Dipartimento di Informatica
Università degli Studi di Verona

Rapporto di ricerca **97/2015**
Research report
August 28, 2015

MIME
A Formal Approach for Multiple Investigation in (Android) Malware Emulation Analysis

Fabio Bellini
Roberto Chiodi
Isabella Mastroeni

Dipartimento di Informatica - Università di Verona
(fabio.bellini|roberto.chiodi)@studenti.univr.it
isabella.mastroeni@univr.it

Questo rapporto è disponibile su Web all'indirizzo:
This report is available on the web at the address:
http://www.di.univr.it/report

Abstract

In this paper, we propose a new dynamic and configurable approach to anti-emulation malware analysis, aiming at improving transparency of existing analyses techniques. First of all, we test the effectiveness of existing widespread free analyzers. We observe that the main problem of these analyses is that they provide static and immutable values to the parameter used in anti-emulation tests. Our approach aims at overcoming these limitations by providing an abstract non-interference-based approach modeling the fact that parameters can be modified dynamically, and the corresponding executions compared.

Keywords: Anti-emulation malware, abstract non-interference, program analysis

1 Introduction

The recent technological escalation led to a massive diffusion of electronic devices among non-expert users. Nowadays, almost everybody has at least one smart-phone, a personal computer or a tablet: these devices provide permanent Internet connection to surf the Web, install applications and keep in touch through social networks. A non-expert user installs around one hundred apps, and uses only less than the half of them [4]. One of the most widespread mobile OS is Android, that have reached more than 1 billion device activations in the last year, with an average of 1.5 million activations per day [2]. By the way, there is another side of the coin: most of the people has no idea of how dangerous could be granting wrong permissions to a suspicious application. By installing software coming from untrusted markets, without paying the right attention, a user may cause/introduce lots of vulnerabilities on his system, such as privilege escalation, remote control, financial charge and data leakage [27]. For instance, one in five Android users faces a mobile threat, and the half of them installs trojans designed to steal money [3]. These numbers are growing very fast, and this clearly makes really important to pay attention to the security issue of Android applications, and also to provide specific tools and frameworks for helping users in enforcing their devices security.

The problem. In order to study malware payloads, it is necessary to analyze these malicious software by using specific tools, based on emulation and virtualization, which statically and dynamically analyze the code. The problem is that some malware try to avoid these analyses by exploiting environment detection tricks which allow them to understand whether they are emulated or not. These techniques are called *anti-emulation checks* [12] or *red pills* [22]. If an anti-emulation check detects the presence of a virtual environment, the malware changes its behavior showing only harmless executions, pretending to be another one or simply aborting the computation. In the other case, the malware executes its payload, revealing its real nature and intent. Malware authors use these checks to improve the efficiency and protection of their creations, taking advantage of virtualization discrepancies. Since the original Rutkowska's intuition, many works have been done in this direction. Paleari et al. have proposed a method to automatize the creation of red pills, generating thousands of mnemonic opcodes that trigger different behaviors in real and emulated environments [17]. Futhermore, lots of anti-emulation checks were find out for many different emulation environments like QEMU, Bochs and VMWare [9, 14, 20, 21, 25]. On the other hand, several tools were developed to reduce discrepancies between real and emulated environments, trying to obtain *perfect transparency* [8, 13, 26]. However, in desktop environments, the fight between malware authors and analysts have reached a deadlock: as Garfinkel et al. observed [10], *"building a transpar-*

ent VMM[1] *is fundamentally infeasible, as well as impractical from a performance and engineering standpoint"*. Thus, VMM become defensive tools where anti-emulation malware does not execute their malicious payloads. Hence, the security focus moved to the mobile environment, in particular Android, where virtualization on devices is inefficient and not widespread nowadays. There are currently some Android analyzers available that scan applications trying to extract their main features like permissions, services or used networks. These results can be used to find out malicious behaviors in Android applications by matching the samples with a database of known malware. The problem, again, is that also Android malware started to embed anti-emulation checks, making them resilient to analyses. In fact, in a recent work Vidas and Christin [24] classified the known Android discrepancies in different categories related to behavior, performance, components and system design. Moreover, in [19], the authors show how simple is to bypass analyzers by using trivial anti-emulation checks making most of the analysis frameworks fail their responses, being unable to detect malicious code. Hence, it is clearly necessary to develop new approaches to the fight against the anti-emulation problem, which, first of all, should improve existing analyzers whose limits make them unable to face current malware.

Our approach. Our primary goal is to test the actual efficiency of the main free widespread analyzers and the detection capability of anti-emulation checks embedded in Android apps. We propose an in-depth investigation: we consider 28 samples belonging to 15 different known malware families. These tests have been conducted on 9 analysis frameworks available online, such as Andrubis and VirusTotal. We analyze the obtained results, providing a more specific perspective on the connection between the state-of-the-art of anti-emulation techniques and our samples sources. This work allows us to identify the limitations of the existing analyzers, such as the lack of versatility and customization, usually caused by the general trend to prefer better performance instead of stronger protection.

Another problem we observe, is that there are many solutions proposed, but there is no formal frameworks that would allow us to semantically understand the problem of anti-emulation. A semantic comprehension would be very important for several reasons. Surely, it would allow us to compare different techniques, but, as we will show, it would also allow us to understand how we can tune our analysis in order to adapt it to the different attacking scenarios that a protection tool may have to face. In the existing literature, there is only one attempt to formalize the notion of anti-emulation [12]. This notion formalizes precisely the intuition that anti-emulation is due to an *interference* between the environment and the program execution. The problem with this notion is that it is too strong, since benign applications

[1] Virtual Machine Monitor

may change behaviors depending on the environment. For instance, an application for handling images could change the definition of images depending on the physical features of the device. For this reason, we would like to tune which interferences are suspicious and which are acceptable, i.e., we need to weaken the admissible degree of interference between the environment and the program. In the context of language-based security, the problem of weakening non-interference has been widely studied. In the last years it has been proposed a general formal framework [11] that we can use for both modeling a weakening of what, of the environment, can interfere with the program (so called declassification [15, 23]) and of what is analyzed about the program, namely the output observation of execution. This framework, called *abstract non-interference*, provides a weakening of interference based on abstract interpretation [6, 7]. Namely, both the property that can or cannot interfere with the output observation, and the observed output observation are modeled as abstractions/properties of the concrete semantics/behavior.

Our contribution. In this paper, we propose an approach based on a formal definition of anti-emulation, given in terms of abstract non-interference [11]. In this way, we can capture malicious behaviors related to anti-emulation in a more specific way: by using abstract non-interference we define anti-emulation as an interference between the environment and the observable application output, namely the behavior of the app. We use this definition as a new formal framework where we can better understand how we can make *anti*-anti-emulation checks stronger depending on the platform we work on. This, in particular, allows us to improve existing analysis tools, providing a first overview of an ideal analysis framework called *Multiple Investigation in Malware Emulation* (MIME). The idea is that, by using an analyzer in MIME style, a user could customize the input environment, manually setting lots of parameters – such as IMEI[2] and IMSI[3] – so that he could observe difference in execution based on the chosen parameters. In this way, MIME is able to mimic most of the existing analyzers by combining the input parameters in the desired manner. Our work is based on Android world, because of the great impact of this mobile OS, but it could be easily adapted to other architectures, by parameterizing the related anti-emulation checks.

2 Limitations of Existing Android Malware Analyses

We started the test phase analyzing the anti-emulation checks in Android well-known malware families. In our work, we consider: *BadNews*, *Base-*

[2]International Mobile Equipment Identity.
[3]International Mobile Subscriber Identity.

Bridge, *BgServ*, *DroidDream Light*, *Droid KungFu* – 1, 2, 3, 4, Sapp, Update –, *FakeMart*, *Geinimi*, *Jifake*, *OBad* and *ZSone*. For each malware family, we chose two different variants to verify how frameworks react to small code differences that are not related to malware payload – only in Jifake and Droid KungFu Update this was not possible, because only one version was available. We submitted all these samples to 9 different analyzers, free and available with Web interface: *AndroTotal Andrubis*, *APKScan*, *Dexter*, *ForeSafe*, *Mobile-SandBox*, *VirusImmune*, *VirusTotal* and *VisualThreat*. In our test we submitted samples which were statically and dinamically analyzed or scanned by a pool of antivirus software: all the previous frameworks could cover one or more of these categories. By summarizing, we collected 252 different combinations malware-analyzer that are fully available in [5] for a more in-depth review. We observed that, in order to avoid emulation, most of malware check several environment issues, such as constants in Android Build class and/or other information as IMEI, IMSI and telephone sensors management. Thus, in order to verify the behavior and, consecutively, the presence of red pills in those malware, we mainly need dynamic analysis: this means that the most complete results come from Andrubis, APKScan, ForeSafe and VirusTotal. Nevertheless, we observe that even these frameworks use trivial anti-emulation-related parameters such IMEI, IMSI, etc. In Table 1, we show the results related to the IMEI and the IMSI values in our target frameworks. Most of the considered analyzers han-

Analysis Framework	IMEI Number	IMSI Number
Andrubis	357242043237517	310005123456789
APK Scan	357242043237511	310260000000000
Foresafe	000000000000000	310260000000000
VirusTotal	pseudorandom	pseudorandom

Table 1: Default IMEI and IMSI values of the target frameworks.

dles these information statically, thus really easily checkable by a malware. Only VirusTotal uses a pseudorandom IMEI and IMSI, but this solution is strongly connected to the submitted sample - for instance different VirusTotal executions on the same malware sample have the same IMEI. This can be extended to the majority of the anti-emulation-related parameters checked in other tests, revealing a deep weakness in these tools.

Other kinds of malware anti-emulation checks are provided in the following examples, where other information is tested in order to break the transparency of the virtual environment. In the following listings, some results related to anti-emulation are shown, obtained by manually inspecting the source code of the malware samples. Specifically, the source code in Listing 1 is taken from `Geinimi` sample, where there is an anti-emulation check that tests the execution environment by inspecting the value of the `android_id`, that is set to `null` when the environment is virtual. If `Geinimi` finds a virtual

environment it immediately alerts the Command and Control (C&C) server by sending the string "Emulator" in the `deviceId` field. The souce code in

```
deviceId=android.provider.Settings.System.getString(context1.
    getContentResolver(),"android_id");
if (deviceId == null){
                deviceId = "Emulator";
}
```

Listing 1: `Geinimi` anti-emulation check inspecting the `android_id` value.

Listing 2 is taken from `Obad` sample. In this case, an obfuscation function is applied to the code, but it is quite easy to observe that the `if` statement contains a check concerning the value of the constant `Build.MODEL`. If it contains default values, for example "sdk", all the activities are closed. We can

```
if(Class.forName("android.os.Build").getField("MODEL").get(null).
    equals(OcOCclc.lcclOlO("dDZu"))){
                System.exit(0);
}
```

Listing 2: Malware `Obad` anti-emulation check inspecting the value of `android.os.Build.MODEL`.

observe that, also in these last examples, the anti-emulation checks involve static values (`deviceId` and `android.os.Build.MODEL`) that, in standard analyses cannot be customizable. In other words, most of the actual frameworks do not provide the possibility to customize the configuration of the virtual machine (in the following simply denoted VM) dynamically, making really easy for a malware to detect the virtual environment.
Finally, the analyzers we considered in the test phase, do not allow multiple execution in different virtual environments, but always provide the same configuration for the VM, hence, if different executions in different environments are required, it is necessary to manually upload the samples in several frameworks. Moreover, this leads to discrepancies in the results because each analyzer decides which analysis information has to be considered important, making analyses comparison really difficult and expensive.

All these limitations make the analysis of anti-emulation malware often imprecise (being detected) and/or expensive. In the following, we start from all these considerations in order to provide a stronger approach to anti-emulation problem, for achieving more flexibility and customization in malware analyses.

3 Some preliminaries

Given two sets S and T, we denote with $\wp(S)$ the powerset of S, with $S \smallsetminus T$ the set-difference between S and T, with $S \subseteq T$ inclusion. S^* denotes the set of all finite sequences of elements in S. A set L with ordering relation $\leq$ is a poset and it is denoted as $\langle L, \leq \rangle$. A poset $\langle L, \leq \rangle$ is a lattice if $\forall x.y \in L$ we have that $x \vee y$ and $x \wedge y$ belong to L. A lattice $\langle L, \leq \rangle$ is complete when for every $X \subseteq L$ we have that $\bigvee X, \bigwedge X \in L$. As usual a complete lattice L, with ordering $\leq$, least upper bound (lub) $\vee$, greatest lower bound (glb) $\wedge$, greatest element (top) $\top$, and least element (bottom) $\bot$ is denoted by $\langle L, \leq, \vee, \wedge, \top, \bot \rangle$. Given $f : S \longrightarrow T$ and $g : T \longrightarrow Q$ we denote with $g \circ f : S \longrightarrow Q$ their composition, i.e., $g \circ f = \lambda x.g(f(x))$. $f : L \longrightarrow D$ on complete lattices is *additive* if for any $Y \subseteq L$, $f(\vee_L Y) = \vee_D f(Y)$.

Abstract Interpretation. Abstract interpretation [6,7] is a formal framework used for reasoning on *properties* rather than on (concrete) data values. We use this framework for modeling both the environment property to vary and the malware analyzed property. The idea is that instead of observing the concrete computation of programs, it is possible to observe only *properties* of the computation. In other words, the malware detector operate on abstract, approximate, semantics rather than on concrete, precise, semantics. Abstract interpretation is a general theory for deriving sound approximations of the semantics of discrete dynamic systems, e.g., programming languages [6]. Approximations can be formulated in terms of closure operators [7]. An *upper closure operator* (uco for short) $\rho : C \to C$ on a poset C, representing concrete objects, is monotone (it preserves order precision), idempotent (it adds the whole approximation in one shot), and extensive (it may only add information): $\forall x \in C.\ x \leq_C \rho(x)$. The upper closure operator is the function that maps the concrete values to their abstract properties, namely with the best possible approximation of the concrete value in the abstract domain. For instance the abstraction *Par*, whose fixpoints are $Par = \{\mathbb{Z}, \mathtt{ev}, \mathtt{od}, \varnothing\}$, associates with each set of integer their sign if the integers have all the same sign, top otherwise. Formally, closure operators ρ are uniquely determined by the set of their fix-points $\rho(C)$, for instance $Par = \{\mathbb{Z}, \mathtt{ev}, \mathtt{od}, \varnothing\}$. For upper closures, $X \subseteq C$ is the set of fix-points of $\rho \in uco(C)$ iff X is a *Moore-family* of C, i.e., $X = \mathcal{M}(X) \stackrel{\text{def}}{=} \{\wedge S \mid S \subseteq X\}$ — where $\wedge\varnothing = \top \in \mathcal{M}(X)$. The set of all upper closure operators on C, denoted $uco(C)$, is called *lattice of abstract interpretations of* C [7], and it is a complete lattice when C is a complete lattice.

Abstract Non-interference. Abstract non-interference (ANI) [11,15,16] is a natural weakening of non-interference by abstract interpretation. Suppose the variables of program split in private (`H`) and public (`L`). Let

$\rho, \phi \in uco(\mathbb{V}^{\mathtt{H}} \times \mathbb{V}^{\mathtt{L}})$, where $\mathbb{V}^{\mathtt{L}}$ and $\mathbb{V}^{\mathtt{H}}$ are the domains of `L` and `H` variables. ρ characterizes the *attacker*, while ϕ is the property stating what, of the private data, can flow to the output observation, also called *declassification*. A program P satisfies ANI if $\forall h_1, h_2 \in \mathbb{V}^{\mathtt{H}}, \forall l \in \mathbb{V}^{\mathtt{L}}$:

$$\phi(h_1) = \phi(h_2) \;\Rightarrow\; \rho([\![P]\!](h_1, l)) = \rho([\![P]\!](h_2, l)). \tag{1}$$

This notion says that, whenever the attacker is able to observe the output property ρ, then it can observe nothing more than the property ϕ of the input. This framework allows us to provide several characterizations concerning non-interference, such as the maximal output observer unable to see interferences or the maximal input information disclosed [11, 16].

Observational Semantics and formal definition of anti-emulation. In order to formally model anti-emulation, we have first to characterize what we observe of the program execution. We focus here on Android applications which are written in Java and compiled to *Dalvik* bytecode [1], with the possibility to use a large part of the standard Java library. These features make hard to provide a formal operational semantics to Android applications [18]. To the best of our knowledge there is only one work aiming at providing an operational semantics for Android programs, and in particular still only for Android activities, whose scope is the development of a static analyzer for Android [18]. Since the aim of our work is not to characterize a formal semantics of Android application, but simply to provide a model of anti-emulation, we suppose to fix an observation of the program execution, later called *semantics*, that models what we observe of the application execution. As future work it would be surely interesting to combine this definition of anti-emulation with existing formal semantics in order to provide a more precise characterization.

Let `App` be the set of applications, namely programs `A` running for Android. According to the definition given by Kang et al. [12], we model the behavior of a program `A` as a function depending on the input memory $\sigma \in$ `Mem` and on the environment `E` $\in$ `Env`. An environment provides "all the aspects of the system the program might query or discover, including the other software installed, the characteristics of hardware, or the time of day" [12]. In order to describe the actions performed by a program we consider a set of *Events* $\mathscr{E}$ which describe the relevant actions performed by the application during its execution, for instance instructions related to the Wi-Fi connection, making phone calls or send an SMS to a certain number, or access to particular information stored in the mobile phone. Let $\Sigma = \mathscr{E} \times$ `Mem` be the set of program states then, the observational semantics is:

$$[\![\cdot]\!] : \mathtt{App} \longrightarrow (\mathtt{Env} \times \mathtt{Mem} \rightarrow \wp(\Sigma^*))$$

Given `A` $\in$ `App`, $[\![$`A`$]\!]$ is a function providing the trace of events executed by the program `A` depending on an hosting environment `E` and on an initial in-

put σ, i.e., $[\![\mathtt{A}]\!] : (\mathtt{E}, \sigma) \mapsto \{\ \tau \mid\ \tau = \langle e_0, \sigma\rangle \ldots \langle e_n, \sigma_n\rangle,\ \text{where } e_i \in \mathscr{E} \text{ in } \mathtt{E}\ \}$. So, the operational semantics of an Android application $\mathtt{A} \in \mathit{App}$, written $[\![\mathtt{A}]\!](\mathit{env}, I)$, is all the execution tracks of the execution of the application A in an environment $\mathit{env} \in \mathtt{E}$ with an input I.

To study anti-emulation means, in practice, to discover all the anti-emulation checks that can be exploited in a virtual environment. Let us recall the only formal characterization of anti-emulation [12].
We say that P uses *anti-emulation techniques* if its execution under a real environment $\mathtt{E}_r$ changes its behavior under an emulated environment $\mathtt{E}_e$, although input σ is the same and environments are very similar: $[\![\mathtt{P}]\!](\mathtt{E}_e, \sigma) \neq [\![\mathtt{P}]\!](\mathtt{E}_r, \sigma)$. In this case, $\neq$ denotes the fact that the two executions are "observationally" different.

4 ANI-based definition of Anti-emulation

Malware anti-emulation checks look for specific environment information in order to understand whether the environment is virtual or not. This information is used to *adapt* the execution to the recognized environment, in particular by hiding malicious behaviors when emulation is suspected.
We already underlined that in this field there are many "ad hoc" solutions proposed, but there is no formal frameworks allowing us to semantically understand the problem of anti-emulation. In the existing literature, there is only one attempt to formalize anti-emulation [12] which is based on the notion of non-interference. We show here that this notion is too strong for really capturing the problem, and we propose a model based on *abstract* non-interference (see Sect. 3). Non-interference, in general, is based on the idea that we have some information to protect that has not to interfere with the observable information. In the anti-emulation field, it is clear that the information to protect is the "kind" (virtual or not) of execution environment: when a malware uses anti-emulation techniques there is a flow of information from the "kind" of execution environment to the malware.

The $\mathscr{M}$ sets of events. Our approach, is based on what we observe of the program executions, i.e., on the granularity of the set $\mathscr{E}$. This set is also important for modeling the events, namely the actions, considered suspicious and therefore denoting the possible executions of malicious code. In order to obtain this characterization we have to identify inside $\mathscr{E}$ the set $\mathscr{M}$ of the suspicious/malicious events. The set $\mathscr{M}$ induces a partition of $\mathscr{E}$: $\mathscr{B} \stackrel{\text{def}}{=} \mathscr{E} \setminus \mathscr{M}$ is the set of all the supposed benign events. The set $\mathscr{M}$ can be extracted depending on known information regarding the sample that we want to analyze. For instance, when considering applications handling images could be *malicious* whereas the action of sending an SMS, while this action is perfectly acceptable for instant messaging Apps. Alternatively, we can use

the common payloads investigated by Zhou and Jiang [27]. The content of $\mathscr{M}$ are, for example, all the instructions regarding sending premium rated SMS, data and information leakage from the device and also installation of application without any request.

The *Sel* and *Obs* properties. Defining anti-emulation in terms of abstract non-interference requires the definition of some abstractions. First of all, we have to define an auxiliary map $\alpha_{\mathscr{E}} : \Sigma^* \to \wp(\mathscr{E})$, extracting, from sequences of states, i.e., pairs of events and memories, only the set of generated events. $\mathfrak{O}_{\mathscr{E}} : \wp(\Sigma^*) \to \wp(\mathscr{E})$ is then defined by additive lift. Let $\tau \in \Sigma^*$ and $X \subseteq \Sigma^*$

$$\alpha_{\mathscr{E}}(\tau) = \begin{cases} \varnothing & \text{if } \tau = \varepsilon \\ \{e_1\} \cup \alpha_{\mathscr{E}}(\langle \tau_2 \dots \tau_n \rangle) & \text{if } \tau = \tau_1 \tau_2 \dots \tau_n,\ \tau_1 = \langle e_1, \sigma_1 \rangle \end{cases}$$
$$\mathfrak{O}_{\mathscr{E}}(X) = \bigcup_{\mathbf{e} \in X} \alpha_{\mathscr{E}}(\mathbf{e})$$

At this point, the idea of abstract non-interference is to decide *which variation* is allowed and *how* this variation can be carried in the observable output. This framework allows us to define a extremely flexible model of anti-emulation where we decide the range of environments whose variation should not be observable by the application. In other words, we can model the transparency *degree* of the virtual environment. It is clear that, in order to capture anti-emulation, in this range we need to have both real and virtual environment. From the formal point of view, we have to decide how we model environment variations. At the same time, we can decide which part of the input has, instead, to stay unchanged among all the analyzed executions. In general, since we aim at observing precisely how the environment affects the execution, we should have to leave unchanged all the other inputs affecting computation.
We use these observations for defining the input abstraction $Sel_{\mathbb{E}}$, which precisely model the only possibility of varying the environment inside the set $\mathbb{E}$: Let $\mathbb{E} \subseteq \texttt{Env}$ modeling the admitted range of variation for environments, and $\sigma \in \texttt{Mem}$ an input for the application `A`:

$$Sel_{\mathbb{E}} : \texttt{Env} \times \texttt{Mem} \longrightarrow \wp(\texttt{Env} \times \texttt{Mem}) \qquad Sel_{\mathbb{E}}(\langle \texttt{E}, \sigma \rangle) = \begin{cases} \langle \mathbb{E}, \sigma \rangle & \text{if } \texttt{E} \in \mathbb{E} \\ \langle \texttt{E}, \sigma \rangle & \text{otherwise} \end{cases}$$

Hence, we say that $(\texttt{E}_1, \sigma_1)$ and $(\texttt{E}_2, \sigma_2)$ are equal under the property $Sel_{\mathbb{E}}$ – and we write $Sel_{\mathbb{E}}(\texttt{E}_1, \sigma_1) = Sel_{\mathbb{E}}(\texttt{E}_2, \sigma_2)$ – if $\texttt{E}_1, \texttt{E}_2 \in \mathbb{E}$ are two environment and $\sigma_1 = \sigma_2$. We abuse notation by denoting with $Sel_{\mathbb{E}}$ also its additive lift to sets, and therefore the corresponding closure operator. It is clear that, in order to detect anti-emulation, $\mathbb{E}$ should include both virtual and real environments.

