Geinimi use SD cards to store and load repackaged malicious applications download from the CnC servers. The `servicestart GoogleKeyboard` represents the launch of a background process named `GoogleKeyboard` (to avoid user detection by looking at the phone task manager) that performs malicious actions, steals information periodically and sends it to the CnC whose URLs are decrypted at runtime.

As a final remark, we note that for some families, static features are more discriminative (e.g., FakeInstaller and JiFake), whereas some others are better distinguished through dynamic features (e.g., GinMaster and MobileTx). These statistics can be used by security analysts to define new signatures for malware classification as they automatically reveal some internals of the code obfuscation techniques adopted for a certain malware family. For example, the number of permissions requested in the FakeInstaller family (both standard and dangerous) can be used as an indicator, whereas in MobileTx family the `author` and the `sendsms` activities can reveal malicious behavior.
Fig. 3: Feature value comparison between malware families. In particular, we report the histogram of the top-5 feature values for the following malware families (number of samples within parenthesis): FakeInstaller (883), Opfake (607), Geinimi (13), MobileTx (21), GinMaster (304), Jifake (27). Each row corresponds to a family, and the feature value is compared against all other malware families in the dataset.