In the abstract non-interference framework, we can also tune what we want to observe in output, namely which observable property has or has not

to be sensitive to the input variation. In the anti-emulation context, we simply aim at observing whether the application shows only benign behaviors or even malicious ones, depending on the variation of the input environment, hence we define $Obs_{\mathscr{M}}$ as an abstraction providing a simple boolean response: Let $X \subseteq \mathscr{E}$

$$Obs_{\mathscr{M}} : \wp(\mathscr{E}) \longrightarrow \{\texttt{True}, \texttt{False}\}$$
$$Obs_{\mathscr{M}}(X) = \begin{cases} \texttt{True} & \text{if } X \cap \mathscr{M} \neq \emptyset \\ \texttt{False} & \text{otherwise} \end{cases}$$

This definition of $Obs_{\mathscr{M}}$ is functional to the purpose of observing the presence of benign executions and executions containing malicious events.

The Model. Starting from the notion of abstract non-interference [11,15] we create a model for anti-emulation. The core of the definition is the flow of information between the execution environment and the application behavior. Namely, if the application execution shows malicious events only in some environment, we say that some anti-emulation mechanism are present. Our definition strongly depends on the set $\mathscr{M}$. Thus, fixed the set $\mathscr{M}$ and given the abstractions *Sel* and $Obs_{\mathscr{M}}$ defined above, an application $\texttt{A}$ does not use *anti-emulation* with respect to $\mathbb{E}$ and $\mathscr{M}$ if:

$$\forall \langle \texttt{E}_1, \sigma_1 \rangle, \langle \texttt{E}_2, \sigma_2 \rangle \in \texttt{Env} \times \texttt{Mem}.\ Sel_{\mathbb{E}}(\langle \texttt{E}_1, \sigma_1 \rangle) = Sel_{\mathbb{E}}(\langle \texttt{E}_2, \sigma_2 \rangle) \Rightarrow \\ Obs_{\mathscr{M}}(\mathfrak{O}_{\mathscr{E}}([\![\texttt{A}]\!](\langle \texttt{E}_1, \sigma_1 \rangle))) = Obs_{\mathscr{M}}(\mathfrak{O}_{\mathscr{E}}([\![\texttt{A}]\!](\langle \texttt{E}_2, \sigma_2 \rangle))) \tag{2}$$

In other words, the malware does not contain any anti-emulation check, with respect to the environment range $\mathbb{E}$ and the malicious actions set $\mathscr{M}$, if by varying the environment inside $\mathbb{E}$ we observe only malicious actions (the malware does not contain anti-emulation checks) or only benign actions (the model does not capture the correct anti-emulation checks of the malware analyzed).

Observations. The formal model of anti-emulation we provide is strongly dependent on the characterization of the sets $\mathbb{E}$ and $\mathscr{M}$. This means that, the accuracy of the model depends on the understanding and on the knowledge we have of the application context. In particular, the way we approximate the set $\mathscr{M}$ affects the presence of both false positives and negatives in the quest of anti-emulation checks. If we under-approximate $\mathscr{M}$ we clearly introduce false negatives, namely there may be anti-emulation malware that are not recognized. On the other hand, if we over-approximate $\mathscr{M}$, then we introduce false positives since we can detect nonexistent anti-emulation checks.
Another interesting observation concerns the definition of $Obs_{\mathscr{M}}$. In fact, we can refine the observation of the environment interference on the observable behavior. For instance, if we consider a further partition of benign

events, i.e., $\mathscr{B} = \mathscr{B}_1 \cup \mathscr{B}_2 \cup \ldots \cup \mathscr{B}_n$, we can, not only detect the presence of anti-emulation checks as before, but we can also understand whether the environment affects the "kind" (in terms of the provided partition) of events (potentially benign) showed by the application. In this case, we could define a function $Obs_{\mathscr{B}}$ as follows: Let $\mathtt{B}_i$ the name given to the partition $\mathscr{B}_i$, for each i between 1 and n, and let $X \subseteq \mathscr{E}$

$$Obs_{\mathscr{B}} : \wp(\mathscr{E}) \longrightarrow \{\mathtt{True}\} \cup \left\{ \mathtt{B}_i \;\middle|\; i \in [1,n] \right\}$$
$$Obs_{\mathscr{B}}(X) = \begin{cases} \mathtt{True} & \text{if } X \cap \mathscr{M} \neq \emptyset \\ \mathtt{B}_i & \text{if } X \subseteq \mathscr{B}_i \end{cases}$$

5 Multiple Investigation in Malware Emulation (MIME)

An empiric approach in anti-emulation investigation is surely slow and time-consuming: It is necessary to upload the same sample different times for each analyzer to use – in our case at least four times for consulting dynamic information. An easier and faster way could be the usage of a single analyzer, but most of the time it is necessary to do multiple and parallel analyses. So, there is no doubt that a single and customizable analyzer could be a better solution.

5.1 The MIME strategy

The approach we propose is an analyzer architecture based in a configurable VM. In this work, we propose a new approach called MIME – Multiple Investigation in Malware Emulation. We already observed that, existing analyses use an environment setting which is static and immutable, in the sense that they cannot be configurated depending on the application contexts, for instance depending on the kind of malware we are analyzing. Moreover, from our empirical studies we observed that the standard anti-emulation checks are based on simple checks of specific parameters values, such as IMEI or IMSI. Hence the problem of existing analyses is that these parameters are set to fixed, and often trivial, values. This means that a truly transparent analyzer should be able to provide the value that the malware expects from a real environment. Unfortunately, it is quite unrealistic to find a value robust to sets of different malware, and not simply to a specific one. The idea we propose is precisely to consider the ANI definition of anti-emulation, where we look for anti-emulation checks by analyzing malware several times, and each time under different environment settings. In other words, we let the input environment to vary, by setting a list of anti-emulation parameters (such as IMEI, IMSI, ...), and we observe how the execution is affected. At this point, our goal is the automation of this formal model by making systematic the variation of the environment setting and automatic the corresponding executions and comparisons. The main idea of MIME is to

perform several executions depending a configurable environment, which is systematically modified until we find an anti-emulation check (detected by an evaluation function) or until we exhaustively explore the space of environments we consider.
In Figure 1, we show this idea where the input is the malware `M` and the machine state `mem`. The analyzer contains a module `Environment setting` which generates all the different configurations for exploring the space of environments to check. Each single execution of the malware inside the analyzer provides in output an observed behavior. This behavior is then evaluated for detecting the presence of anti-emulation checks.

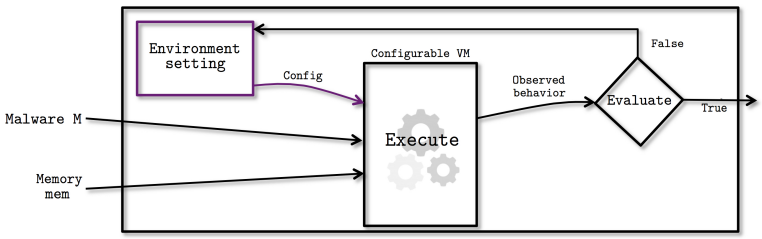


Figure 1: Simple architecture of a MIME customizable analyzer.

Configuring MIME architectures. Let us deeper explain the idea of systematic and automated environment setting. We propose to choose a pool of n anti-emulation-connected input parameters. We associate with each parameter a list of prearranged values, in order to automatize the environment setting. It is worth noting, that both the set of parameters and the corresponding values can be easily customized. In the MIME strategy, we represent these parameters like *rotors*, and each value corresponds to a rotor position: by changing only one position at a time, we can detect which are the malware reactions. In particular, the idea is to explore the space of combinations starting from the simpler tests and moving toward the more sophisticated ones, i.e., higher position in rotors corresponds to more *transparent* parameter values.
In Table 2 we show an example of rotor pool for MIME approach and, in particular, in Table 3 it is shown an example of values of the IMEI rotor.

In general, let $\mathtt{p}_i$ the i-th parameter, let $\mathtt{R}_i$ be the rotor for $\mathtt{p}_i$, and let $\mathtt{V}_i$ be the set of values for $\mathtt{p}_i$. This idea, in our formal model corresponds to consider a set $\mathbb{E}_i$ for each parameter $\mathtt{p}_i$, which simply corresponds to the execution environment where the parameter p_i is set to one of the values in $\mathtt{V}_i$, while all the other parameters are set to a default initial value. This choice is necessary since we aim at understanding precisely whether the parameter p_i, and not others, may affect execution. In this case, we consider Eq. 2, with input abstraction $Sel_{\mathbb{E}_i}$. Namely, the MIME strategy proposes

Rotors	Description
IMEI	list of statical and pseudorandom IMEIs
IMSI	list of statical and pseudorandom IMSIs
device model	list of real and virtual device models
device version	list of real and virtual device versions
SIM serial	list of statical and pseudorandom SIM serials
calls	the occurrence or absence of dialed/recived calls
SMS	the occurrence or absence of sent/recived text messages
contacts	the occurrence or absence of a contact list
battery level	list of battery level in [0, 100]
DNS	list of real and virtual DNS values
sensor mgmt	the occurrence or absence of a proper sensor management

Table 2: An example of MIME approach rotors.

Rotor position	IMEI Number	Description
p_0	000000000000000	Foresafe or standard VM IMEI
p_1	357242043237511	Apk Scan IMEI
p_2	357242043237517	Andrubis IMEI
p_3	357242043237515	IMEI similar to Android analysis framework
p_4	pseudorandom1	IMEI generated with specific random generators
p_5	pseudorandom2	IMEI generated with specific random generators
p_6	pseudorandom3	IMEI generated with specific random generators
p_7	pseudorandom4	IMEI generated with specific random generators

Table 3: Example of a rotor related to device IMEI value.

to verify n times the Eq. 2, each time with respect one parameter $\mathtt{p}_i$, i.e., with respect to $\mathbb{E}_i$.

Evaluating the observed behavior. In order to understand whether we detect an anti-emulation check or not we need an evaluating process. In particular, the evaluation function returns a boolean value identifying the presence of at least one malicious action in $\mathscr{M}$. This evaluation function is used for detecting anti-emulation simply by comparing different executions, namely if the malware, in one or more environments, executes some malicious events, while in other environments its execution is harmless, we label this difference as related to an anti-emulation check. Formally, the evaluation corresponds to the function $Obs_{\mathcal{M}} \circ \mathfrak{O}_{\mathscr{E}}$ which extracts from execution traces the set of executed observable events, and it checks whether this set contains some malicious events from $\mathscr{M}$.

5.2 Using MIME for analyzing anti-emulation malware

In this section, we explain how we use the MIME strategy for improving the transparency of existing analyses. It is clear that the price to pay is in the performance of the analysis, but the interesting aspect of this strategy is that each result we collect can be used to improve our knowledge of existing anti-emulation techniques. In particular, the high flexibility of this

approach allows us to easily implement any additional information we could have on the malware to analyze. For instance, if we precisely know the kind of anti-emulation test performed by the malware then we act only on the rotors values concerning these tests, being completely useless to change other values. Hence, the approach can be completely adapted to the particular knowledge we have on the malware to analyze. It is clear, though, that otherwise we have to check all the possibilities.

Let us explain the MIME strategy proposed in Listing 3 and in Listing 4. Let `Rotors` be the matrix of all rotors, each rotor i has a number of possible different values $\texttt{max}_i$, for instance in Table 3 the IMEI rotor $\texttt{R}_1$ has $\texttt{max}_1 = 7$, having 7 different possible values. Suppose to have $n+1$ rotors, then we define `max` as maximal value in $\left\{ \texttt{max}_i \;\middle|\; i \in [0, n] \right\}$. Let `M` be the analyzed malware, and `mem` the machine state memory. `Config` is the array containing the $n+1$ positions of the rotors used for setting the environment. `Execute` corresponds to the observation of the malware execution, formally it corresponds to the observed semantics $[\![\cdot]\!]$ where `Config` corresponds precisely to its environment input. `Evaluate` corresponds to the evaluation function that, as we noticed before, is modeled by the output abstraction $Obs_{\mathcal{M}} \circ \mathfrak{D}_{\mathscr{E}}$. Finally, `position_anti_emu` is the array of the rotor positions where an anti-emulation check is detected by the evaluation.
Listing 3 implements the idea that we first compute the default configuration of rotor parameters, whose evaluation `val_0` is `true` if a malicious action in $\mathscr{M}$ is observed. This corresponds to the worst possible VM for detecting anti-emulation malware. Then we execute the malware in the smarter configuration possible in our model, where the rotors are set to the maximal values, and we evaluate in `val_m` whether the corresponding execution exhibits malicious events. If the two values are different it means that somewhere in the code, there is an anti-emulation check, and therefore we launch the function `Catching_anti_emu` looking for the identification of the anti-emulation checks. If the two values are both equal to `true` then it means that the malware does not use anti-emulation checks. Finally, if the values are both equal to `false`, and we knew that it was a malware, it means that it uses an anti-emulation check based on different parameters or it uses a conjunctive combination of tests on the known parameters. We lose this situation since we check parameters one at time. However, to the best of our knowledge, based on the experimental results, this last situation is not used by anti-emulation checks.

Listing 4 shows the pseudo-code of the function `Catching_anti_emu`. In this case, we have to vary the environment setting looking for the parameters responsible of the anti-emulation check. Since we aim at observing the interference of each single parameter on the malware behavior, we let only one rotor at time to change value, while all the others are set to default initial values. For this reason, each time we finish to analyze the interference of one rotor, we reset it before changing rotor. We always check all the rotors

```
Function: Mime
Input: M, Rotors[n+1][max],mem
result = null;
for each k in [0,n] Config[k]=0; //Environment reset (rotors initial
    pos)
trace = Execute(M,Config,mem);
val_0=Evaluate(trace);
for each k in [0,n] Config[k]=max_k; //Environment setting to max
    rotors pos
trace = Execute(M,Config,mem);
val_m = Evaluate(trace);
if (val_0 != val_m) result = to_string(Catching_anti_emu(M, Rotors,mem
    ));
if (val_0 == val_m)
        if (val_0) result = malware; // M is a malware without anti-
            emulation
        else result = pot_not_malware; //M is not recognized as
            malware
Output: result
```

Listing 3: MIME approach in anti-emulation malware recognition.

since there may be more than one anti-emulation check. `val` becomes `true` if some malicious action is detected, at this point since we know that there was also an harmless execution (the routine is called only in this case), it means that the current rotor contains an anti-emulation check in the current position, that we store in `position_anti_emu`. At the end of the execution, this vector contains all the rotor positions, namely the parameters values, used in anti-emulation checks. If at the end this vector is all `null`, then it means that the anti-emulation checks involve unobserved parameters or are based on different techniques.

```
Function: Catching_anti_emu
Input: M, Rotors[n+1][max],mem
position_anti_emu[n] = null;
for each i in [0,n] {
        for each k in [0,n] Config[k]=0; //Environment reset
        for each j in [0, max_i-1]{
                Config[j]=Rotors[i,j];
                trace = Execute(M,Config,mem);
                val = Evaluate (trace);
                if (val) position_anti_emu[i] = j; break;
                else     j = j+1;
        }
        i = i+1; //change rotor
}
Output: position_anti_emu
```

Listing 4: Catching anti-emulation checks in MIME.

An example: The analysis of `Obad`. Let us consider the trojan malware for Android `Backdoor.AndroidOS.Obad` – also known as `Obad`. It is

able to send SMS to premium-rate numbers or downloading other malware. It uses several techniques in order to thwart analyses, like code obfuscation and anti-emulation. Our analyses conducted by Andrubis, APKScan, VirusTotal and ForeSafe have collected no malicious events: they have just highlighted lots of permissions required in `manifest.xml`, but not used in practice [5]. `Obad` checks anti-emulation by investigating on the constant `android.os.Build.MODEL`, and it closes all the running activities if a known emulation-related value is recognized. By using MIME approach, `Obad` will be forced to show its malicious behavior, even if it is executed in a virtual environment. In order to analyze the payload of `Obad`, we should work with the *device model rotor* (see Table 2), until we find the right device model value that nullifies the `Obad` anti-emulation trick.
For example, the execution of `Obad`, with the VM *device model* configured as "sdk", does not show any malicious action, but if we set the *device model* as a real mobile Android device, surely malicious actions are produced, such as a premium-rate SMS sent.

This strategy works fine when the analyst already knows something about the malware to study. In a scenario where `Obad` is a brand new malware and we want to use MIME strategy to understand what anti-emulation check it implements, we have to work with all the rotors. For this malware, the manipulation of parameters such as IMEI, IMSI or SMS will simply not produce any malicious behavior, while only the *device model* rotor produces some differences in execution, related to the structure of the constant `Build.MODEL`. In Table 4 we show a potential (partial) response of the execution of `Mime` on the malware `Obad`.

Rotors	`Obad` Execution Results	Position
IMEI rotor	No malicious behavior found.	
IMSI rotor	No malicious behavior found.	
device model rotor	Malicious behavior found: SMS sent.	5
device version rotor	No malicious behavior found.	
...	...	

Table 4: An example of MIME examination of `Obad`.

6 Future Works

We develop our approach in the Android word since no much works have been done heretofore in this field. However, our approach to anti-emulation can be easly generalized to any platform. In this case, it is necessary to change the `Evironment setting` and the VM, in order to let it analyze desktop malware. Obviously, different rotors must be configured with parameters that are related to anti-emulation in desktop environments. Until now, no implementation of our approach has been made, so a possible

future implementation of MIME will be useful to successfully analyze anti-emulation malware. Finally, our ANI model of anti-emulation is strongly related to the definition of the $\mathscr{M}$ set of the malicious events. We would like to improve this model and study in depth the relation between the $\mathscr{M}$ set and the anti-emulation checks detection in malware.
+++Fuzzing, scalability, false positives

References

[1] Dalvik docs mirror. http://www.milk.com/kodebase/dalvik-docs-mirror/.

[2] Google inc. http://google.com.

[3] Kaspersky labs. https://securelist.com.

[4] Yahoo labs. http://labs.yahoo.com.

[5] F. Bellini, R. Chiodi, and I. Mastroeni. Mime: A formal approach for multiple investigation in (android) malware emulation analysis. Technical Report RR ??/2015, 2015. `http://+++`.

[6] P. Cousot and R. Cousot. Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Conference Record of the 4th ACM Symposium on Principles of Programming Languages* (*POPL '77*), pages 238–252. ACM Press, 1977.

[7] P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Conference Record of the 6th ACM Symposium on Principles of Programming Languages* (*POPL '79*), pages 269–282. ACM Press, 1979.

[8] Artem Dinaburg, Paul Royal, Monirul Sharif, and Wenke Lee. Ether: Malware analysis via hardware virtualization extensions. In *Proceedings of the 15th ACM Conference on Computer and Communications Security*, CCS '08, pages 51–62, New York, NY, USA, 2008. ACM.

[9] Peter Ferrie. Attacks on virtual machine emulators. In *Technical Report*. Symantec Corporation, 2007.

[10] Tal Garfinkel, Keith Adams, Andrew Warfield, and Jason Franklin. Compatibility is not transparency: Vmm detection myths and realities. In *Proceedings of the 11th USENIX Workshop on Hot Topics in Operating Systems*, HOTOS'07, pages 6:1–6:6, Berkeley, CA, USA, 2007. USENIX Association.

[11] R. Giacobazzi and I. Mastroeni. Abstract non-interference: Parameterizing non-interference by abstract interpretation. In *Proc. of the 31st Annual ACM SIGPLAN-SIGACT Symp. on Principles of Programming Languages (POPL '04)*, pages 186–197. ACM-Press, 2004.

[12] Min Gyung Kang, Heng Yin, Steve Hanna, Stephen McCamant, and Dawn Song. Emulating emulation-resistant malware. In *Proceedings of the 1st ACM Workshop on Virtual Machine Security*, VMSec '09, pages 11–22, New York, NY, USA, 2009. ACM.

[13] Martina Lindorfer, Clemens Kolbitsch, and Paolo Milani Comparetti. Detecting environment-sensitive malware. In *Proceedings of the 14th International Conference on Recent Advances in Intrusion Detection*, RAID'11, pages 338–357, Berlin, Heidelberg, 2011. Springer-Verlag.

[14] Tom Liston and Ed Skoudis. On the cutting edge: Thwarting virtual machine detection, 2006.

[15] I. Mastroeni. On the rôle of abstract non-interference in language-based security. In K. Yi, editor, *Third Asian Symp. on Programming Languages and Systems (APLAS '05)*, volume 3780 of *Lecture Notes in Computer Science*, pages 418–433. Springer-Verlag, 2005.

[16] I. Mastroeni. Abstract interpretation-based approaches to security - A survey on abstract non-interference and its challenging applications. In *Semantics, Abstract Interpretation, and Reasoning about Programs: Essays Dedicated to David A. Schmidt on the Occasion of his Sixtieth Birthday, Manhattan, Kansas, USA, 19-20th September 2013.*, pages 41–65, 2013.

[17] Roberto Paleari, Lorenzo Martignoni, Giampaolo Fresi Roglia, and Danilo Bruschi. A fistful of red-pills: How to automatically generate procedures to detect cpu emulators. In *Proceedings of the 3rd USENIX Conference on Offensive Technologies*, WOOT'09, pages 2–2, Berkeley, CA, USA, 2009. USENIX Association.

[18] E. Payet and F. Spoto. An operational semantics for android activities. In *Proc. of the ACM SIGPLAN Symp. on Partial Evaluation and Semantics-Based Program Manipulation (PEPM'14)*, pages 121 – 132. ACM Press, 2014.

[19] Thanasis Petsas, Giannis Voyatzis, Elias Athanasopoulos, Michalis Polychronakis, and Sotiris Ioannidis. Rage against the virtual machine: Hindering dynamic analysis of android malware. In *Proceedings of the Seventh European Workshop on System Security*, EuroSec '14, pages 5:1–5:6, New York, NY, USA, 2014. ACM.

[20] Danny Quist, Val Smith, and Offensive Computing. Detecting the presence of virtual machines using the local data table. *Offensive Computing*, 2006.

[21] Thomas Raffetseder, Christopher Kruegel, and Engin Kirda. Detecting system emulators. In *Proceedings of the 10th International Conference on Information Security*, ISC'07, pages 1–18, Berlin, Heidelberg, 2007. Springer-Verlag.

[22] Joanna Rutkowska. Red pill... or how to detect vmm using (almost) one cpu instruction, 2004.

[23] A. Sabelfeld and D. Sands. Declassification: Dimensions and principles. *J. of Computer Security*, 2007.

[24] Timothy Vidas and Nicolas Christin. Evading android runtime analysis via sandbox detection. In *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, ASIA CCS '14, pages 447–458, New York, NY, USA, 2014. ACM.

[25] Kalpa Vishnani, Alwyn R Pais, and Radhesh Mohandas. Detecting & defeating split personality malware. In *SECURWARE 2011, The Fifth International Conference on Emerging Security Information, Systems and Technologies*, pages 7–13, 2011.

[26] Lok-Kwong Yan, Manjukumar Jayachandra, Mu Zhang, and Heng Yin. V2e: Combining hardware virtualization and softwareemulation for transparent and extensible malware analysis. *SIGPLAN Not.*, 47(7):227–238, March 2012.

[27] Yajin Zhou and Xuxian Jiang. Dissecting android malware: Characterization and evolution. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, SP '12, pages 95–109, Washington, DC, USA, 2012. IEEE Computer Society.

Appendix: Test results

In this appendix we present our Summary Tables, which collect all the useful information related to 252 different analyses on 28 malware samples.

In order to discover if anti-emulation techniques are common also in Android malware, we investigate 15 different malware families: *BadNews*, *BaseBridge*, *BgServ*, *DroidDream Light*, *Droid KungFu* 1, 2, 3, 4, Sapp, Update , *FakeMart*, *Geinimi*, *Jifake*, *OBad* and *ZSone*.

We examined, where it was possible, 2 samples for each family, in order to compare the results considering how analyzers react to different samples of the same family. The analyzers we used are: *AndroTotal*, *Andrubis*, *APKScan*, *Dexter*, *ForeSafe*, *Mobile-SandBox*, *VirusImmune*, *VirusTotal* and *VisualThreat*.

Since no unified overview of the analysis was possible, we manually selected all the useful information that came from analyses. In particular, we selected anti-emulation related data, and we catalogue them in five sections, as follows:

- General Information;
- Antivirus Scan and Name Distribution;
- Used Elements Analysis;
- Network Analysis;
- Potentially Dangerous Operations.

There follows a brief description of each section, focusing on the information reported.

General Information This section contains the features of the .apk sample file, like its MD5 code and its dimension.

Antivirus Scan and Name Distribution This is the summary of 89 antivirus scans. In order to give a quick overview of the difference between the two versions of each sample, we assigned a particular color depending on the accuracy of the antivirus response. Table 5 shows the color legend adopted.

In order to make more immediate the consultation of this Summary Tables, we also decided to take account of the name distribution: we assigned to each scan a score, depending on the accuracy of the antivirus classification. Table 6 shows the score legend adopted.

Color	Symbol	Meaning
ruby red		A malware was detected.
ruby red	*	A malware was detected in both of samples, but the names are different.
bold italic red	#	A malware was detected in the sample B, but no malware was detected in the sample A.
red		In the sample B the malware was detected in a more specific way than in the sample A.
light green	^	In the sample B the malware was detected in a less specific way than in the sample A.
bold italic green	$	A malware was detected in the sample A, but no malware was detected in the sample B.

Table 5: Color legend adopted in the Summary Tables.

Score	Meaning
-1	No malware was detected.
0	The name assigned to the malware is completely wrong.
1	The name assigned to the malware is generic without any specification about its family.
2	The name assigned to the malware is partially correct because it regards a family linked to the sample one.
3	The name assigned to the malware is correct (or an alias).

Table 6: Color legend adopted in the Summary Tables.

Used Elements Analysis In this section we present an overview of static and dynamic information related to the sample source. In this section the information represented concerns permissions declared and used, activities and intents.

Network Analysis This is the most important section from an anti-emulation standpoint. In this section are represented all the interaction of the malware with the network: in particular we collect messages, HTTP/DNS requests and network connections.

Potentially Dangerous Operations This is a review of VisualThreat analysis, where we decided to show also some dynamic information. For each potentially dangerous operation, we also show how many time this operation was executed.

BadNews A

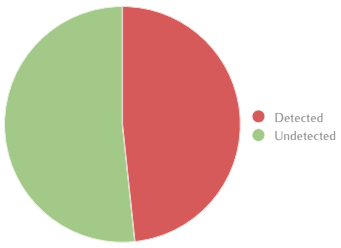
MD5	98cfa989d78eb85b86c497ae5ce8ca19
SHA-1	8d0cc1dab447130ab99528be89681f2f35d0294e
SHA-256	89a8c758f45d86bf0aee1496fd48036fad55805927327d89af6ec1d7337a3938
API Level	10
File Dimension (MB)	3.20
Package Name	live.photo.savanna
Other Names	livehotosvnn 89a8c758f45d86bf0aee1496fd48036fad55805927327d89af6ec1d7337a3938
Used Features	android.software.live_wallpaper android.hardware.wifi android.hardware.touchscreen

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.InfoStealer.BB
Adobe Malware Classifier	
Aegislab	BadNews
Agnitum	
AhnLab-V3	Android-Malicious/BadNews
ALYac	
Anchivia	
Antiy-AVL	
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Android:BadNew-Z [PUP]
AVG	Android/Generic.AP
Avira	Android/BadNews.A, Android/BadNews.A.Gen
AVware	Trojan.AndroidOS.Androways.a
Baidu	
BitDefender	Android.Trojan.InfoStealer.BB
Bkav	
ByteHero	
ClamAV	Andr.Trojan.Badnews
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.98CFA989!Olympus, AndroidOS/BadNews.A.gen!Eldorado
Digital Patrol	
DrWeb	Android.Androways.1.origin
EmsiSoft	Android.Trojan.InfoStealer.BB (B)
Epoolsoft	
eScan	Android.Trojan.InfoStealer.BB
F-Mirc	
F-Prot	
F-Secure	Trojan:Android/Badnews.gen!65232C
FileMedic	
FilsecLab Twister	Android.BadNew.A.towm
Fortinet	Android/BadNews.A!tr.dldr
GData	Android.Trojan.InfoStealer.BB
GFI Vipre	Trojan.AndroidOS.Androways.a
Ikarus	AndroidOS.BadNews.A
Immunos	Andr.Trojan.Badnews
Jiangmin	
K7 Antivirus	Trojan (0001140e1)
K7GW Antivirus	Trojan (0001140e1)
Kaspersky	not-a-virus:HEUR:AdWare.AndroidOS.Anways.a
Kingsoft	Android.Troj.Fakeinst.sc.(kcloud)
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!98CFA989D78E
McAfee GW	
Microsoft	
NANO AntiVirus	Trojan.Android.Anways.cwyczq
NOD32	Android/BadNew.A
NoraLabs NoraScan	
Norman	
Norton Symantec	Trojan.Gen.2
nProtect	
OfficeMalScanner	

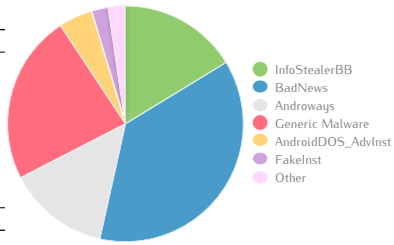
Antivirus	Result
Panda	
PathFinder	Malware
Preventon	Andr/BadNews-A
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Trojan.InfoStealer.BB
Segurmatica	
Segurmatica KE	not-a-virus:HEUR:AdWare.AndroidOS.Anways.a
Solo	
Sophos	Andr/BadNews-A
SUPERAntiSpyware	
Team Cymru	Malware
The Cleaner	
The Hacker	
TotalDefense	
TotalDefense Cloud	
Tencent	Trojan.Android.Agent.CF077D29
Trend Micro	ANDROIDOS_ADVINST.A, ANDROID.EC9F40F0
Trend Micro-Housecall	ANDROIDOS_ADVINST.A
TrustPort	
TT Livescan	
VBA32	
Vexira	
VirIT eXplorer	Android.Trj.BadNews.A
VIRobot	Android.Trojan.InfoStealer.BB[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.BadNews.A

Detected	43
Undetected	46
Sum	89



Name Distribution

Name	Amount	Score
InfoStealerBB	7	0
BadNews	16	3
Androways	6	2
Generic Malware	10	1
AndroidDOS_AdvInst	2	0
FakeInst	1	0
Other	1	1
Sum	43	



Average Score	0,28

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.ACCESS_WIFI_STATE	Allows applications to access information about WI-FI networks
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting
android.permission.SYSTEM_ALERT_WINDOW	Allows an application to open windows using the type TYPE_SYSTEM_ALERT, shown on top of all other applications
android.permission.VIBRATE	Allows access to the vibrator
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage
com.android.launcher.permission.INSTALL_SHORTCUT	Allows an application to install a shortcut in Launcher

Used Permissions	Description	API calls
android.permission.ACCESS_FINE_LOCATION °	Allows an app to access precise location from location sources such as GPS, cell towers, and WI-FI	android/location/LocationManager;-> getBestProvider
android.permission.ACCESS_NETWORK_STATE		android/net/ConnectivityManager;-> getActiveNetworkInfo
android.permission.INTERNET		java/net/DatagramSocket
android.permission.READ_CONTACTS °	Allows an application to read the user's contacts data	android/content/ContentResolver;->query
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;-> getDeviceId
android.permission.VIBRATE		android/os/Vibrator;->vibrate
android.permission.WAKE_LOCK °	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming	android/media/MediaPlayer;->start

Used Intents
android.intent.action.BOOT_COMPLETED
android.intent.action.PHONE_STATE

Activities	Used	Provided by Android	Provided by Third-Parties
com.android.system.AppDownloaderActivity	✔		

Services	Used	Provided by Android	Provided by Third-Parties
com.androways.advsystem.AdvService	✔	✔	✔
com.android.vending.util.WorkService	✔	✔	
live.photo.savanna.MainActivity	✔	✔	✔

Receivers	Used	Provided by Android	Provided by Third-Parties
com.androways.advsystem.AReceiver	✔	✔	✘
com.androways.advsystem.BootReceiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
-			

Used Networks
-

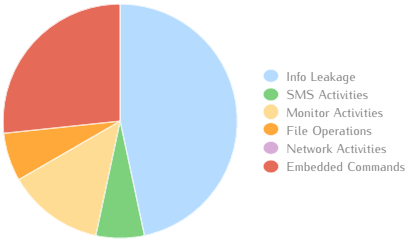
Native Libraries Loaded
/data/data/live.photo.savanna/lib/libandengine.so 0x40516618

Network Analysis

Hardcoded URLs	IP	Region
schemas.android.com	-	-
http://androways.com (malevolo)	91.226.212.65	Ukraine

Potentially Dangerous Operations

	Name	Description
Info Leakage	Call_Query	List phone call records
	Contact_Query	List contacts
	GPS_Get	Retrieve GPS information
	Location_Last_Get	Retrieve last phone location
	Phone_IMEI_Get	Retrieve IMEI
	Phone_Number_Get	Retrieve current phone number
	SMS_Query	List SMS
SMS Activities	Notification_Send	Send notifications
Monitor Activities	GPS_Spy	Spy GPS states
	Location_Spy	Spy location
File Operations	File_Erase	Delete file
Network Activities	-	
Embedded Commands	unix-compress	Compress file
	unix-diff	Display line-by-line differences between pairs of text files
	unix-mkdir	Make a directory
	unix-sleep	Suspend execution for a specified interval



Info Leakage	7
SMS Activities	1
Monitor Activities	2
File Operations	1
Network Activities	0
Embedded Commands	4

BadNews B

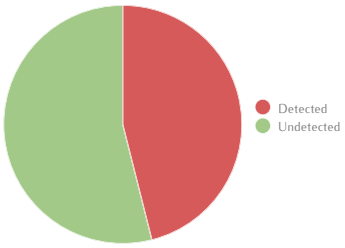
MD5	5b08c96794ad5f95f9b42989f5e767b5
SHA-1	f1b351d1280422c5d1e3d2b1b04cb96a5d195f62
SHA-256	3ed1e8ea99365c17127726a6bababdf5a77610b3a5b138f5c9e0b637bfc3879f
API Level	0
File Dimension (MB)	3.93
Package Name	ru.blogspot.playsib.savageknife
Other Names	rublogsotlysibsvgenife.apk 3ed1e8ea99365c17127726a6bababdf5a77610b3a5b138f5c9e0b637bfc3879f
Used Features	android.hardware.wifi android.hardware.touchscreen android.hardware.screen.portrait

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.InfoStealer.BB
Adobe Malware Classifier	
Aegislab	BadNews
Agnitum	
AhnLab-V3	Android-Malicious/BadNews
ALYac	
Anchivia	
Antiy-AVL	
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Android:InfoStealer-I [Trj] *^
AVG	Android/Generic.AP
Avira	Android/BadNews.A.Gen
AVware	Trojan.AndroidOS.Generic.A *
Baidu	
BitDefender	Android.Trojan.InfoStealer.BB
Bkav	
ByteHero	
ClamAV	Andr.Trojan.Badnews
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.5B08C967!Olympus *, AndroidOS/BadNews.A.gen!E!dorado
Digital Patrol	
DrWeb	Android.Androways.1.origin
EmsiSoft	Android.Trojan.InfoStealer.BB (B)
Epoolsoft	
eScan	Android.Trojan.InfoStealer.BB
F-Mirc	
F-Prot	
F-Secure	Trojan:Android/InfoStealer.I *^
FileMedic	
FilsecLab Twister	Android.BadNew.A.jwjr *
Fortinet	Android/BadNews.A!tr.dldr
GData	Android.Trojan.InfoStealer.BB
GFI Vipre	Trojan.AndroidOS.Generic.A *
Ikarus	Trojan.AndroidOS.BadNews *
Immunos	Andr.Trojan.Badnews
Jiangmin	
K7 Antivirus	Trojan (0001140e1)
K7GW Antivirus	Trojan (0001140e1)
Kaspersky	not-a-virus:HEUR:AdWare.AndroidOS.Anways.a
Kingsoft	Android.Troj.Fakeinst.sc.(kcloud)
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!5B08C96794AD *
McAfee GW	
Microsoft	
NANO AntiVirus	Trojan.Android.Anways.cwyczq
NOD32	Android/BadNew.A
NoraLabs NoraScan	
Norman	
Norton Symantec	Trojan.Gen.2
nProtect	
OfficeMalScanner	

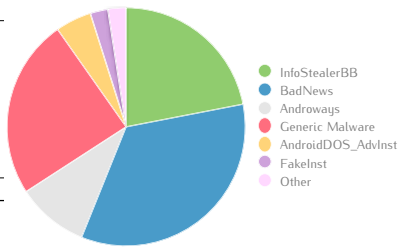
Antivirus	Result
Panda	
PathFinder	*NO MALWARE $*
Preventon	Andr/BadNews-A
Protector Plus	
PSafe Antivirus	
Qihoo 360	Win32/Trojan.f61 *
Quick Heal (Cat)	
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Trojan.InfoStealer.BB
Segurmatica	
Segurmatica KE	not-a-virus:HEUR:AdWare.AndroidOS.Anways.a
Solo	
Sophos	Andr/BadNews-A
SUPERAntiSpyware	
Team Cymru	*NO MALWARE $*
The Cleaner	
The Hacker	
TotalDefense	
TotalDefense Cloud	
Tencent	Trojan.Android.Agent.4D6AC939 *
Trend Micro	ANDROIDOS_ADVINST.A, ANDROID.EC9F40F0
Trend Micro-Housecall	ANDROIDOS_ADVINST.A
TrustPort	
TT Livescan	
VBA32	
Vexira	
VirIT eXplorer	Android.Trj.BadNews.B *
VIRobot	Android.Trojan.InfoStealer.BB[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.BadNews.A

Detected	41
Undetected	48
Sum	89



Name Distribution

Name	Amount	Score
InfoStealerBB	9	0
BadNews	14	3
Androways	4	0
Generic Malware	10	1
AndroidDOS_AdvInst	2	0
FakeInst	1	0
Other	1	1
Sum	41	



Average Score	0,06

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.ACCESS_WIFI_STATE	Allows applications to access information about WI-FI networks
android.permission.INSTALL_PACKAGES	Allows an application to install packages
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting
android.permission.RESTART_PACKAGES	This constant was deprecated in API level 8
android.permission.VIBRATE	Allows access to the vibrator
android.permission.WAKE_LOCK	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage
com.android.launcher.permission.INSTALL_SHORTCUT	Allows an application to install a shortcut in Launcher

Used Permissions	Description	API calls
android.permission.ACCESS_NETWORK_STATE		android/net/ConnectivityManager;->getActiveNetworkInfo
android.permission.FACTORY_TEST °	Run as a manufacturer test application, running as the root user	android/content/pm/ApplicationInfo/lflags
android.permission.INTERNET		android/webkit/WebView
android.permission.READ_CONTACTS °	Allows an application to read the user's contacts data	android/content/ContentResolver;->query
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getDeviceId
android.permission.VIBRATE		android/app/NotificationManager;->Notify
android.permission.WAKE_LOCK		android/media/MediaPlayer;->start

Used Intents
android.intent.action.BOOT_COMPLETED
android.intent.action.MAIN
android.intent.action.PHONE_STATE
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.google.ads.AdActivity	✗	✔	✗
ru.blogspot.playsib.savageknife.GameActivity	✔	✔	✔

Services	Used	Provided by Android	Provided by Third-Parties
com.mobidisplay.advertsv1.AdvService	✔	✔	✔

Receivers	Used	Provided by Android	Provided by Third-Parties
com.mobidisplay.advertsv1.BootReceiver	✔	✔	✗
com.mobidisplay.advertsv1.AReceiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties

Used Networks
-

Native Libraries Loaded
/data/data/ru.blogspot.playsib.savageknife/lib/libnativebuffer.so 0x40516ae0

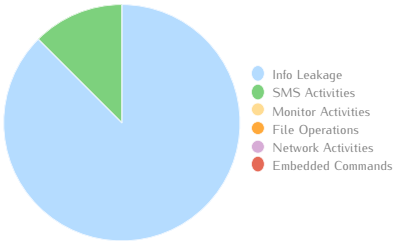
Network Analysis

Hardcoded URLs	IP	Region
mobidisplay.net	188.130.251.44	Russian Federation
e.admob.com	203.208.49.185	China - Beijing
schemas.android.com	-	-
media.admob.com	117.144.231.206	China - Beijing
www.gstatic.com	117.144.231.206	China - Beijing

Request	IP	Region	Type
media.admob.com	74.125.237.25	United States - Mountain View	HTTP GET / DNS
googleads.g.doubleclick.net	74.125.237.25	United States - Mountain View	HTTP GET / DNS
csi.gstatic.com	173.194.34.143	United States - Mountain View	HTTP GET / DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	Call_Query	List phone call records
	Contact_Query	List contacts
	Network_NetProvider_Get	Retrieve network provider information
	Location_Get	Retrieve current phone location
	Phone_IMEI_Get	Retrieve IMEI
	Phone_Number_Get	Retrieve current phone number
	SMS_Query	List SMS
SMS Activities	Notification_Send	Send notifications
Monitor Activities	-	
File Operations	-	
Network Activities	-	
Embedded Commands	-	



Info Leakage	7
SMS Activities	1
Monitor Activities	0
File Operations	0
Network Activities	0
Embedded Commands	0

BaseBridge A

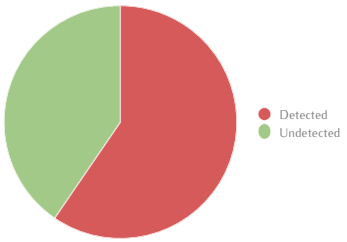
MD5	e5108aac09d9726aaf700727fb4bc937
SHA-1	4d7e5692dcc1cadb8ddb391da06cf367eeae0eb2
SHA-256	ac6fc1cbf61a6d7980d01199d63aa46b78db4ac9cb3235c85ea9bb74d856dcbd
API Level	0
File Dimension (MB)	1.45
Package Name	com.keji.danti419
Other Names	3ed1e8ea99365c17127726a6bababdf5a77610b3a5b138f5c9e0b637bfc3879f
Used Features	android.hardware.wifi android.hardware.touchscreen android.hardware.screen.portrait android.hardware.telephony

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.BaseBridge.A
Adobe Malware Classifier	
Aegislab	BaseBridge
Agnitum	
AhnLab-V3	Android-Malicious/BaseBridge
ALYac	
Anchivia	
Antiy-AVL	
Anvisoft	
Anvisoft Cloud	
ArcaVir	Androidos.basebrid.ae
Avast	Android:BaseBridge-L [Trj]
AVG	Android_c.HKK
Avira	Android/BaseBrid.C.Gen, Android/BaseBrid.O
AVware	Trojan.AndroidOS.BaseBridge.c
Baidu	Trojan.Android.BaseBridge.bC
BitDefender	Android.Trojan.BaseBridge.A
Bkav	
ByteHero	
ClamAV	Andr.Basebridge-28
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.BA59B02F!Olympus, AndroidOS/BaseBridge.B
Digital Patrol	Backdoor.AndroidOS.BaseBrid.a
DrWeb	Android.Basebridge.4.origin
EmsiSoft	Android.Trojan.BaseBridge.A (B)
Epoolsoft	
eScan	Android.Trojan.BaseBridge.A, Android.Trojan.BaseBridge.G [ZP]
F-Mirc	
F-Prot	AndroidOS/BaseBridge.B
F-Secure	Trojan:Android/BaseBridge.S
FileMedic	
FilsecLab Twister	Android.BaseBridge.C.bvtl, Android.M.untr
Fortinet	Android/Basebridge.AA!tr
GData	Android.Trojan.BaseBridge.A
GFI Vipre	Trojan.AndroidOS.BaseBridge.c
Ikarus	Trojan.AndroidOS.BaseBridge
Immunos	Andr.Trojan.Anserver-1
Jiangmin	Backdoor/AndroidOS.cw, Backdoor/AndroidOS.azt
K7 Antivirus	
K7GW Antivirus	Trojan (0048d5051)
Kaspersky	HEUR:Backdoor.AndroidOS.BaseBrid.a
Kingsoft	Android.Troj.at_Keji.a.(kcloud)
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!E5108AAC09D9
McAfee GW	
Microsoft	Trojan:AndroidOS/BaseBridge.B
NANO AntiVirus	Trojan.Android.BaseBrid.cwyczu
NOD32	Android/BaseBridge.C, Android/BaseBridge.D
NoraLabs NoraScan	
Norman	doslegacy/Suspicious_Gen2.RWWNU
Norton Symantec	Trojan.Gen.2
nProtect	
OfficeMalScanner	

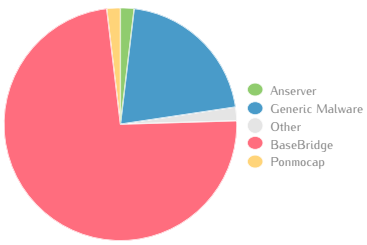
Antivirus	Result
Panda	Generic Malware
PathFinder	
Preventon	Andr/Answer-A, Andr/BBridge-A
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Android.BaseBridge.C
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Trojan.BaseBridge.A
Segurmatica	
Segurmatica KE	HEUR:Backdoor.AndroidOS.BaseBrid.a
Solo	
Sophos	Andr/Answer-A, Andr/BBridge-A
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	AndroidOS/MalAndroid
TotalDefense Cloud	Win32/Ponmocup!CcAOPFB, Win32/Ponmocup!CcQYGd
Tencent	Dos.Backdoor.Basebrid.Ahns
Trend Micro	AndroidOS_BASEBRIDGE.BLK, Android.28470EF1
Trend Micro-Housecall	AndroidOS_BASEBRIDGE.BLK
TrustPort	Android.Trojan.BaseBridge.G
TT Livescan	
VBA32	Backdoor.AndroidOS.BaseBrid.ae, Backdoor.AndroidOS
Vexira	
VirIT eXplorer	Android.Trj.BaseBird.AL
VIRobot	Android.Trojan.BaseBridge.A[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.BaseBridge.SMA

Detected	53
Undetected	36
Sum	89



Name Distribution

Name	Amount	Score
Anserver	1	2
Generic Malware	11	1
Other	1	1
BaseBridge	39	3
Ponmocap	1	0
Sum	53	



Average Score	1,07

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.ACCESS_WIFI_STATE	Allows applications to access information about WI-FI networks
android.permission.CALL_PHONE	Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call being placed
android.permission.DISABLE_KEYGUARD	Allows applications to disable the keyguard
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.READ_SMS	Allows an application to read SMS messages
android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting
android.permission.RECEIVE_SMS	Allows an application to monitor incoming SMS messages, to record or perform processing on them
android.permission.RESTART_PACKAGES	This constant was deprecated in API level 8
android.permission.SEND_SMS	Allows an application to send SMS messages
android.permission.VIBRATE	Allows access to the vibrator
android.permission.WAKE_LOCK	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming
android.permission.WRITE_APN_SETTINGS	Allows applications to write the apn settings
android.permission.WRITE_CONTACTS	Allows an application to write (but not read) the user's contacts data
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage
android.permission.WRITE_SMS	Allows an application to write SMS messages

Used Permissions	Description	API calls
android.permission.ACCESS_NETWORK_STATE		android/net/ConnectivityManager;->getActiveNetworkInfo
android.permission.DISABLE_KEYGUARD		android/app/KeyguardManager$KeyguardLock;->disableKeyguard
android.permission.FACTORY_TEST °	Run as a manufacturer test application, running as the root user	android/content/pm/ApplicationInfo/Iflags
android.permission.INTERNET		java/net/DatagramSocket
android.permission.READ_CONTACTS °	Allows an application to read the user's contacts data	android/content/ContentResolver;->query
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getSubscriberId
android.permission.RESTART_PACKAGES		android/app/ActivityManager;->restartPackage
android.permission.SEND_SMS		android/telephony/SmsManager;->sendTextMessage
android.permission.VIBRATE		android/app/NotificationManager;->Notify

Used Intents
android.intent.action.ACTION_POWER_CONNECTED
android.intent.action.BATTERY_LOW
android.intent.action.BATTERY_OKAY
android.intent.action.BOOT_COMPLETED
android.intent.action.INPUT_METHOD_CHANGED
android.intent.action.MAIN
android.intent.action.USER_PRESENT
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.android.battery.BalckActivity	✗	✓	✗
com.android.battery.BalckActivity2	✗	✓	✗
com.android.battery.KillThreeSixZero	✓	✓	✗
com.keji.danti.Background	✗	✓	✗
com.keji.danti.Boutique	✓	✓	✗
com.keji.danti.History	✗	✓	✗
com.keji.danti.Lists	✗	✓	✗
com.keji.danti.MainA	✓	✓	✓
com.keji.danti.Setting	✓	✓	✗
com.keji.danti.TextDetail	✗	✓	✗

Services	Used	Provided by Android	Provided by Third-Parties
com.android.battery.BridgeProvider	✓	✓	✓
com.android.music.MediaPlaybackService	✓	✓	
com.android.battery.AdSmsService	✓	✓	✗
com.android.battery.PhoneService	✓	✓	✗

Receivers	Used	Provided by Android	Provided by Third-Parties
com.android.battery.BaseBroadcastReceiver	✓	✓	✓

Providers	Used	Provided by Android	Provided by Third-Parties
android.provider.Telephony.SMS_RECEIVED	✓		
android.provider.Telephony.SIM_FULL	✓		
android.provider.Telephony.WAP_PUSH_RECEIVED	✓		

Used Networks
android.net.conn.CONNECTIVITY_CHANGE

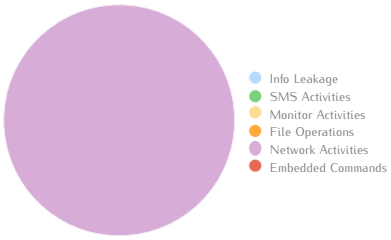
Network Analysis

Hardcoded URLs	IP	Region
maps.google.com	74.125.235.164	United States - Mountain View
schemas.android.com	-	-
wap.soso.com	220.181.124.2	China - Beijing

Request	IP	Region	Type
dev.adtouchnetwork.net	54.72.9.51	United States - Woodbridge	HTTP POST / DNS
dev.adtouchnetwork.net	61.155.178.159	China - Nanjing	HTTP POST
tx.cookier.co.cc	112.175.243.12	South Korea - Seul	DNS
b3.cookier.co.cc	112.175.243.12	South Korea - Seul	DNS
clock.isc.org	149.20.64.28	United States - Palo Alto	DNS
-	51.9.72.54.in-addr.arpa	United Kingdom	DNS
-	199.2.137.140	United States	HTTP GET / POST

Potentially Dangerous Operations

	Name	Description
Info Leakage	Unable to Analyze	
SMS Activities	Unable to Analyze	
Monitor Activities	Unable to Analyze	
File Operations	Unable to Analyze	
Network Activities	TAINT_IMSI	b3.cookier.co.cc:8080 (2 times)
Embedded Commands	Unable to Analyze	



Info Leakage	0
SMS Activities	0
Monitor Activities	0
File Operations	0
Network Activities	2
Embedded Commands	0

BaseBridge B

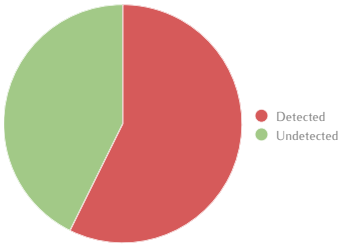
MD5	936162a5cdfc1e73a1d8740ab1d164b2
SHA-1	bea3692585279f964d253b1ab29ebaffe393fa65
SHA-256	58781d1e86b8ea935c6ae7145b0a46e70e92d10e39f02404dc5bfab6e4d1bded
API Level	0
File Dimension (MB)	1.46
Package Name	com.keji.danti427
Other Names	bea3692585279f964d253b1ab29ebaffe393fa65
Used Features	android.hardware.wifi android.hardware.touchscreen android.hardware.screen.portrait android.hardware.telephony

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.BaseBridge.A
Adobe Malware Classifier	
Aegislab	BaseBridge
Agnitum	
AhnLab-V3	Android-Malicious/BaseBridge
ALYac	
Anchivia	
Antiy-AVL	
Anvisoft	
Anvisoft Cloud	
ArcaVir	*NO MALWARE $*
Avast	Android:BaseBridge-L [Trj]
AVG	Android_c.EDM *
Avira	Android/BaseBrid.C.Gen, Android/BaseBrid.O
AVware	Trojan.AndroidOS.BaseBridge.c
Baidu	Trojan.Android.BaseBridge.bC
BitDefender	Android.Trojan.BaseBridge.A
Bkav	
ByteHero	
ClamAV	Andr.Basebridge-28
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.BA59B02F!Olympus, AndroidOS/BaseBridge.B
Digital Patrol	*NO MALWARE $*
DrWeb	Android.Basebridge.4.origin
EmsiSoft	Android.Trojan.BaseBridge.A (B)
Epoolsoft	
eScan	Android.Trojan.BaseBridge.A, Android.Trojan.BaseBridge.G [ZP]
F-Mirc	
F-Prot	AndroidOS/BaseBridge.B
F-Secure	Trojan:Android/BaseBridge.S
FileMedic	
FilsecLab Twister	Android.BaseBridge.C.bvtl, Android.M.sdfa *
Fortinet	Android/Basebridge.AA!tr
GData	Android.Trojan.BaseBridge.A
GFI Vipre	Trojan.AndroidOS.BaseBridge.c
Ikarus	Trojan.AndroidOS.BaseBridge
Immunos	Andr.Trojan.Anserver-1
Jiangmin	Backdoor/AndroidOS.cw, Backdoor/AndroidOS.dw *
K7 Antivirus	
K7GW Antivirus	Trojan (0048d5051)
Kaspersky	HEUR:Backdoor.AndroidOS.BaseBrid.a
Kingsoft	Troj.Lotoor.a.(kcloud) *
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!936162A5CDFC *
McAfee GW	
Microsoft	Trojan:AndroidOS/BaseBridge.B
NANO AntiVirus	Trojan.Android.BaseBrid.cwyczu
NOD32	Android/BaseBridge.C, Android/BaseBridge.D
NoraLabs NoraScan	
Norman	doslegacy/Suspicious_Gen2.RWWNU
Norton Symantec	Trojan.Gen.2
nProtect	
OfficeMalScanner	

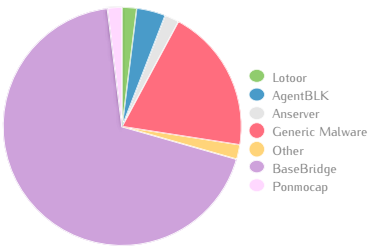
Antivirus	Result
Panda	Generic Malware
PathFinder	
Preventon	Andr/Ansver-A, Andr/BBridge-A
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Android.BaseBridge.C
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Trojan.BaseBridge.A
Segurmatica	
Segurmatica KE	HEUR:Backdoor.AndroidOS.BaseBrid.a
Solo	
Sophos	Andr/Ansver-A, Andr/BBridge-A
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	AndroidOS/MalAndroid
TotalDefense Cloud	Win32/Ponmocup!CTYNVFB *, Win32/Ponmocup!CcQYGd
Tencent	Dos.Backdoor.Basebrid.Hryf *
Trend Micro	AndroidOS_AGENTBLK.200 *, Android.28470EF1
Trend Micro-Housecall	AndroidOS_AGENTBLK.200 *
TrustPort	Android.Trojan.BaseBridge.G
TT Livescan	
VBA32	Backdoor.AndroidOS.BaseBrid.ae, Backdoor.AndroidOS
Vexira	
VirIT eXplorer	Android.Trj.BaseBird.AL
VIRobot	Android.Trojan.BaseBridge.A[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.BaseBridge.F *

Detected	51
Undetected	38
Sum	89



Name Distribution

Name	Amount	Score
Lotoor	1	2
AgentBLK	2	0
Anserver	1	2
Generic Malware	10	1
Other	1	1
BaseBridge	35	3
Ponmocap	1	0
Sum	51	



Average Score	0,92

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.ACCESS_WIFI_STATE	Allows applications to access information about WI-FI networks
android.permission.CALL_PHONE	Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call being placed
android.permission.DISABLE_KEYGUARD	Allows applications to disable the keyguard
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.READ_SMS	Allows an application to read SMS messages
android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting
android.permission.RECEIVE_SMS	Allows an application to monitor incoming SMS messages, to record or perform processing on them
android.permission.RESTART_PACKAGES	This constant was deprecated in API level 8
android.permission.SEND_SMS	Allows an application to send SMS messages
android.permission.VIBRATE	Allows access to the vibrator
android.permission.WAKE_LOCK	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming
android.permission.WRITE_APN_SETTINGS	Allows applications to write the apn settings
android.permission.WRITE_CONTACTS	Allows an application to write (but not read) the user's contacts data
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage
android.permission.WRITE_SMS	Allows an application to write SMS messages

Used Permissions	Description	API calls
android.permission.ACCESS_NETWORK_STATE		android/net/ConnectivityManager;->getActiveNetworkInfo
android.permission.DISABLE_KEYGUARD		android/app/KeyguardManager$KeyguardLock;->disableKeyguard
android.permission.FACTORY_TEST °	Run as a manufacturer test application, running as the root user	android/content/pm/ApplicationInfo/Iflags
android.permission.INTERNET		java/net/DatagramSocket
android.permission.READ_CONTACTS °	Allows an application to read the user's contacts data	android/content/ContentResolver;->query
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getSubscriberId
android.permission.RESTART_PACKAGES		android/app/ActivityManager;->restartPackage
android.permission.SEND_SMS		android/telephony/SmsManager;->sendTextMessage
android.permission.VIBRATE		android/app/NotificationManager;->Notify

Used Intents
android.intent.action.ACTION_POWER_CONNECTED
android.intent.action.BATTERY_LOW
android.intent.action.BATTERY_OKAY
android.intent.action.BOOT_COMPLETED
android.intent.action.INPUT_METHOD_CHANGED
android.intent.action.MAIN
android.intent.action.USER_PRESENT
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.android.battery.BalckActivity	✕	✔	✕
com.android.battery.BalckActivity2	✕	✔	✕
com.android.battery.KillThreeSixZero	✔	✔	✕
com.keji.danti.Background	✕	✔	✕
com.keji.danti.Boutique	✔	✔	✕
com.keji.danti.History	✕	✔	✕
com.keji.danti.Lists	✕	✔	✕
com.keji.danti.MainA	✔	✔	✔
com.keji.danti.Setting	✔	✔	✕
com.keji.danti.TextDetail	✕	✔	✕

Services	Used	Provided by Android	Provided by Third-Parties
com.android.battery.BridgeProvider	✔	✔	✔
com.android.music.MediaPlaybackService	✔	✔	
com.android.battery.AdSmsService	✔	✔	✕
com.android.battery.PhoneService	✔	✔	✕

Receivers	Used	Provided by Android	Provided by Third-Parties
com.android.battery.BaseBroadcastReceiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
android.provider.Telephony.SMS_RECEIVED	✔		
android.provider.Telephony.SIM_FULL	✔		
android.provider.Telephony.WAP_PUSH_RECEIVED	✔		

Used Networks
android.net.conn.CONNECTIVITY_CHANGE

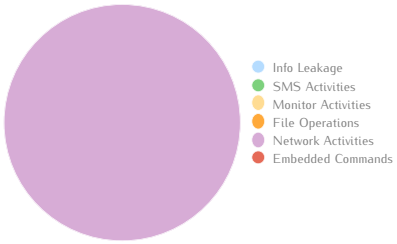
Network Analysis

Hardcoded URLs	IP	Region
maps.google.com	74.125.235.164	United States - Mountain View
schemas.android.com	-	-
wap.soso.com	220.181.124.2	China - Beijing

Request	IP	Region	Type
dev.adtouchnetwork.net	54.72.9.51	United States - Woodbridge	HTTP POST / DNS
dev.adtouchnetwork.net	61.155.178.159	China - Nanjing	HTTP POST
tx.cookier.co.cc	112.175.243.12	South Korea - Seul	DNS
b3.cookier.co.cc	112.175.243.12	South Korea - Seul	DNS
clock.isc.org	149.20.64.28	United States - Palo Alto	DNS
-	51.9.72.54.in-addr.arpa	United Kingdom	DNS
-	199.2.137.140	United States	HTTP GET / POST

Potentially Dangerous Operations

	Name	Description
Info Leakage	Unable to Analyze	
SMS Activities	Unable to Analyze	
Monitor Activities	Unable to Analyze	
File Operations	Unable to Analyze	
Network Activities	TAINT_IMSI	b3.cookier.co.cc:8080 (2 times)
Embedded Commands	Unable to Analyze	



Info Leakage	0
SMS Activities	0
Monitor Activities	0
File Operations	0
Network Activities	2
Embedded Commands	0

BGServ A

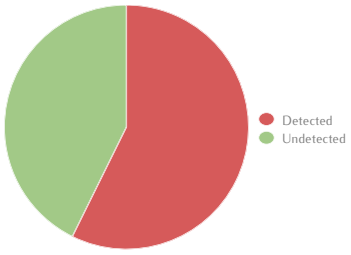
MD5	955f3696bd38dfe7a49afdd4f8f31f95
SHA-1	03f9fc8769422f66c59922319bffad46d0ceea94
SHA-256	937315f1ec9e850d738e45607290fd01c2fa33ffdb1ac11201467441646657d2
API Level	3
File Dimension (MB)	0.33
Package Name	com.virsir.android.chinamobile10086
Other Names	03f9fc8769422f66c59922319bffad46d0ceea94
Used Features	android.hardware.location android.hardware.location.gps android.hardware.location.network android.hardware.wifi android.hardware.telephony android.hardware.touchscreen

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.BgServ.A
Adobe Malware Classifier	
Aegislab	Fake10086
Agnitum	
AhnLab-V3	Android-Malicious/BgService
ALYac	
Anchivia	
Antiy-AVL	Trojan/win32.agent
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Android:BGServ-G [Trj]
AVG	Android/Serb
Avira	Android/SerBG.b
AVware	Trojan.AndroidOS.Lanucher.A
Baidu	Backdoor.AndroidOS.SerBG.Arkz
BitDefender	Android.Trojan.BgServ.A
Bkav	
ByteHero	
ClamAV	Andr.BGServ-4
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.955F3696!Olympus, AndroidOS/BgServ
Digital Patrol	Backdoor.AndroidOS.SerBG.b
DrWeb	Android.Youlubg.2
EmsiSoft	Android.Trojan.BgServ.A (B)
Epoolsoft	
eScan	Android.Trojan.BgServ.A[ZP]
F-Mirc	
F-Prot	AndroidOS/BgServ
F-Secure	Trojan:Android/Bgserv.A
FileMedic	
FilsecLab Twister	Android.M.tmmu
Fortinet	Android/Fake10086.A!tr
GData	Android.Trojan.BgServ.A
GFI Vipre	Trojan.AndroidOS.Lanucher.A
Ikarus	Trojan.AndroidOS.Masnu
Immunos	Andr.BGServ-4
Jiangmin	Backdoor/AndroidOS.byz
K7 Antivirus	
K7GW Antivirus	Trojan (0001140e1)
Kaspersky	HEUR:Backdoor.AndroidOS.SerBG.a
Kingsoft	Troj.BgServ.a.(kcloud)
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!E5108AAC09D9
McAfee GW	
Microsoft	TrojanSpy:AndroidOS/Lanucher.A
NANO AntiVirus	Trojan.Android.SerBG.cwydad
NOD32	Android/Bgserv.B
NoraLabs NoraScan	
Norman	doslegacy/Suspicious_Gen2.PMXQX
Norton Symantec	Backdoor.Trojan
nProtect	
OfficeMalScanner	

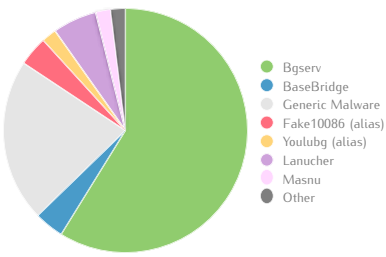
Antivirus	Result
Panda	
PathFinder	
Preventon	Andr/BBridge-A
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Android.BgServ.A
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Trojan.BgServ.A
Segurmatica	
Segurmatica KE	HEUR:Backdoor.AndroidOS.SerBG.a
Solo	
Sophos	Andr/BBridge-A Andr/BBridge-A
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	
TotalDefense Cloud	Heur/Backdoor!CYeeNS
Tencent	Trojan.Android.Agent.8A60CE65
Trend Micro	AndroidOS_BGSRV.A, Android.69EEF8D1
Trend Micro-Housecall	AndroidOS_BGSRV.A
TrustPort	Android.Trojan.BgServ.A
TT Livescan	
VBA32	Backdoor.AndroidOS.SerBG.b
Vexira	
VirIT eXplorer	Android.Bkd.BgServ.A
VIRobot	Android.Trojan.BgServ.A[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.Bgserv.B

Detected	51
Undetected	38
Sum	89



Name Distribution

Name	Amount	Score
Bgserv	30	3
BaseBridge	2	0
Generic Malware	11	1
Fake10086 (alias)	2	3
Youlubg (alias)	1	3
Lanucher	3	2
Masnu	1	0
Other	1	1
Sum	**51**	



Average Score	0,89

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_COARSE_LOCATION	Allows an app to access approximate location derived from network location sources such as cell towers and WI-FI
android.permission.ACCESS_FINE_LOCATION	Allows an app to access precise location from location sources such as GPS, cell towers, and WI-FI
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.ACCESS_WIFI_STATE	Allows applications to access information about WI-FI networks
android.permission.CHANGE_NETWORK_STATE	Allows applications to change network connectivity state
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.READ_SMS	Allows an application to read SMS messages
android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting
android.permission.RECEIVE_SMS	Allows an application to monitor incoming SMS messages, to record or perform processing on them
android.permission.SEND_SMS	Allows an application to send SMS messages
android.permission.WAKE_LOCK	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage

Used Permissions	Description	API calls
android.permission.ACCESS_FINE_LOCATION		android/location/LocationManager;->getBestProvider
android.permission.ACCESS_NETWORK_STATE		android/net/ConnectivityManager;->getNetworkInfo
android.permission.ACCESS_WIFI_STATE		android/net/wifi/WifiManager;->getConnectionInfo
android.permission.INTERNET		android/webkit/WebView
android.permission.READ_CONTACTS °	Allows an application to read the user's contacts data	android/content/ContentResolver;->query
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getDeviceId
android.permission.SEND_SMS		android/telephony/SmsManager;->sendTextMessage
android.permission.VIBRATE °	Allows access to the vibrator	android/app/NotificationManager;->Notify
android.permission.WAKE_LOCK		android/os/PowerManager$WakeLock;->acquire

Used Intents
android.intent.action.BOOT_COMPLETED
android.intent.action.CREATE_SHORTCUT
android.intent.action.MAIN
android.intent.action.SEND_MESSAGE
android.intent.category.DEFAULT
android.intent.category.DEFAULT
android.intent.category.LAUNCHER

Native Libraries Loaded
/system/lib/libmedia_jni.so 0x0
/system/lib/libexif.so 0x0
/system/lib/libsoundpool.so 0x0
/system/lib/libwebcore.so 0x0
/system/lib/libandroid_servers.so 0x0

Activities	Used	Provided by Android	Provided by Third-Parties
com.mms.bg.ui.FakeLanucherActivity	✔	✔	✔
com.virsir.android.chinamobile10086.MainView	✔	✔	✘
com.virsir.android.chinamobile10086. PromotionView	✔	✔	✘
com.virsir.android.chinamobile10086.Root	✔	✔	✘
com.virsir.android.chinamobile10086. SearchOfficesView	✔	✔	✘
com.virsir.android.chinamobile10086.ShortCut	✔	✔	✔
com.virsir.android.chinamobile10086.news.News	✔	✔	✘
com.virsir.android.chinamobile10086.news. NewsBrowser	✔	✔	✘
com.virsir.android.chinamobile10086.news. NewsChannelSelector	✔	✔	✘
com.virsir.android.chinamobile10086.news. NewsDetails	✔	✔	✘

Services	Used	Provided by Android	Provided by Third-Parties
com.mms.bg.ui.BgService	✔	✔	✔
com.virsir.android.chinamobile10086. CheckUpdateService	✔	✔	✘
com.virsir.android.chinamobile10086.SMSService	✔	✔	✘
com.android.music.MediaPlaybackService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
com.mms.bg.transaction.PrivilegedSmsReceiver	✔	✔	✔
com.mms.bg.transaction.SmsReceiver	✔	✔	✔
com.mms.bg.ui.AutoSMSRecevier	✔	✔	✔
com.mms.bg.ui.BootReceiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
android.provider.Telephony.SMS_RECEIVED	✔		

Used Networks
android.net.conn.CONNECTIVITY_CHANGE

Toast Messages
对不起，您的软件不支持电子市场 [Sorry, your software does not support the electronic market]

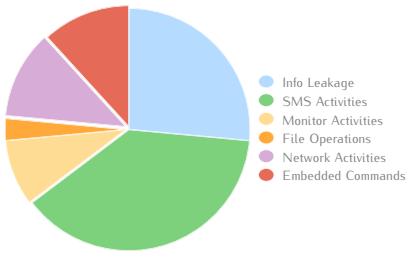
Network Analysis

Hardcoded URLs	IP	Region
apps.virsir.com	209.141.55.182	United States - San Jose
schemas.android.com	-	-
news.163.com	117.144.231.206	China - Beijing
ent.163.com	112.25.33.28	China - Beijing
d.wiyun.com	119.254.87.201	China - Beijing
data.flurry.com	117.144.231.200	China - Beijing
ajax.googleapis.com	117.144.231.205	China - Beijing
tech.163.com	112.25.33.28	China - Beijing
money.163.com	111.1.53.220	China - Beijing
maps.google.com	74.125.235.164	United States - Mountain View
www.youlubg.com	59.188.232.71	Hong Kong
mmsc.monternet.com	-	-
gate.baidu.com	111.13.12.14	China - Beijing
211.136.165.53	211.136.165.53	China - Shanghai
market.android.com	117.144.231.205	China - Beijing

Request	IP	Region	Type
data.flurry.com	74.217.75.7	United States - Seattle	HTTP POST / DNS
apps.virsir.com	209.241.55.182	United States / Canada	HTTP GET / DNS
d.wiyun.com	119.254.87.201	China - Beijing	HTTP GET / DNS
-	13.203.52.216.in-addr.arpa	United States - Norwalk	DNS
-	182.55.141.209.in-addr.arpa	Singapore	DNS
-	201.87.254.119.in-addr.arpa	Brasil	DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	Call_Query	List phone call records
	Contact_Query	List contacts
	GPS_Get	Retrieve GPS information
	Location_Last_Get	Retrieve last phone location
	Location_Get	Retrieve current phone location
	Network_NetProvider_Get	Retrieve network provider information
	Phone_IMEI_Get	Retrieve IMEI
	Phone_Number_Get	Retrieve current phone number
	SMS_Query	List SMS
SMS Activities	Contact_Create	Create contact
	Contact_Erase	Delete contact
	Database_Erase	Delete database
	Notification_Send	Send notifications
	SMS_Analysis	Analysis SMS messages
	SMS_Create_Message	Create SMS Inbox
	SMS_Delete_Message	Delete SMS Inbox
	SMS_Erase	Delete SMS
	SMS_Intercept	Intercept SMS
	SMS_Send	Send "1234567" to 10086 (4 times)
Monitor Activities	Database_Spy	Spy database
	GPS_Spy	Spy GPS state
	Location_SPY	Spy location
File Operations	File_Erase	Delete file
Network Activities	TAINT_IMEI	d.wiyun.com:80 (4 times)
Embedded Commands	unix-compress	Compress file
	unix-mkdir	Make a directory
	unix-sleep	Suspend execution for a specified interval
	unix-su	Set super-user mode



Info Leakage	9
SMS Activities	13
Monitor Activities	3
File Operations	1
Network Activities	4
Embedded Commands	4

BGServ B

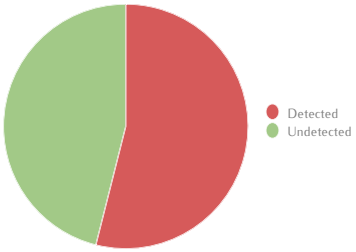
MD5	ea2db6c29fde7caa371cf3b4adc85cba
SHA-1	e9c841757db6816f978deb573fd8e8ed0fe6be3b
SHA-256	c63984592be2fd37f263ee80819c023a46478bedad8a1e8aeecff8315f7df2c5
API Level	3
File Dimension (MB)	0.31
Package Name	com.virsir.android.chinamobile10086
Other Names	e9c841757db6816f978deb573fd8e8ed0fe6be3b
Used Features	android.hardware.location android.hardware.location.gps android.hardware.location.network android.hardware.wifi android.hardware.telephony android.hardware.touchscreen

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.BgServ.A
Adobe Malware Classifier	
Aegislab	Fake10086
Agnitum	
AhnLab-V3	Android-Malicious/BgService
ALYac	
Anchivia	
Antiy-AVL	*NO MALWARE $*
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Android:BGServ-G [Trj]
AVG	Android/Serb
Avira	Android/SerBG.E *
AVware	Trojan.AndroidOS.Lanucher.A
Baidu	Backdoor.AndroidOS.SerBG.AXxB *
BitDefender	Android.Trojan.BgServ.A
Bkav	
ByteHero	
ClamAV	Andr.BGServ-12 *
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.EA2DB6C2!Olympus *, AndroidOS/BgServ.A *
Digital Patrol	*NO MALWARE $*
DrWeb	Android.Youlubg.1 *
EmsiSoft	Android.Trojan.BgServ.A (B)
Epoolsoft	
eScan	Android.Trojan.BgServ.A[ZP]
F-Mirc	
F-Prot	AndroidOS/BgServ.A *
F-Secure	Trojan:Android/Bgserv.A
FileMedic	
FilsecLab Twister	Android.M.crus *
Fortinet	Android/Fake10086.A!tr
GData	Android.Trojan.BgServ.A
GFI Vipre	Trojan.AndroidOS.Lanucher.A
Ikarus	Trojan.AndroidOS.SerBG *£
Immunos	Andr.BGServ-12 *
Jiangmin	Backdoor/AndroidOS.cc *
K7 Antivirus	
K7GW Antivirus	Trojan (0001140e1)
Kaspersky	HEUR:Backdoor.AndroidOS.SerBG.a
Kingsoft	Troj.BgServ.a.(kcloud)
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!EA2DB6C29FDE *
McAfee GW	
Microsoft	*NO MALWARE $*
NANO AntiVirus	Trojan.Android.SerBG.cwydad
NOD32	Android/Bgserv.D *
NoraLabs NoraScan	
Norman	doslegacy/Suspicious_Gen2.QROZO *
Norton Symantec	Android.Bgserv *£
nProtect	
OfficeMalScanner	

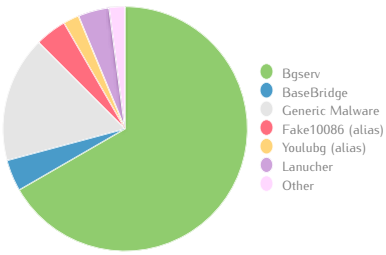
Antivirus	Result
Panda	
PathFinder	
Preventon	Andr/BBridge-A
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Android.BgServ.A
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Trojan.BgServ.A
Segurmatica	
Segurmatica KE	HEUR:Backdoor.AndroidOS.SerBG.a
Solo	
Sophos	Andr/BBridge-A Andr/BBridge-A
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	
TotalDefense Cloud	Heur/Backdoor!CARQPFB *, Heur/Backdoor!CTaRNS *
Tencent	Dos.Backdoor.Serbg.Ajvh *£
Trend Micro	AndroidOS_BGSERV.A *, Android.1543EFF9 *
Trend Micro-Housecall	AndroidOS_BGESRV.A *
TrustPort	Android.Trojan.BgServ.A
TT Livescan	
VBA32	Backdoor.AndroidOS.SerBG.d *
Vexira	
VirIT eXplorer	Android.Bkd.BgServ.B *
VIRobot	Android.Trojan.BgServ.A[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.Bgserv.B

Detected	48
Undetected	41
Sum	89



Name Distribution

Name	Amount	Score
Bgserv	32	3
BaseBridge	2	0
Generic Malware	8	1
Fake10086 (alias)	2	3
Youlubg (alias)	1	3
Lanucher	2	2
Other	1	1
Sum	**48**	



Average Score	0,87

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_COARSE_LOCATION	Allows an app to access approximate location derived from network location sources such as cell towers and WI-FI
android.permission.ACCESS_FINE_LOCATION	Allows an app to access precise location from location sources such as GPS, cell towers, and WI-FI
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.ACCESS_WIFI_STATE	Allows applications to access information about WI-FI networks
android.permission.CHANGE_NETWORK_STATE	Allows applications to change network connectivity state
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.READ_SMS	Allows an application to read SMS messages
android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting
android.permission.RECEIVE_SMS	Allows an application to monitor incoming SMS messages, to record or perform processing on them
android.permission.SEND_SMS	Allows an application to send SMS messages
android.permission.WAKE_LOCK	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage

Used Permissions	Description	API calls
android.permission.SEND_SMS		android/telephony/SmsManager;->sendTextMessage
android.permission.WAKE_LOCK		android/os/PowerManager$WakeLock;->acquire
android.permission.ACCESS_FINE_LOCATION		android/location/LocationManager;->getBestProvider
android.permission.ACCESS_WIFI_STATE		android/net/wifi/WifiManager;->getConnectionInfo
android.permission.INTERNET		org/apache/http/impl/client/DefaultHttpClient
android.permission.VIBRATE °	Allows access to the vibrator	android/app/NotificationManager;->Notify
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getDeviceId
android.permission.ACCESS_NETWORK_STATE		android/net/ConnectivityManager;->getActiveNetworkInfo
android.permission.READ_CONTACTS °	Allows an application to read the user's contacts data	android/content/ContentResolver;->query

Used Intents
android.intent.action.BOOT_COMPLETED
android.intent.action.CREATE_SHORTCUT
android.intent.action.MAIN
android.intent.action.SEND_MESSAGE
android.intent.category.DEFAULT
android.intent.category.DEFAULT
android.intent.category.LAUNCHER

Native Libraries Loaded
/system/lib/libmedia_jni.so 0x0
/system/lib/libexif.so 0x0
/system/lib/libsoundpool.so 0x0
/system/lib/libwebcore.so 0x0

Activities	Used	Provided by Android	Provided by Third-Parties
com.mms.bg.ui.FakeLanucherActivity	✔	✔	✔
com.virsir.android.chinamobile10086.MainView	✔	✔	✘
com.virsir.android.chinamobile10086.PromotionView	✔	✔	✘
com.virsir.android.chinamobile10086.Root	✔	✔	✘
com.virsir.android.chinamobile10086.SearchOfficesView	✔	✔	✘
com.virsir.android.chinamobile10086.ShortCut	✔	✔	✔
com.virsir.android.chinamobile10086.news.News	✔	✔	✘
com.virsir.android.chinamobile10086.news.NewsBrowser	✔	✔	✘
com.virsir.android.chinamobile10086.news.NewsChannelSelector	✔	✔	✘
com.virsir.android.chinamobile10086.news.NewsDetails	✔	✔	✘

Services	Used	Provided by Android	Provided by Third-Parties
com.mms.bg.ui.BgService	✔	✔	✔
com.virsir.android.chinamobile10086.CheckUpdateService	✔	✔	✘
com.virsir.android.chinamobile10086.SMSService	✔	✔	✘
com.android.music.MediaPlaybackService	✔	✔	

Used Networks
-

Toast Messages
对不起，您的软件不支持电子市场
[Sorry, your software does not support the electronic market]

Receivers	Used	Provided by Android	Provided by Third-Parties
com.mms.bg.transaction.PrivilegedSmsReceiver	✔	✔	✔
com.mms.bg.transaction.SmsReceiver	✔	✔	✔
com.mms.bg.ui.AutoSMSRecevier	✔	✔	✔
com.mms.bg.ui.BootReceiver	✔	✔	✔
com.mms.bg.ui.InternetStatusReceiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
android.provider.Telephony.SMS_RECEIVED	✔		

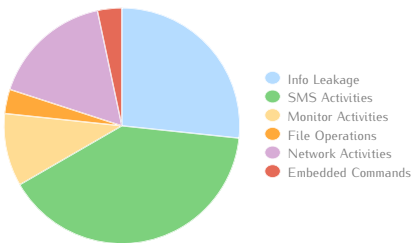
Network Analysis

Hardcoded URLs	IP	Region
gate.baidu.com	111.13.12.14	China - Beijing
maps.google.com	74.125.235.164	United States - Mountain View
ajax.googleapis.com	117.144.231.205	China - Beijing
tech.163.com	112.25.33.28	China - Beijing
schemas.android.com	-	-
data.flurry.com	117.144.231.200	China - Beijing
d.wiyun.com	119.254.87.201	China - Beijing
news.163.com	117.144.231.206	China - Beijing
apps.virsir.com	209.141.55.182	United States - San Jose
www.youlubg.com	59.188.232.71	Hong Kong
market.android.com	117.144.231.205	China - Beijing
www.androidicons.com	80.237.132.63	Germany - Höst
ent.163.com	112.25.33.28	China - Beijing
money.163.com	111.1.53.220	China - Beijing

Request	IP	Region	Type
data.flurry.com	74.217.75.7	United States - Seattle	HTTP POST / DNS
apps.virsir.com	209.141.55.182	United States / Canada	HTTP GET / DNS
d.wiyun.com	119.254.87.201	China - Beijing	HTTP GET / DNS
-	13.203.52.216.in-addr.arpa	United States - Norwalk	DNS
-	182.55.141.209.in-addr.arpa	Singapore	DNS
-	201.87.254.119.in-addr.arpa	Brasil	DNS
-	7.75.217.74.in-addr.arpa	United States - Columbus	DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	Call_Query	List phone call records
	Contact_Query	List contacts
	GPS_Get	Retrieve GPS information
	Location_Get	Retrieve current phone location
	Location_Last_Get	Retrieve last phone location
	Network_NetProvider_Get	Retrieve network provider information
	Phone_IMEI_Get	Retrieve IMEI
	SMS_Query	List SMS
SMS Activities	Contact_Erase	Delete contact
	Database_Erase	Delete database
	Notification_Send	Send notifications
	SMS_Analysis	Analysis SMS messages
	SMS_Delete_Message	Delete SMS Inbox
	SMS_Erase	Delete SMS
	SMS_Intercept	Intercept SMS
	SMS_Send	Send "1234567" to 10086 (5 times)
Monitor Activities	Database_Spy	Spy database
	GPS_Spy	Spy GPS state
	Location_SPY	Spy location
File Operations	File_Erase	Delete file
Network Activities	TAINT_IMEI	d.wiyun.com:80 (5 times)
Embedded Commands	unix-sleep	Suspend execution for a specified interval



Info Leakage	8
SMS Activities	12
Monitor Activities	3
File Operations	1
Network Activities	5
Embedded Commands	1

DroidDream Light A

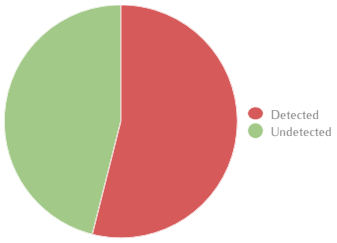
MD5	23fe7f0942667867fa14ddd7ac855e14
SHA-1	132f70936801d48da0677dedb09ef526ff1403ee
SHA-256	37c95029de50c52e3416b394e2feb27ac9e1fc11954ff87064e613f0c9917b33
API Level	8
File Dimension (MB)	0.18
Package Name	com.move.app2sd
Other Names	132f70936801d48da0677dedb09ef526ff1403ee
Used Features	android.hardware.screen.portrait android.hardware.telephony android.hardware.touchscreen

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.DDLight.D
Adobe Malware Classifier	
Aegislab	DorDrae
Agnitum	
AhnLab-V3	Android-Malicious/LightDD
ALYac	
Anchivia	
Antiy-AVL	
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Android:DorDrae-A [Trj]
AVG	Android_mc.IE
Avira	Android/Lightdd.A.Gen
AVware	Trojan.AndroidOS.DDLight.b
Baidu	Trojan.AndroidOS.DorDrae.aYm
BitDefender	Android.Trojan.DDLight.D
Bkav	
ByteHero	
ClamAV	Andr.Trojan.DroidDreamLight
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBL.23FE7F09!Olympus, AndroidOS/DroidDream.C
Digital Patrol	Trojan-Downloader.AndroidOS.DorDrae.cw
DrWeb	Android.DDLight.2.origin
EmsiSoft	Android.Trojan.DDLight.D (B)
Epoolsoft	
eScan	Android.Trojan.DDLight.D[ZP]
F-Mirc	
F-Prot	AndroidOS/DroidDream.C
F-Secure	Trojan:Android/DroidDream.gen!65232C
FileMedic	
FilsecLab Twister	Android.M.avhw
Fortinet	
GData	Android.Trojan.DDLight.D
GFI Vipre	Trojan.AndroidOS.DDLight.b
Ikarus	Trojan.AndroidOS.DorDrae, AndroidOS.Suspect.Manifest
Immunos	Andr.Trojan.DroidDreamLight
Jiangmin	TrojanDownloader.AndroidOS.ek
K7 Antivirus	
K7GW Antivirus	Trojan (0048d6381)
Kaspersky	HEUR:Trojan-Downloader.AndroidOS.DorDrae.a
Kingsoft	Android.Troj.DroidDream.cr.(kcloud), Android.Troj.DroidDream.b.(kcloud)
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!23FE7F094266
McAfee GW	
Microsoft	TrojanSpy:AndroidOS/DDLight.B
NANO AntiVirus	Trojan.Android.DDLight.cwhwqy
NOD32	Android/Lightdd.D
NoraLabs NoraScan	
Norman	
Norton Symantec	Android.Lightdd
nProtect	
OfficeMalScanner	

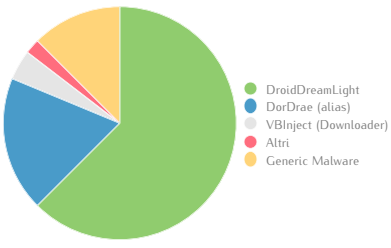
Antivirus	Result
Panda	
PathFinder	
Preventon	Andr/DDLight-A
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Android.LightDD.B
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Trojan.DDLight.D
Segurmatica	
Segurmatica KE	HEUR:Trojan-Downloader.AndroidOS.DorDrae.a
Solo	
Sophos	Andr/DDLight-A
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	
TotalDefense Cloud	Win32/VBInject!CFOFDe, Win32/VBInject!CCQFDe
Tencent	Win32.Trojan-Downloader.Dordrae.nqk
Trend Micro	ANDROIDOS_DDLIGHT.SMA, ANDROID.8DFEA8C4
Trend Micro-Housecall	ANDROIDOS_DDLIGHT.SMA
TrustPort	Android.Trojan.DDLight.D
TT Livescan	
VBA32	Trojan-Downloader.AndroidOS.DorDrae.cw
Vexira	
VirIT eXplorer	Android.Trj.DroidDream.T
VIRobot	Android.Trojan.DDLight.D[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.DDLight.SMA

Detected	48
Undetected	41
Sum	89



Name Distribution

Name	Amount	Score
DroidDreamLight	30	3
DorDrae (alias)	9	3
VBInject (Downloader)	2	0
Altri	1	1
Generic Malware	6	1
Sum	**48**	



Average Score	0,93

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.CLEAR_APP_CACHE	Allows an application to clear the caches of all installed applications on the device
android.permission.DELETE_CACHE_FILES	Allows an application to delete cache files
android.permission.GET_ACCOUNTS	Allows access to the list of accounts in the Accounts Service
android.permission.GET_PACKAGE_SIZE	Allows an application to find out the space used by any package
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_CONTACTS	Allows an application to read the user's contacts data
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.READ_SMS	Allows an application to read SMS messages
android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting
android.permission.VIBRATE	Allows access to the vibrator

Used Permissions	Description	API calls
android.permission.ACCESS_FINE_LOCATION °	Allows an app to access precise location from location sources such as GPS, cell towers, and WI-FI	android/telephony/TelephonyManager;->getCellLocation
android.permission.ACCESS_NETWORK_STATE		android/net/ConnectivityManager;->getActiveNetworkInfo
android.permission.FACTORY_TEST °	Run as a manufacturer test application, running as the root user	android/content/pm/ApplicationInfo/lflags
android.permission.GET_ACCOUNTS		android/accounts/AccountManager;->getAccounts
android.permission.INTERNET		android/webkit/WebView
android.permission.READ_CONTACTS		android/content/ContentResolver;->query
android.permission.READ_LOGS °	Allows an application to read the low-level system log files	java/lang/Runtime;->exec
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getDeviceId
android.permission.SEND_SMS		android/telephony/SmsManager;->sendMultipartTextMessage
android.permission.VIBRATE		android/app/NotificationManager;->Notify

Used Intents
android.intent.action.BOOT_COMPLETED
android.intent.action.MAIN
android.intent.action.PACKAGE_ADDED
android.intent.action.PACKAGE_CHANGED
android.intent.action.PACKAGE_REMOVED
android.intent.action.PACKAGE_REPLACED
android.intent.action.PHONE_STATE
android.intent.category.DEFAULT
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.google.ads.AdActivity	✗	✓	✗
com.move.app2sd.App2SdActivity	✓	✓	✗
com.move.app2sd.MainTab	✓	✓	✓
com.move.app2sd.Preferences	✓	✓	✗

Services	Used	Provided by Android	Provided by Third-Parties
com.move.app2sd.strategy.service.CelebrateService	✓	✓	✗
com.android.musicfx.Compatibility$Service	✓	✓	
com.android.vending.util.WorkService	✓	✓	
com.android.music.MediaPlaybackService	✓	✓	

Receivers	Used	Provided by Android	Provided by Third-Parties
com.move.app2sd.Receiver	✓	✓	✓
com.move.app2sd.strategy.core.RebirthReceiver	✓	✓	✓

Providers	Used	Provided by Android	Provided by Third-Parties
-			

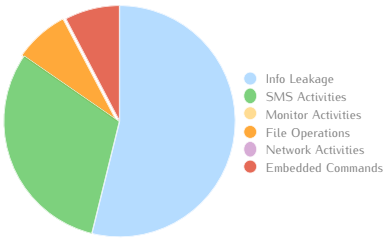
Used Networks
-

Network Analysis

Hardcoded URLs	IP	Region
sites.google.com	37.61.54.158	Azerbaigian - Baku
market.android.com	117.144.231.205	China - Beijing
www.googleadservices.com	203.208.36.13	China - Beijing
schemas.android.com	-	-
c.admob.com	203.208.46.186	China - Beijing
googleads.g.doubleclick.net	203.208.46.185	China - Beijing
www.gstatic.com	117.144.231.206	China - Beijing
a.admob.com	165.193.245.52	United States - Mountain View

Potentially Dangerous Operations

	Name	Description
Info Leakage	App_Info_Get	Retrieve package installation information
	Call_Query	List phone call records
	Contact_Query	List contacts
	Location_Get	Retrieve current phone location
	Phone_IMEI_Get	Retrieve IMEI
	Phone_IMSI_Get	Retrieve IMSI
	SMS_Query	List SMS
SMS Activities	Contact_Create	Create contact
	Notification_Send	Send notifications
	SMS_Create_Message	Create SMS Inbox
	SMS_Send	Send SMS
Monitor Activities	-	
File Operations	File_Erase	Delete file
Network Activities	-	
Embedded Commands	unix-sleep	Suspend execution for a specified interval



Info Leakage	7
SMS Activities	4
Monitor Activities	0
File Operations	1
Network Activities	0
Embedded Commands	1

DroidDream Light B

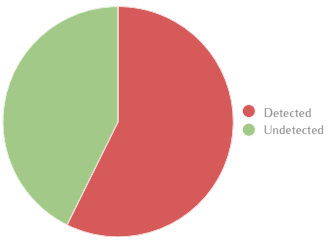
MD5	e6892f111d132efe5cb54a2cfc6a7c98
SHA-1	cd49c650889d7f06c4faf662218ff58e16d15ce4
SHA-256	ae7b91a971c3e3ba924f6930390b7016b7f95bb759be49a6221260c18784f62d
API Level	6
File Dimension (MB)	0.23
Package Name	com.lesson.share
Other Names	cd49c650889d7f06c4faf662218ff58e16d15ce4
Used Features	android.hardware.screen.portrait android.hardware.telephony android.hardware.touchscreen android.hardware.location android.hardware.location.gps android.hardware.location.network

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.DDLight.D
Adobe Malware Classifier	
Aegislab	DorDrae
Agnitum	
AhnLab-V3	Android-Malicious/LightDD
ALYac	
Anchivia	
Antiy-AVL	
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Android:DorDrae-A [Trj]
AVG	Android/Droiddrea *£, Android_mc.BCV *
Avira	Android/Lightdd.A.Gen
AVware	Trojan.AndroidOS.DDLight.b
Baidu	Trojan.AndroidOS.DorDrae.AGXT *
BitDefender	Android.Trojan.DDLight.D
Bkav	
ByteHero	
ClamAV	Andr.Lightdd *
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBLE6892F11!Olympus *, AndroidOS/DroidDream.C
Digital Patrol	Trojan-Downloader.AndroidOS.DorDrae.cw
DrWeb	Android.DDLight.2.origin
EmsiSoft	Android.Trojan.DDLight.D (B)
Epoolsoft	
eScan	Android.Trojan.DDLight.D[ZP]
F-Mirc	
F-Prot	AndroidOS/DroidDream.C
F-Secure	Trojan:Android/DroidDream.gen!65232C
FileMedic	
FilsecLab Twister	Android.M.vaij *
Fortinet	
GData	Android.Trojan.DDLight.D
GFI Vipre	Trojan.AndroidOS.DDLight.b
Ikarus	Trojan.AndroidOS.DorDrae, AndroidOS.Suspect.Manifest
Immunos	Andr.Trojan.DroidDreamLight
Jiangmin	TrojanDownloader.AndroidOS.y *
K7 Antivirus	
K7GW Antivirus	Trojan (0048d6381)
Kaspersky	HEUR:Trojan-Downloader.AndroidOS.DorDrae.a
Kingsoft	Android.Troj.DroidDream.b.(kcloud)
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!E6892F111D13 *
McAfee GW	
Microsoft	TrojanSpy:AndroidOS/DDLight.B
NANO AntiVirus	Trojan.Android.DDLight.cwhwqy
NOD32	Android/Lightdd.D, Android/Lightdd.B *
NoraLabs NoraScan	
Norman	*doslegacy/Suspicious_Gen2.SMFRN #*
Norton Symantec	Android.Lightdd
nProtect	
OfficeMalScanner	

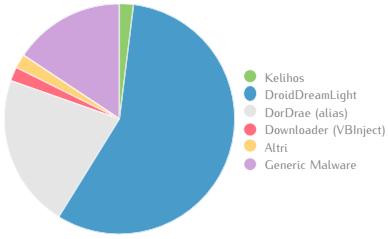
Antivirus	Result
Panda	
PathFinder	*Malware #*
Preventon	Andr/DDLight-A
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Android.LightDD.B
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Trojan.DDLight.D
Segurmatica	
Segurmatica KE	HEUR:Trojan-Downloader.AndroidOS.DorDrae.a
Solo	
Sophos	Andr/DDLight-A
SUPERAntiSpyware	
Team Cymru	*Malware #*
The Cleaner	
The Hacker	
TotalDefense	
TotalDefense Cloud	Win32/Kelihos!CPWMaAB *, Win32/Kelihos!CQaeZc *
Tencent	Dos.Trojan-downloader.Dordrae.Akov *
Trend Micro	AndroidOS_DORDRAE.N *, Android.F3EDE361
Trend Micro-Housecall	AndroidOS_DORDRAE.N *
TrustPort	Android.Trojan.DDLight.D
TT Livescan	
VBA32	Trojan-Downloader.AndroidOS.DorDrae.bp *
Vexira	
VirIT eXplorer	Android.Trj.DroidDream.AL *
VIRobot	Android.Trojan.DDLight.D[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.DDLight.SMA

Detected	51
Undetected	38
Sum	89



Name Distribution

Name	Amount	Score
Kelihos	1	0
DroidDreamLight	29	3
DorDrae (alias)	11	3
Downloader (VBInject)	1	0
Altri	1	1
Generic Malware	8	1
Sum	**51**	



Average Score	1,02

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_COARSE_LOCATION	Allows an app to access approximate location derived from network location sources such as cell towers and WI-FI
android.permission.ACCESS_FINE_LOCATION	Allows an app to access precise location from location sources such as GPS, cell towers, and WI-FI
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.GET_ACCOUNTS	Allows access to the list of accounts in the Accounts Service
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_CONTACTS	Allows an application to read the user's contacts data
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.READ_SMS	Allows an application to read SMS messages
android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting

Used Permissions	Description	API calls
android.permission.ACCESS_FINE_LOCATION		android/location/LocationManager;->isProviderEnabled
android.permission.ACCESS_NETWORK_STATE		android/net/ConnectivityManager;->getActiveNetworkInfo
android.permission.FACTORY_TEST °	Run as a manufacturer test application, running as the root user	android/content/pm/ApplicationInfo/lflags
android.permission.GET_ACCOUNTS		android/accounts/AccountManager;->getAccounts
android.permission.INTERNET		android/webkit/WebView
android.permission.READ_CONTACTS		android/content/ContentResolver;->query
android.permission.READ_LOGS °	Allows an application to read the low-level system log files	java/lang/Runtime;->exec
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getDeviceId
android.permission.SEND_SMS °	Allows an application to send SMS messages	android/telephony/SmsManager;->sendMultipartTextMessage
android.permission.VIBRATE °	Allows access to the vibrator	android/app/NotificationManager;->Notify

Used Intents
android.intent.action.BOOT_COMPLETED
android.intent.action.MAIN
android.intent.action.PACKAGE_ADDED
android.intent.action.PACKAGE_CHANGED
android.intent.action.PACKAGE_REMOVED
android.intent.action.PACKAGE_REPLACED
android.intent.action.PHONE_STATE
android.intent.category.DEFAULT
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.google.ads.AdActivity	✕	✔	✕
com.lesson.share.SuperShareActivity	✔	✔	✔
com.lesson.share.appshare.AppShareActivity	✔	✔	✕
com.lesson.share.contactsshare.ContactsShareActivity	✔	✔	✕
com.lesson.share.contactsshare.Preferences	✔	✔	✕
com.lesson.share.locationshare.Preferences	✔	✔	✕
com.lesson.share.locationshare.Sharelocation	✔	✔	✕
com.lesson.share.photoshare.PhotoShareActivity	✔	✔	✕

Services	Used	Provided by Android	Provided by Third-Parties
com.lesson.share.strategy.service.CelebrateService	✔	✔	✕
com.android.music.MediaPlaybackService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
com.lesson.share.appshare.Receiver	✔	✔	✔
com.lesson.share.strategy.core.RebirthReceiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
-			

Used Networks
-

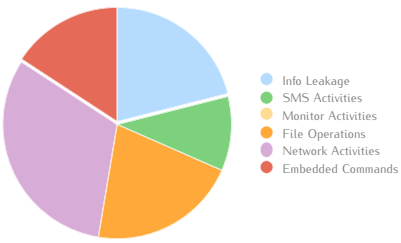
Network Analysis

Hardcoded URLs	IP	Region
c.admob.com	203.208.46.186	China - Beijing
market.android.com	117.144.231.205	China - Beijing
schemas.android.com	-	-
sites.google.com	37.61.54.158	Azerbagijan - Baku
a.admob.com	165.193.245.52	United States - Mountain View
googleads.g.doubleclick.net	203.208.46.185	China - Beijing
maps.google.com	74.125.235.164	United States - Mountain View
www.googleadservices.com	203.208.36.13	China - Beijing
www.gstatic.com	117.144.231.206	China - Beijing

Request	IP	Region	Type
juodaleety.com	69.43.161.174	Australia - Beaumaris	HTTP POST / DNS
guyeoacdoo.com	-	-	DNS
oucameyed.com	-	-	DNS
iuoytread.com	-	-	DNS
(oucameyed.com?)	208.73.211.161	United States - Los Angeles	HTTP POST
(oucameyed.com?)	208.73.211.236	United States - Los Angeles	HTTP POST
(oucameyed.com?)	209.99.40.222		HTTP POST

Potentially Dangerous Operations

	Name	Description
Info Leakage	App_Info_Get	Retrieve package installation information
	Call_Query	List phone call records
	Contact_Get	Get contact
	Contact_Query	List contacts
	Location_Get	Retrieve current phone location
	Phone_IMEI_Get	Retrieve IMEI
	Phone_IMSI_Get	Retrieve IMSI
	SMS_Query	List SMS
SMS Activities	Contact_Create	Create contact
	Notification_Send	Send notifications
	SMS_Create_Message	Create SMS Inbox
	SMS_Send	Send SMS
Monitor Activities	-	
File Operations	File_Erase	Delete file
	TAINT_SMS	/data/data/com.lesson.share/files/sms7 (3 times)
	TAINT_CALL_LOG	/data/data/com.lesson.share/files/calllog8 (4 times)
Network Activities	TAINT_IMEI, TAINT_IMSI	oucameyed.com:80 (12 times)
Embedded Commands	unix-gzip	Compress a file and add the extensi
	unix-kill	Terminate a process
	unix-login	Log in to the system
	unix-md	Make a directory
	unix-mkdir	Make a directory
	unix-sleep	Suspend execution for a specified interval



Info Leakage	8
SMS Activities	4
Monitor Activities	0
File Operations	8
Network Activities	12
Embedded Commands	6

DroidKungFu1 A

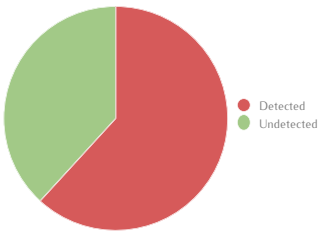
MD5	06dea6a4b6f77167eaf7a42cb9861bbe
SHA-1	25b55588a296a58191fd2daa6de2aab3951eb99d
SHA-256	5d3a915b34d0925b9ea4a7e33e8e70a428b22ce57cd17cfb20df37f463502b82
API Level	3
File Dimension (MB)	0.74
Package Name	com.tutusw.fingerscanner
Other Names	25b55588a296a58191fd2daa6de2aab3951eb99d
Used Features	android.hardware.screen.portrait android.hardware.wifi android.hardware.touchscreen

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.DroidKungFu.A
Adobe Malware Classifier	
Aegislab	DroidKungFu
Agnitum	
AhnLab-V3	Android-Malicious/KungFu
ALYac	
Anchivia	
Antiy-AVL	
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Other:Malware-gen [Trj], Android:KungFu-CP
AVG	Android_mc.GCS, Android/KungFu, Android_mc.QY
Avira	TR/Agent.44191, Android/DroidKungFu.A.Gen
AVware	Exploit.Linux.Generic.Elf, Trojan.AndroidOS.DroidK
Baidu	Backdoor.AndroidOS.KungFu.Az
BitDefender	Android.Trojan.DroidKungFu.A
Bkav	
ByteHero	
ClamAV	Andr.KungFu-10
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.E741A9BC!Olympus, AndroidOS/DroidKungFu.A, AndroidOS/DroidKungFu.O
Digital Patrol	Backdoor.AndroidOS.KungFu.a
DrWeb	Android.Gongfu.2
EmsiSoft	Android.Trojan.DroidKungFu.A (B)
Epoolsoft	
eScan	Android.Trojan.DroidKungFu.A[ZP]
F-Mirc	
F-Prot	AndroidOS/DroidKungFu.A
F-Secure	Trojan:Android/DroidKungFu.A
FileMedic	
FilsecLab Twister	Android.DroidKungFu.Y.alvo
Fortinet	Android/DroidKungFu.AW!tr.bdr
GData	Android.Trojan.DroidKungFu.A
GFI Vipre	Exploit.Linux.Generic.Elf
Ikarus	Trojan.AndroidOS.DroidKungFu, AndroidOS.Suspect.Manifest
Immunos	Andr.Trojan.DroidKungFu
Jiangmin	Backdoor/AndroidOS.k, Backdoor/AndroidOS.cy
K7 Antivirus	
K7GW Antivirus	Trojan (0048d55f1)
Kaspersky	HEUR:Backdoor.AndroidOS.KungFu.a
Kingsoft	Win32.Hack.AndroidOS.a.(kcloud), Android.Troj.Kongfu.op.(kcloud)
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!06DEA6A4B6F7
McAfee GW	
Microsoft	Trojan:AndroidOS/DroidKrungFu.A
NANO AntiVirus	Trojan.Android.KungFu.cvxvgh
NOD32	Android/DroidKungFu.W.Gen, Android/DroidKungFu.Y
NoraLabs NoraScan	
Norman	doslegacy/Suspicious_Gen3.AEOWP
Norton Symantec	Android.Fokonge
nProtect	
OfficeMalScanner	

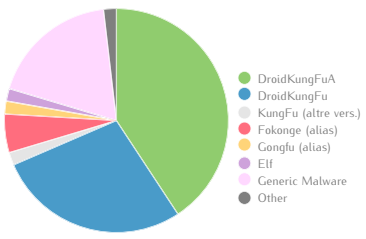
Antivirus	Result
Panda	Generic Malware
PathFinder	Malware
Preventon	Andr/KongFu-N, Andr/KongFu-A
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Exploit.Kongfu.N66, Android.Kungfu.A
RHBVS	
Rising	NORMAL:Trojan.Agent.fzv!1612479, DEX:System.Fokong
Rising Cloud	NORMAL:Trojan.Agent.fzv!1612479, DEX:System.Fokong
SecureIT	Android.Trojan.DroidKungFu.A
Segurmatica	
Segurmatica KE	HEUR:Backdoor.AndroidOS.KungFu.a
Solo	
Sophos	Andr/KongFu-N, Andr/KongFu-A
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	Kugfu.XAWM!suspicious
TotalDefense Cloud	Heur/Backdoor!CYLbBe, Heur/Backdoor!CVbHHW
Tencent	Trojan.Android.Agent.DF7F9E55
Trend Micro	ANDROIDOS_KUNGFU.HBT, ANDROID.8DFEA8C4
Trend Micro-Housecall	ANDROIDOS_KUNGFU.HBT
TrustPort	Android.Trojan.DroidKungFu.A
TT Livescan	
VBA32	Backdoor.AndroidOS.KungFu.a
Vexira	
VirIT eXplorer	Android.Trj.KungFu.AE
VIRobot	Android.Trojan.DroidKungFu.A[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.DroidKungFu.SMA

Detected	55
Undetected	34
Sum	89



Name Distribution

Name	Amount	Score
DroidKungFuA	22	3
DroidKungFu	15	3
KungFu (altre vers.)	1	2
Fokonge (alias)	3	3
Gongfu (alias)	1	3
Elf	1	1
Generic Malware	10	1
Other	1	1
Sum	**55**	



Average Score	1,16

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.ACCESS_WIFI_STATE	Allows applications to access information about WI-FI networks
android.permission.CHANGE_WIFI_STATE	Allows applications to change Wi-Fi connectivity state
android.permission.DISABLE_KEYGUARD	Allows applications to disable the keyguard
android.permission.INSTALL_PACKAGES	Allows an application to install packages
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting
android.permission.VIBRATE	Allows access to the vibrator
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage

Used Permissions	Description	API calls
android.permission.ACCESS_NETWORK_STATE		android/net/ConnectivityManager;->getNetworkInfo
android.permission.ACCESS_WIFI_STATE		android/net/wifi/WifiManager;->getWifiState
android.permission.CHANGE_WIFI_STATE		android/net/wifi/WifiManager;->setWifiEnabled
android.permission.DISABLE_KEYGUARD		android/app/KeyguardManager$KeyguardLock;->disableKeyguard
android.permission.INTERNET		java/net/HttpURLConnection
android.permission.READ_LOGS °	Allows an application to read the low-level system log files	java/lang/Runtime;->exec
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getDeviceId
android.permission.VIBRATE		android/os/Vibrator;->vibrate
android.permission.WAKE_LOCK °	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming	android/media/MediaPlayer;->start

Used Intents
android.intent.action.BATTERY_CHANGED_ACTION
android.intent.action.BOOT_COMPLETED
android.intent.action.MAIN
android.intent.action.SIG_STR
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.google.ssearch.Dialog	✔	✔	✘
com.tutusw.fingerscanner.FingerprintActivity	✔	✔	✘
com.tutusw.fingerscanner.HelpActivity	✔	✔	✘
com.tutusw.fingerscanner.SettingsActivity	✔	✔	✔

Services	Used	Provided by Android	Provided by Third-Parties
com.google.ssearch.SearchService	✔	✔	✘
com.tutusw.fingerscanner.SleepService	✔	✔	✘
com.android.vending.util.WorkService	✔	✔	
com.android.music.MediaPlaybackService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
com.google.ssearch.Receiver	✔	✔	✔
com.tutusw.fingerscanner.BootReceiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
-			

Used Networks
-

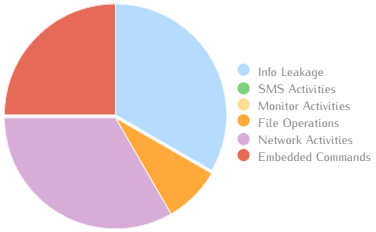
Network Analysis

Hardcoded URLs	IP	Region
android.thinkchange.mobi	205.196.221.2	United States - Brea
search.gongfu-android.com	62.173.145.83	Russian Federation
schemas.android.com	-	-

Request	IP	Region	Type
android.clients.google.com	173.194.116.167	United States - Mountain View	HTTP POST / DNS
-	163.116.194.173.in-addr.arpa	France	DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	App_Info_Get	Retrieve package installation information (2 times)
	Phone_IMEI_Get	Retrieve IMEI
	Phone_Number_Get	Retrieve current phone number
SMS Activities	-	
Monitor Activities	-	
File Operations	OS_Kill	Terminate a process
Network Activities	Network_Access	Access network (4 times)
Embedded Commands	unix-mkdir	Make a directory
	unix-sleep	Suspend execution for a specified interval
	unix-su	Set super-user mode



Info Leakage	4
SMS Activities	0
Monitor Activities	0
File Operations	1
Network Activities	4
Embedded Commands	3

DroidKungFu1 B

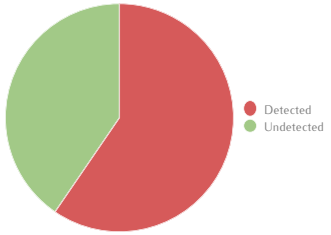
MD5	b34c011a87746ed07a57afe96a819212
SHA-1	a80bdca60dee7d6e6284647eb6a62b045020da0c
SHA-256	aebb5050f17588f0d3936b1b13bf7dcd856a7acd8db107c4853e7a9058d2a0ca
API Level	3
File Dimension (MB)	0.25
Package Name	com.tutusw.phonespeedup
Other Names	a80bdca60dee7d6e6284647eb6a62b045020da0c
Used Features	android.hardware.screen.portrait android.hardware.wifi android.hardware.touchscreen

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.DroidKungFu.A
Adobe Malware Classifier	
Aegislab	DroidKungFu
Agnitum	
AhnLab-V3	Android-Malicious/KungFu
ALYac	
Anchivia	
Antiy-AVL	
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Other:Malware-gen [Trj], Android:KungFu-CP
AVG	Sexy *, Android/KungFu, Android_mc.QY
Avira	TR/Agent.44191, Android/DroidKungFu.A.Gen
AVware	Exploit.Linux.Generic.Elf, Trojan.AndroidOS.DroidK
Baidu	Backdoor.AndroidOS.KungFu.Az
BitDefender	Android.Trojan.DroidKungFu.A
Bkav	
ByteHero	
ClamAV	Andr.KungFu-10
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.E741A9BC!Olympus, AndroidOS/DroidKungFu.A, AndroidOS/DroidKungFu.E *
Digital Patrol	Backdoor.AndroidOS.KungFu.a
DrWeb	Android.Gongfu.2
EmsiSoft	Android.Trojan.DroidKungFu.A (B)
Epoolsoft	
eScan	Android.Trojan.DroidKungFu.A[ZP]
F-Mirc	
F-Prot	AndroidOS/DroidKungFu.A
F-Secure	Trojan:Android/DroidKungFu.C *
FileMedic	
FilsecLab Twister	Android.DroidKungFu.Y.alvo
Fortinet	Android/DroidKungFu.AW!tr.bdr
GData	Android.Trojan.DroidKungFu.A
GFI Vipre	Exploit.Linux.Generic.Elf
Ikarus	Trojan.AndroidOS.DroidKungFu, Backdoor.AndroidOS.KungFu *, AndroidOS.DroidKungFu *
Immunos	Andr.Trojan.DroidKungFu
Jiangmin	Backdoor/AndroidOS.k, Backdoor/AndroidOS.gt *
K7 Antivirus	
K7GW Antivirus	Trojan (0048d55f1)
Kaspersky	HEUR:Backdoor.AndroidOS.KungFu.a
Kingsoft	Win32.Troj.KungFu.re.(kcloud) *, Android.Troj.Kongfu.op.(kcloud)
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!B34C011A8774 *
McAfee GW	
Microsoft	Trojan:AndroidOS/DroidKrungFu.A
NANO AntiVirus	Trojan.Android.KungFu.cvxvgh
NOD32	Android/DroidKungFu.W.Gen, Android/DroidKungFu.Y
NoraLabs NoraScan	
Norman	doslegacy/Suspicious_Gen3.AEOWP
Norton Symantec	Android.Fokonge
nProtect	
OfficeMalScanner	

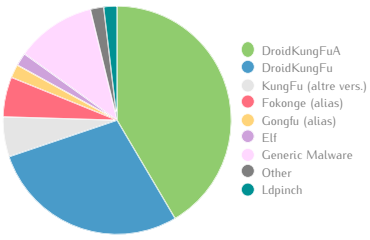
Antivirus	Result
Panda	*NO MALWARE $*
PathFinder	*NO MALWARE $*
Preventon	Andr/KongFu-N, Andr/KongFu-A
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Exploit.Kongfu.N66, Android.Kungfu.A
RHBVS	
Rising	NORMAL:Trojan.Agent.fzv!1612479, DEX:System.Fokong
Rising Cloud	NORMAL:Trojan.Agent.fzv!1612479, DEX:System.Fokong
SecureIT	Android.Trojan.DroidKungFu.A
Segurmatica	
Segurmatica KE	HEUR:Backdoor.AndroidOS.KungFu.a
Solo	
Sophos	Andr/KongFu-N, Andr/KongFu-A
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	Kugfu.XAWM!suspicious
TotalDefense Cloud	Win32/Ldpinch!CdaLPFB *, Heur/Backdoor!CVbHHW
Tencent	Dos.Backdoor.Kungfu.Pdce *
Trend Micro	AndroidOS_DroidKungFu.SMA *, Android.92C878B9 *
Trend Micro-Housecall	AndroidOS_DroidKungFu.SMA *, Android.92C878B9 *
TrustPort	Android.Trojan.DroidKungFu.A
TT Livescan	
VBA32	Backdoor.AndroidOS.KungFu.a
Vexira	
VirIT eXplorer	Android.Trj.KungFu.AE
VIRobot	Android.Trojan.DroidKungFu.A[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.DroidKungFu.SMA

Detected	53
Undetected	36
Sum	89



Name Distribution

Name	Amount	Score
DroidKungFuA	22	3
DroidKungFu	15	3
KungFu (altre vers.)	3	2
Fokonge (alias)	3	3
Gongfu (alias)	1	3
Elf	1	1
Generic Malware	6	1
Other	1	1
Ldpinch	1	0
Sum	**53**	



Average Score	1,13

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.ACCESS_WIFI_STATE	Allows applications to access information about WI-FI networks
android.permission.CHANGE_WIFI_STATE	Allows applications to change Wi-Fi connectivity state
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting
android.permission.VIBRATE	Allows access to the vibrator
android.permission.WAKE_LOCK	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage

Used Permissions	Description	API calls
android.permission.ACCESS_NETWORK_STATE		android/net/ConnectivityManager;->getNetworkInfo
android.permission.ACCESS_WIFI_STATE		android/net/wifi/WifiManager;->getWifiState
android.permission.CHANGE_WIFI_STATE		android/net/wifi/WifiManager;->setWifiEnabled
android.permission.INTERNET		java/net/HttpURLConnection
android.permission.READ_LOGS °	Allows an application to read the low-level system log files	java/lang/Runtime;->exec
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getDeviceId
android.permission.VIBRATE		android/app/NotificationManager;->notify
android.permission.WAKE_LOCK		android/os/PowerManager$WakeLock;->release

Used Intents
android.intent.action.BATTERY_CHANGED_ACTION
android.intent.action.BOOT_COMPLETED
android.intent.action.MAIN
android.intent.action.SIG_STR
android.intent.category.LAUNCHER
Speedup.intent.action.updatewidget

Activities	Used	Provided by Android	Provided by Third-Parties
com.google.ssearch.Dialog	✔	✔	✘
com.tutusw.phonespeedup.AboutActivity	✔	✔	✘
com.tutusw.phonespeedup.AdvancedActivity	✔	✔	✘
com.tutusw.phonespeedup.Home	✔	✔	✘
com.tutusw.phonespeedup.InfoActivity	✔	✔	✘
com.tutusw.phonespeedup.IntroActivity	✔	✔	✔
com.tutusw.phonespeedup.PerflockActivity	✘	✔	✘
com.tutusw.phonespeedup.ProfileEditActivity	✘	✔	✘
com.tutusw.phonespeedup.ProfilesActivity	✔	✔	✘
com.tutusw.phonespeedup.Setcpu	✘	✔	✘
com.tutusw.phonespeedup.StresstestActivity	✔	✔	✘
com.tutusw.phonespeedup.WidgetConfigActivity	✔	✔	✔

Services	Used	Provided by Android	Provided by Third-Parties
com.google.ssearch.SearchService	✔	✔	✘
com.tutusw.phonespeedup.ProfilesService	✔	✔	✘
com.tutusw.phonespeedup.StartupService	✔	✔	✘
com.tutusw.phonespeedup.WidgetService	✔	✔	✘

Receivers	Used	Provided by Android	Provided by Third-Parties
com.google.ssearch.Receiver	✔	✔	✔
com.tutusw.phonespeedup.StartupReceiver	✔	✔	✘
com.tutusw.phonespeedup.Widget	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
android.appwidget.provider	✔		

Used Networks
-

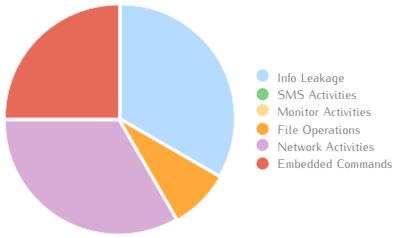
Network Analysis

Hardcoded URLs	IP	Region
android.thinkchange.mobi	205.196.221.2	United States - Brea
search.gongfu-android.com	62.173.145.83	Russian Federation
schemas.android.com	-	-

Request	IP	Region	Type
android.clients.google.com	173.194.116.163	United States - Mountain View	HTTP POST / DNS
-	163.116.194.173.in-addr.arpa	France	DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	App_Info_Get	Retrieve package installation information (2 times)
	Phone_IMEI_Get	Retrieve IMEI
	Phone_Number_Get	Retrieve current phone number
SMS Activities	-	
Monitor Activities	-	
File Operations	OS_Kill	Terminate a process
Network Activities	Network_Access	Access network (4 times)
Embedded Commands	unix-mkdir	Make a directory
	unix-sleep	Suspend execution for a specified interval
	unix-su	Set super-user mode



Info Leakage	4
SMS Activities	0
Monitor Activities	0
File Operations	1
Network Activities	4
Embedded Commands	3

DroidKungFu2 A

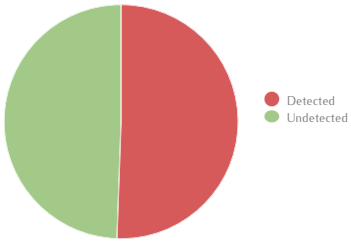
MD5	4247a3b9ae9896ded35f61d1279b7b2e
SHA-1	057694b62bfd6a488f3db80454bbd48bf84f68e7
SHA-256	30866091584856ac8a7f353172c3d9b0643602f351be56ba92b4ab2dfd68230d
API Level	3
File Dimension (MB)	1.04
Package Name	com.tutusw.onekeyvpn
Other Names	057694b62bfd6a488f3db80454bbd48bf84f68e7
Used Features	android.hardware.touchscreen

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.DroidKungFu.C
Adobe Malware Classifier	
Aegislab	DroidKungFu
Agnitum	
AhnLab-V3	Android-Malicious/KungFu
ALYac	
Anchivia	
Antiy-AVL	
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	ELF:KungFu-C [Trj], Android:DroidKungFu-F
AVG	Android_c.BRH
Avira	TR/Agent.18316, Android/DroidKungFu.E.Gen
AVware	Trojan.AndroidOS.DroidKungFu.a
Baidu	Backdoor.AndroidOS.KungFu.aob
BitDefender	Android.Trojan.DroidKungFu.C
Bkav	
ByteHero	
ClamAV	
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	ELF/Andr/KungFu.A, AndroidOS/DroidKungFu.B
Digital Patrol	
DrWeb	Android.Gongfu.12
EmsiSoft	Android.Trojan.DroidKungFu.C (B)
Epoolsoft	
eScan	Android.Trojan.DroidKungFu.C[ZP]
F-Mirc	
F-Prot	ELF/Andr/KungFu.A
F-Secure	Trojan:Android/DroidKungFu.Q
FileMedic	
FilsecLab Twister	Android.DroidKungFu.F.hfhc, Android.M.gmkm
Fortinet	Android/DroidKungFu.AW!tr.bdr
GData	Android.Trojan.DroidKungFu.C
GFI Vipre	Trojan.AndroidOS.DroidKungFu.a
Ikarus	Trojan.AndroidOS.DroidKungFu, Backdoor.AndroidOS.KungFu
Immunos	
Jiangmin	Backdoor/AndroidOS.aar, Backdoor/AndroidOS.wha
K7 Antivirus	
K7GW Antivirus	Trojan (0048d5541)
Kaspersky	Backdoor.AndroidOS.KungFu.hb
Kingsoft	Troj.KillAll.a.(kcloud), Android.Troj.hh_KungFu.a.(kcloud)
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!4247A3B9AE98
McAfee GW	
Microsoft	Trojan:Linux/DroidKrungFu
NANO AntiVirus	Trojan.Android.KungFu.cvxvgh
NOD32	Android/DroidKungFu.F, Android/DroidKungFu.K
NoraLabs NoraScan	
Norman	
Norton Symantec	Android.Gonfu
nProtect	
OfficeMalScanner	

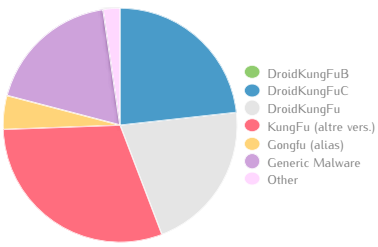
Antivirus	Result
Panda	
PathFinder	
Preventon	Andr/KongFu-A
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Exploit.DroidKungFu.C5, Android.Kungfu.C
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Trojan.DroidKungFu.C
Segurmatica	
Segurmatica KE	HEUR:Backdoor.AndroidOS.KungFu.hb
Solo	
Sophos	Andr/KongFu-N, Andr/KongFu-A
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	
TotalDefense Cloud	Heur/Backdoor!CVLZXY
Tencent	Dos.Backdoor.Kungfu.Pabv
Trend Micro	AndroidOS_DROIDKUNGFU.B, Android.8E8C2A0A
Trend Micro-Housecall	Suspicious_GEN.F47V1201
TrustPort	Android.Trojan.DroidKungFu.C
TT Livescan	
VBA32	
Vexira	
VirIT eXplorer	Android.Trj.KungFu.IJ
VIRobot	
VirusBuster	
Zillya!	Trojan.DroidKungFu..1
Zoner Antivirus	Trojan.AndroidOS.DroidKungFu.C

Detected	45
Undetected	44
Sum	89



Name Distribution

Name	Amount	Score
DroidKungFuB	2	3
DroidKungFuC	10	3
DroidKungFu	9	3
KungFu (altre vers.)	13	2
Gongfu (alias)	2	3
Generic Malware	8	1
Other	1	1
Sum	**45**	



Average Score	0,67

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.BROADCAST_STICKY	Allows an application to broadcast sticky intents
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_PHONE_STATE	Allows read only access to phone state

Used Permissions	Description	API calls
android.permission.INTERNET		java/net/Socket
android.permission.READ_LOGS °	Allows an application to read the low-level system log files	java/lang/Runtime;->exec
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getDeviceId
android.permission.VIBRATE °	Allows access to the vibrator	android/app/NotificationManager;->notify

Used Intents
android.intent.action.BOOT_COMPLETED
android.intent.action.MAIN
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.tutusw.onekeyvpn.AdvancedSettings	✔	✔	✘
com.tutusw.onekeyvpn.EditConfig	✔	✔	✘
com.tutusw.onekeyvpn.EditConfigPreferences	✔	✔	✘
com.tutusw.onekeyvpn.EnterPassphrase	✔	✔	✘
com.tutusw.onekeyvpn.EnterUserPassword	✔	✔	✘
com.tutusw.onekeyvpn.ImportFiles	✔	✔	✘
com.tutusw.onekeyvpn.OpenVpnSettings	✔	✔	✔

Services	Used	Provided by Android	Provided by Third-Parties
com.tutusw.onekeyvpn.service.OpenVpnService	✘	✔	✘
com.android.vending.util.WorkService	✔	✔	
com.android.music.MediaPlaybackService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
com.tutusw.onekeyvpn.util.BootCompletedReceiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
-			

Used Networks
-

Toast Messages
You need to install 'OI File Manager' from the market!
No directory selected!
Selected directory does not exists!
Selected file must be a directory!
VPN DNS is only supported in one tunnel!
您的手机不符合本软件运行的要求，您需要先root您的手机！您可以选择z4root、Androot Universal、visionaryplus等软件进行root！ [Your phone does not meet the requirements to run this software, you need to root your phone! You can choose z4root, Androot Universal, visionaryplus or other software]

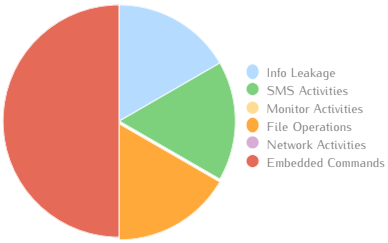
Network Analysis

Hardcoded URLs	IP	Region
schemas.android.com	-	-

Request	IP	Region	Type
android.clients.google.com	173.194.116.160	United States - Mountain View	HTTP POST / DNS
-	160.116.194.173.in-addr.arpa	South Africa	DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	Phone_IMEI_Get	Retrieve IMEI
SMS Activities	Notification_Send	Send notifications
Monitor Activities	-	
File Operations	File_Erase	Delete file
Network Activities	-	
Embedded Commands	unix-mkdir	Make a directory
	unix-sleep	Suspend execution for a specified interval
	unix-su	Set super-user mode



Info Leakage	1
SMS Activities	1
Monitor Activities	0
File Operations	1
Network Activities	0
Embedded Commands	3

DroidKungFu2 B

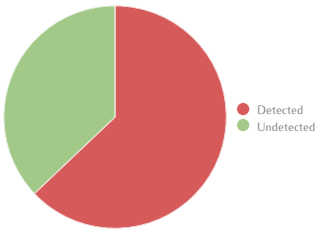
MD5	fd92a299dd5e574d0d21d13856e9b988
SHA-1	f30c4058f1e6cb46f81d21b263cf3545463827 5a
SHA-256	fe98a9b6d1acf4e2b52caf0015e90b9fab856b0c0aa581d526f3d2951b2f7904
API Level	3
File Dimension (MB)	0.70
Package Name	com.tutusw.fingerscanner
Other Names	f30c4058f1e6cb46f81d21b263cf35454638275a, fe98a9b6d1acf4e2b52caf0015e90b9fab856b0c0aa581d526f3d2951b2f7904
Used Features	android.hardware.screen.portrait android.hardware.wifi android.hardware.touchscreen

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.DroidKungFu.L *^
Adobe Malware Classifier	
Aegislab	DroidKungFu
Agnitum	***Backdoor.AndroidOS.KungFu.B #***
AhnLab-V3	Android-Malicious/KungFu
ALYac	
Anchivia	
Antiy-AVL	***Backdoor/AndroidOS.KungFu, #*** ***Exploit/Linux.Lotoor #***
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	ELF:KungFu-C, ELF:Lootor-E *, ELF:KungFu-A *
AVG	Sexy *
Avira	Android/Malmix2.3 *, EXP/Linux.Lotoor.P *
AVware	Trojan.AndroidOS.DroidKungFu.a
Baidu	Backdoor.AndroidOS.KungFu.Ap *
BitDefender	Android.Trojan.DroidKungFu.L *^
Bkav	
ByteHero	
ClamAV	***Andr.KungFu-8 #***
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.FD92A299!Olympus *, AndroidOS/DroidKungFu.A *^
Digital Patrol	***Backdoor.AndroidOS.KungFu.a #***
DrWeb	Android.Gongfu.6 *, Android.Gongfu.8 *
EmsiSoft	Android.Trojan.DroidKungFu.L *^ (B)
Epoolsoft	
eScan	Android.Trojan.DroidKungFu.L *^ [ZP]
F-Mirc	
F-Prot	AndroidOS/DroidKungFu.A *
F-Secure	Trojan:Android/DroidKungFu.A *
FileMedic	
FilsecLab Twister	Expli.Linux.Lotoor.x.uqtc *, Android.DroidKungFu.C.t *£
Fortinet	Android/DroidKungFu.AW!tr.bdr, Android/DroidKungFu.B!tr *£
GData	Android.Trojan.DroidKungFu.L *^
GFI Vipre	Trojan.AndroidOS.DroidKungFu.a
Ikarus	Trojan.AndroidOS.DroidKungFu Backdoor.AndroidOS.KungFu,
Immunos	***Andr.KungFu-8 #***
Jiangmin	Backdoor/AndroidOS.hd *, Exploit.Linux.ao *
K7 Antivirus	
K7GW Antivirus	Trojan (0048d55f1) *
Kaspersky	Backdoor.AndroidOS.KungFu.z *
Kingsoft	Android.Troj.KillAll.b.(kcloud) *
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!FD92A299DD5E *, Artemis!2D782F81C83D *
McAfee GW	
Microsoft	Trojan:Linux/DroidKrungFu.A *^
NANO AntiVirus	Trojan.Android.KungFu.cvxvgj *£
NOD32	Android/DroidKungFu.C *£, Android/DroidKungFu.X.Gen *
NoraLabs NoraScan	
Norman	
Norton Symantec	Android.Gonfu
nProtect	
OfficeMalScanner	

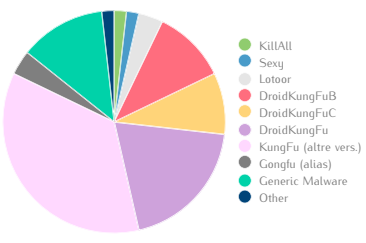
Antivirus	Result
Panda	
PathFinder	
Preventon	Andr/KongFu-A
Protector Plus	***Backdoor.AndroidOS.KungFu.B #***
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Exploit.DroidKungFu.C3 *, Exploit.Lotoor.C29 *
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Trojan.DroidKungFu.L *^
Segurmatica	
Segurmatica KE	Backdoor.AndroidOS.KungFu.z *
Solo	
Sophos	Andr/KongFu-A
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	***Kugfu.XAWM!suspicious #,*** ***AndroidOS/KungFu #***
TotalDefense Cloud	Heur/Backdoor!CKYTWFB *, Heur/Backdoor!CcCRNY *
Tencent	Dos.Backdoor.Kungfu.Egny *
Trend Micro	ANDROIDOS_KUNGFU.HATA *, Android.8E8C2A0A
Trend Micro-Housecall	ANDROIDOS_KUNGFU.HATA *£
TrustPort	Android.Exploit.Exploid.G *^
TT Livescan	
VBA32	***Backdoor.AndroidOS.KungFu.a #***
Vexira	***Backdoor.AndroidOS.KungFu.B #***
VirIT eXplorer	Exploit.Linux.Lotoor.X *
VIRobot	***Android.Trojan.DroidKungFu.B[b] #,*** ***Trojan.Linux.A.EX-Lotoor.7032 #***
VirusBuster	***Backdoor.AndroidOS.KungFu.B #***
Zillya!	Trojan.DroidKungFu..6 *
Zoner Antivirus	Trojan.AndroidOS.DroidKungFu.A *^

Detected	56
Undetected	33
Sum	89



Name Distribution

Name	Amount	Score
KillAll	1	0
Sexy	1	0
Lotoor	2	0
DroidKungFuB	6	3
DroidKungFuC	5	3
DroidKungFu	11	3
KungFu (altre vers.)	20	2
Gongfu (alias)	2	3
Generic Malware	7	1
Other	1	1
Sum	**56**	



Average Score	0,98

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_WIFI_STATE	Allows applications to access information about WI-FI networks
android.permission.CHANGE_WIFI_STATE	Allows applications to change Wi-Fi connectivity state
android.permission.DISABLE_KEYGUARD	Allows applications to disable the keyguard
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting
android.permission.VIBRATE	Allows access to the vibrator

Used Permissions	Description	API calls
android.permission.ACCESS_WIFI_STATE		android/net/wifi/WifiManager;->getWifiState
android.permission.CHANGE_WIFI_STATE		android/net/wifi/WifiManager;->setWifiEnabled
android.permission.DISABLE_KEYGUARD		android/app/KeyguardManager$KeyguardLock;->disableKeyguard
android.permission.INTERNET		java/net/HttpURLConnection
android.permission.READ_LOGS °	Allows an application to read the low-level system log files	java/lang/Runtime;->exec
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getDeviceId
android.permission.VIBRATE		android/os/Vibrator;->vibrate
android.permission.WAKE_LOCK °	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming	android/media/MediaPlayer;->start

Used Intents
android.intent.action.BATTERY_CHANGED_ACTION
android.intent.action.BOOT_COMPLETED
android.intent.action.MAIN
android.intent.action.SIG_STR
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.eguan.state.Dialog	✔	✔	✘
com.tutusw.fingerscanner.FingerprintActivity	✔	✔	✘
com.tutusw.fingerscanner.HelpActivity	✔	✔	✘
com.tutusw.fingerscanner.SettingsActivity	✔	✔	✔

Services	Used	Provided by Android	Provided by Third-Parties
com.eguan.state.StateService	✔	✔	✘
com.tutusw.fingerscanner.SleepService	✔	✔	✘
com.android.vending.util.WorkService	✔	✔	
com.android.music.MediaPlaybackService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
com.eguan.state.Receiver	✔	✔	✔
com.tutusw.fingerscanner.BootReceiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
-			

Used Networks
-

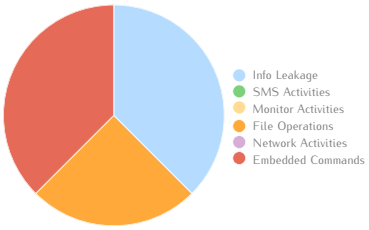
Network Analysis

Hardcoded URLs	IP	Region
android.thinkchange.mobi	205.196.221.2	United States - Brea
schemas.android.com	-	-

Request	IP	Region	Type
android.clients.google.com	173.194.116.168	-	HTTP POST / DNS
-	168.116.194.173.in-addr.arpa	United States - Hightstown	DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	App_Info_Get	Retrieve package installation information
	Phone_IMEI_Get	Retrieve IMEI
	Phone_Number_Get	Retrieve current phone number
SMS Activities	-	
Monitor Activities	-	
File Operations	File_Erase	Delete file
	OS_Kill	Terminate a process
Network Activities	-	
Embedded Commands	unix-mkdir	Make a directory
	unix-sleep	Suspend execution for a specified interval
	unix-su	Set super-user mode



Info Leakage	3
SMS Activities	0
Monitor Activities	0
File Operations	2
Network Activities	0
Embedded Commands	3

DroidKungFu3 A

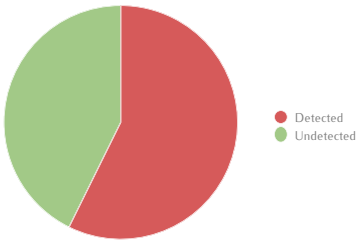
MD5	5520fec164f45396dc0831a5e20623ab
SHA-1	5d81e5ded988b406ac71578d5cf885600b72c23f
SHA-256	f3f52121296119ff32c334075ea80b74495fde648a7204bed66268b285fbf199
API Level	3
File Dimension (MB)	0.35
Package Name	com.gp.tiltmazes
Other Names	5d81e5ded988b406ac71578d5cf885600b72c23f
Used Features	

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.DroidKungFu.D
Adobe Malware Classifier	
Aegislab	DroidKungFu
Agnitum	
AhnLab-V3	Android-Malicious/KungFu
ALYac	
Anchivia	
Antiy-AVL	
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Android:Fokonge-C [Trj]
AVG	Android_mc.AFF
Avira	Android/DroidKungFu.A.Gen, Android/KungFu.cp.5
AVware	Trojan.AndroidOS.DroidKungFu.c
Baidu	Backdoor.AndroidOS.KungFu.ao
BitDefender	Android.Trojan.DroidKungFu.D
Bkav	
ByteHero	
ClamAV	Andr.Trojan.DroidKungFu
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.5520FEC1!Olympus, AndroidOS/AdrAds.A
Digital Patrol	
DrWeb	Android.Gongfu.2.origin
EmsiSoft	Android.Trojan.DroidKungFu.D (B)
Epoolsoft	
eScan	Android.Trojan.DroidKungFu.A[ZP], Android.Trojan.DroidKungFu.D
F-Mirc	
F-Prot	AndroidOS/AdrAds.A
F-Secure	Trojan:Android/DroidKungFu.gen!65232C
FileMedic	
FilsecLab Twister	Android.M.uell
Fortinet	Adware/Domob.A
GData	Android.Trojan.DroidKungFu.D
GFI Vipre	Trojan.AndroidOS.DroidKungFu.a
Ikarus	Trojan.AndroidOS.DroidKungFu, Backdoor.AndroidOS.KungFu, AndroidOS.Suspect.Manifest
Immunos	Andr.Trojan.DroidKungFu
Jiangmin	Backdoor/AndroidOS.il
K7 Antivirus	
K7GW Antivirus	Trojan (0001140e1)
Kaspersky	HEUR:Backdoor.AndroidOS.KungFu.a
Kingsoft	Android.Troj.KillAll.b.(kcloud), Android.Troj.Kongfu.op.(kcloud)
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!5520FEC164F4
McAfee GW	
Microsoft	Trojan:Linux/DroidKrungFu.C
NANO AntiVirus	Riskware.Android.Wooboo.cthjxd, Trojan.Android.WqM
NOD32	Android/DroidKungFu.G, Android/DroidKungFu.R.Gen
NoraLabs NoraScan	
Norman	doslegacy/Suspicious_Gen2.TMOQA
Norton Symantec	Android.Fokonge
nProtect	
OfficeMalScanner	

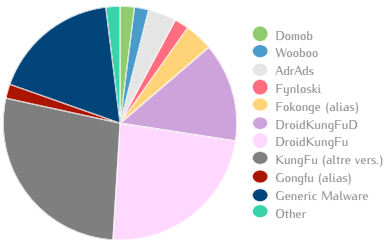
Antivirus	Result
Panda	
PathFinder	Malware
Preventon	Andr/KongFu-A
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Android.Kungfu.C
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Trojan.DroidKungFu.D
Segurmatica	
Segurmatica KE	HEUR:Backdoor.AndroidOS.KungFu.a
Solo	
Sophos	Andr/KongFu-A
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	
TotalDefense Cloud	Win32/Fynloski!COKEKf, Heur/Backdoor!CCWZAe
Tencent	Dos.Backdoor.Kungfu.Stka
Trend Micro	ANDROIDOS_KUNGFU.HBT, ANDROID.8249BCED
Trend Micro-Housecall	ANDROIDOS_KUNGFU.HBT
TrustPort	Android.Trojan.DroidKungFu.A
TT Livescan	
VBA32	Backdoor.AndroidOS.KungFu.fa
Vexira	
VirIT eXplorer	Android.Trj.KungFu.AJ
VIRobot	Android.Trojan.DroidKungFu.D[b]
VirusBuster	
Zillya!	Trojan.DroidKungFu..7
Zoner Antivirus	Trojan.AndroidOS.DroidKungFu.SMA

Detected	51
Undetected	38
Sum	89



Name Distribution

Name	Amount	Score
Domob	1	2
Wooboo	1	0
AdrAds	2	0
Fynloski	1	0
Fokonge (alias)	2	3
DroidKungFuD	7	3
DroidKungFu	12	3
KungFu (altre vers.)	14	2
Gongfu (alias)	1	2
Generic Malware	9	1
Other	1	1
Sum	**51**	



Average Score	0,75

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_FINE_LOCATION	Allows an app to access precise location from location sources such as GPS, cell towers, and WI-FI
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	Allows an application to access extra location provider commands
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.ACCESS_WIFI_STATE	Allows applications to access information about WI-FI networks
android.permission.CHANGE_WIFI_STATE	Allows applications to change Wi-Fi connectivity state
android.permission.GET_TASKS	This constant was deprecated in API level 21
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_EXTERNAL_STORAGE	Allows an application to read from external storage
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting
android.permission.VIBRATE	Allows access to the vibrator
android.permission.WAKE_LOCK	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage

Used Permissions	Description	API calls
android.permission.ACCESS_FINE_LOCATION		android/location/LocationManager;->getBestProvider
android.permission.ACCESS_NETWORK_STATE		android/net/ConnectivityManager;->getActiveNetworkInfo
android.permission.ACCESS_WIFI_STATE		android/net/wifi/WifiManager;->getWifiState
android.permission.CHANGE_WIFI_STATE		android/net/wifi/WifiManager;->setWifiEnabled
android.permission.FACTORY_TEST °	Run as a manufacturer test application, running as the root user	android/content/pm/ApplicationInfo/Iflags
android.permission.GET_TASKS		android/app/ActivityManager;->getRunningTasks
android.permission.INTERNET		java/net/Socket
android.permission.READ_CONTACTS °	Allows an application to read the user's contacts data	android/content/ContentResolver;->query
android.permission.READ_LOGS °	Allows an application to read the low-level system log files	java/lang/Runtime;->exec
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getDeviceId
android.permission.VIBRATE		android/app/NotificationManager;->notify
android.permission.WAKE_LOCK		android/os/PowerManager$WakeLock;->acquire

Used Intents
android.intent.action.BATTERY_CHANGED_ACTION
android.intent.action.BOOT_COMPLETED
android.intent.action.MAIN
android.intent.action.SIG_STR
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
cn.domob.android.ads.DomobActivity	✔	✔	✘
com.adwo.adsdk.AdwoAdBrowserActivity	✘	✔	✘
com.google.update.Dialog	✔	✔	✘
com.gp.tiltmazes.SelectMazeActivity	✘	✔	✘
com.gp.tiltmazes.TiltMazesActivity	✘	✔	✔
com.waps.OffersWebView	✘	✔	✘

Services	Used	Provided by Android	Provided by Third-Parties
com.google.update.UpdateService	✔	✔	✘
com.android.vending.util.WorkService	✔	✔	
com.android.music.MediaPlaybackService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
ccom.google.update.Receiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
-			

Used Networks
-

Toast Messages	
开始下载	[Start download]
正在下载,请稍候...	[Loading, please wait]
正在准备下载,请稍候...	[Preparing to download, please wait]
加载中,请稍候...	[Loading, please wait]

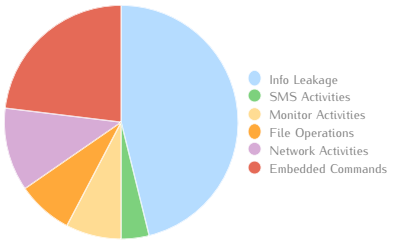
Network Analysis

Hardcoded URLs	IP	Region
clk.adsmogo.com	115.182.31.7	China - Beijing
r2.adwo.com	42.62.76.8	China - Beijing
imp.adsmogo.com	115.182.31.7	China - Beijing
www.adwo.com	42.62.76.6	China - Beijing
www.adsmogo.com	115.182.31.10	China - Beijing
blk.adsmogo.com	115.182.31.7	China - Beijing
cus.adsmogo.com	115.182.31.7	China - Beijing
app.wapx.cn	219.234.85.220	China - Beijing
e.domob.cn	58.83.143.20	China - Beijing
r.domob.cn	58.83.143.24	China - Beijing
maps.google.com	74.125.235.164	United States - Mountain View
ads.wapx.cn	117.144.231.205	China - Beijing
cfg.adsmogo.com	115.182.31.2	China - Beijing
cfg.adsmogo.com	117.144.231.202	China - Beijing
req.adsmogo.com	117.144.231.206	China - Beijing
market.android.com	117.144.231.205	China - Beijing
schemas.android.com	-	-

Request	IP	Region	Type
cfg.adsmogo.com	115.182.31.7	China - Beijing	HTTP GET / DNS
app.wapx.cn	219.234.85.238	China - Beijing	HTTP GET / DNS
ads.wapx.cn	219.234.85.236	China - Beijing	HTTP POST / DNS
code.google.com	74.125.237.5	United States - Mountain View	HTTP GET / DNS
-	2.31.182.115.in-addr.arpa	United Kingdom	DNS
-	243.85.234.219.in-addr.arpa	-	DNS
android.clients.google.com	173.194.116.166	United States - Mountain View	HTTP POST / DNS
-	166.116.194.173.in-addr.arpa	United States - Kingsport	DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	App_Get_Tasks	Retrieve running task information
	App_Info_Get	Retrieve package installation information
	Call_Query	List phone call records
	Contact_Query	List contacts
	GPS_Get	Retrieve GPS information
	Location_Get	Retrieve current phone location
	Location_Last_Get	Retrieve last phone location
	Network_Provider_Get	Retrieve network provider information
	Phone_IMEI_Get	Retrieve IMEI
	Phone_IMSI_Get	Retrieve IMSI
	Phone_Number_Get	Retrieve current phone number
	SMS_Query	List SMS
SMS Activities	Notification_Send	Send notifications
Monitor Activities	GPS_Spy	Spy GPS states
	Location_Spy	Spy location
File Operations	File_Erase	Delete file
	OS_Kill	Terminate a process
Network Activities	TAINT_IMEI, TAINT_IMSI	app.wapx:80 (3 times)
Embedded Commands	unix-compress	Compress a file
	unix-gzip	Compress a file and add the extension .gz
	unix-md	Make a directory
	unix-mkdir	Make a directory
	unix-sleep	Suspend execution for a specified interval
	unix-su	Set super-user mode



Info Leakage	12
SMS Activities	1
Monitor Activities	2
File Operations	2
Network Activities	3
Embedded Commands	6

DroidKungFu3 B

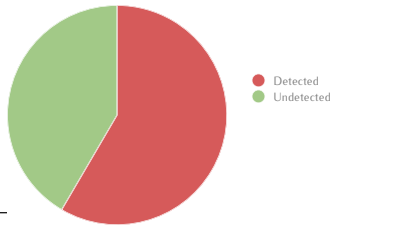
MD5	8344c2cd2a36840b4123a0b1939b03d7
SHA-1	411c2363b4847aa1ce073a3a6c3a07d9bdbe03f3
SHA-256	5b8d52abe9fa8e849a89cf87f90cb07e77bb429e0fe5f518873c8b26ee231a87
API Level	7
File Dimension (MB)	0.58
Package Name	com.mogo.gongfupuzzle
Other Names	411c2363b4847aa1ce073a3a6c3a07d9bdbe03f3
Used Features	android.hardware.location android.hardware.location.gps android.hardware.location.network android.hardware.wifi android.hardware.telephony android.hardware.touchscreen android.hardware.screen.portrait

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.DroidKungFu.D
Adobe Malware Classifier	
Aegislab	DroidKungFu
Agnitum	
AhnLab-V3	Android-Malicious/KungFu
ALYac	
Anchivia	
Antiy-AVL	
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Android:Fokonge-C [Trj]
AVG	Android/KungFu *£, Android/Kungf *
Avira	Android/DroidKungFu.A.Gen, Android/KungFu.cz.1 *
AVware	Trojan.AndroidOS.DroidKungFu.c
Baidu	Backdoor.AndroidOS.KungFu.aLh *, Backdoor.AndroidOS.KungFu.AjX *
BitDefender	Android.Trojan.DroidKungFu.D
Bkav	
ByteHero	
ClamAV	Andr.Trojan.DroidKungFu
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.8344C2CD!Olympus *, AndroidOS/AdrAds.A
Digital Patrol	
DrWeb	Android.Gongfu.2.origin
EmsiSoft	Android.Trojan.DroidKungFu.D (B)
Epoolsoft	
eScan	Android.Trojan.DroidKungFu.A[ZP], Android.Trojan.DroidKungFu.D
F-Mirc	
F-Prot	AndroidOS/AdrAds.A
F-Secure	Android.Trojan.DroidKungFu.D *
FileMedic	
FilsecLab Twister	Android.M.hfib *
Fortinet	Adware/Waps.G *, Android/DroidKungFu.AW!tr.bdr *
Gdata	Android.Trojan.DroidKungFu.D
GFI Vipre	Trojan.AndroidOS.DroidKungFu.c *
Ikarus	Trojan.AndroidOS.DroidKungFu, Backdoor.AndroidOS.KungFu
Immunos	Andr.Trojan.DroidKungFu
Jiangmin	Backdoor/AndroidOS.sm
K7 Antivirus	
K7GW Antivirus	Trojan (0048d5431) *
Kaspersky	HEUR:Backdoor.AndroidOS.KungFu.a
Kingsoft	Android.Troj.KillAll.b.(kcloud), Android.Troj.Kongfu.op.(kcloud)
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!8344C2CD2A36 *
McAfee GW	
Microsoft	***NO MALWARE $***
NANO AntiVirus	Riskware.Android.Wooboo.cthjxd, Trojan.Android.WqM
NOD32	Android/DroidKungFu.G, Android/DroidKungFu.AB.Gen *
NoraLabs NoraScan	
Norman	doslegacy/Suspicious_Gen2.TMOQA
Norton Symantec	Trojan.Gen.2 *^
nProtect	
OfficeMalScanner	

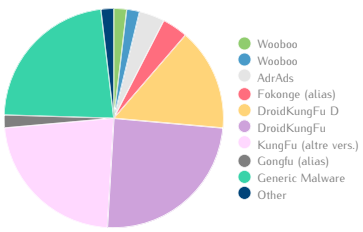
Antivirus	Result
Panda	
PathFinder	Malware
Preventon	Andr/KongFu-B *
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Android.Kungfu.C
RHBVS	
Rising	***DEX:System.Fokonge!1.9DA8 #***
Rising Cloud	
SecureIT	Android.Trojan.DroidKungFu.D
Segurmatica	
Segurmatica KE	HEUR:Backdoor.AndroidOS.KungFu.a
Solo	
Sophos	Andr/KongFu-B *
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	***AndroidOS/KungFu #, Kugfu.XAVN!suspicious #***
TotalDefense Cloud	Heur/Backdoor!CRYJPFB *, Heur/Backdoor!CeUYbc *
Tencent	Trojan.Android.Agent.649ED9F3 *^
Trend Micro	ANDROIDOS_KUNGFU.HATA *, ANDROID.DDA41826 *
Trend Micro-Housecall	Suspicious_GEN.F47V0105 *^
TrustPort	Android.Trojan.DroidKungFu.A
TT Livescan	
VBA32	Backdoor.AndroidOS.KungFu.fa, Backdoor.AndroidOS.KungFu.a *
Vexira	
VirIT eXplorer	Android.Trj.KungFu.FW *
VIRobot	Android.Trojan.DroidKungFu.D[b]
VirusBuster	
Zillya!	Trojan.DroidKungFu..5 *
Zoner Antivirus	Trojan.AndroidOS.DroidKungFu.SMA

Detected	52
Undetected	37
Sum	89



Name Distribution

Name	Amount	Score
Wooboo	1	0
AdrAds	2	0
Fokonge (alias)	2	3
DroidKungFu D	8	3
DroidKungFu	13	3
KungFu (altre vers.)	12	2
Gongfu (alias)	1	3
Generic Malware	12	1
Other	1	1
Sum	**52**	



Average Score	0,81

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_COARSE_LOCATION	Allows an app to access approximate location derived from network location sources such as cell towers and WI-FI
android.permission.ACCESS_FINE_LOCATION	Allows an app to access precise location from location sources such as GPS, cell towers, and WI-FI
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	Allows an application to access extra location provider commands
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.ACCESS_WIFI_STATE	Allows applications to access information about WI-FI networks
android.permission.CHANGE_WIFI_STATE	Allows applications to change Wi-Fi connectivity state
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_EXTERNAL_STORAGE	Allows an application to read from external storage
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.READ_SMS	Allows an application to read SMS messages
android.permission.VIBRATE	Allows access to the vibrator
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage
android.permission.WRITE_SMS	Allows an application to write SMS messages

Used Permissions	Description	API calls
android.permission.ACCESS_FINE_LOCATION		android/location/LocationManager;->getLastKnownLocation
android.permission.ACCESS_NETWORK_STATE		android/net/ConnectivityManager;->getActiveNetworkInfo
android.permission.ACCESS_WIFI_STATE		android/net/wifi/WifiManager;->getWifiState
android.permission.CHANGE_WIFI_STATE		android/net/wifi/WifiManager;->setWifiEnabled
android.permission.GET_TASKS °	This constant was deprecated in API level 21	android/app/ActivityManager;->getRunningTasks
android.permission.INTERNET		android/webkit/WebView
android.permission.READ_CONTACTS °	Allows an application to read the user's contacts data	android/content/ContentResolver;->query
android.permission.READ_LOGS °	Allows an application to read the low-level system log files	java/lang/Runtime;->exec
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getDeviceId
android.permission.VIBRATE		android/app/NotificationManager;->notify

Used Intents
android.intent.action.BATTERY_CHANGED_ACTION
android.intent.action.BOOT_COMPLETED
android.intent.action.MAIN
android.intent.action.SIG_STR
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.adwo.adsdk.AdwoAdBrowserActivity	✔	✔	✘
com.adwo.adsdk.AdwoSplashAdActivity	✔	✔	✘
com.google.ads.AdActivity	✘	✔	✘
com.google.update.Dialog	✔	✔	✘
com.mogo.gongfupuzzle.Main	✔	✔	✘
com.mogo.gongfupuzzle.begin	✔	✔	✔
com.vpon.adon.android.WebInApp	✘	✔	✘
com.waps.OffersWebView	✘	✔	✘

Services	Used	Provided by Android	Provided by Third-Parties
com.google.update.UpdateService	✔	✔	✘
com.android.vending.util.WorkService	✔	✔	
com.android.music.MediaPlaybackService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
ccom.google.update.Receiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
-			

Used Networks
-

Toast Messages	
加载中,请稍候...	[Loading, please wait]
正在下载,请稍候...	[Loading, please wait]
正在加载	[Loading]

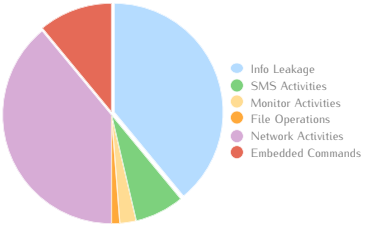
Network Analysis

Request	IP	Region	Type
cfg.adsmogo.com	115.182.31.7	China - Beijing	HTTP GET / DNS
app.waps.cn	219.234.85.220	China - Beijing	HTTP GET / DNS
cus.adsmogo.com	115.182.31.7	China - Beijing	HTTP GET / DNS
ads.waps.cn	219.234.85.237	China - Beijing	HTTP POST / DNS
appcdn.wapx.cn	61.156.157.181	China - Jinan	HTTP GET / DNS
appcdn.wapx.cn	60.221.236.138	China - Taiyuan	HTTP GET / DNS
app.wapx.cn	219.234.85.238	China - Beijing	HTTP GET / DNS
-	2.31.182.115.in-addr.arpa	United Kingdom	DNS
-	243.85.234.219.in-addr.arpa	-	DNS
android.clients.google.com	173.194.116.168	United States - Mountain View	HTTP POST / DNS
imgcdn.wapx.cn	101.226.200.182	China - Shanghai	HTTP GET / DNS
storage.adsmogo.com	119.188.139.105	China - Jinan	HTTP GET
cus.adsmogo.com	115.182.31.2	China - Beijing	HTTP GET

Hardcoded URLs	IP	Region
app.waps.cn	219.234.85.243	China - Beijing
ditu.google.cn	117.144.231.200	China - Beijing
ditu.google.com	74.125.235.161	United States - Mountain View
imp.adsmogo.com	115.182.31.7	China - Beijing
ads.waps.cn	117.144.231.205	China - Beijing
blk.adsmogo.com	115.182.31.7	China - Beijing
www.adwo.com	42.62.76.6	China - Beijing
maps.google.com	74.125.235.164	United States - Mountain View
schemas.android.com	-	-
cus.adsmogo.com	115.182.31.7	China - Beijing
gad.ju6666.com	-	-
clk.adsmogo.com	115.182.31.7	China - Beijing
r2.adwo.com	42.62.76.8	China - Beijing
tw.ad.adon.vpon.com	202.153.194.26	Taiwan
sites.google.com	37.61.54.158	Azerbaigian - Baku
googleads.g.doubleclick.net	203.208.46.185	China - Beijing
a.admob.com	165.193.245.52	United States - Mountain View
219.234.85.214	219.234.85.214	China - Beijing
c.admob.com	203.208.46.186	China - Beijing
maps.google	-	-
beta.vpon.com	114.34.173.45	Taiwan - Taipei
www.gstatic.com	117.144.231.206	China - Beijing
req.adsmogo.com	117.144.231.206	China - Beijing
www.googleadservices.com	203.208.36.13	China - Beijing
www.youtube.com	203.98.7.65	New Zeland - Waikanae
cn.ad.adon.vpon.com	114.80.83.204	China - Shanghai
cfg.adsmogo.com	117.144.231.202	China - Beijing
www.vpon.com	202.153.194.29	Taiwan
www.adsmogo.com	115.182.31.10	China - Beijing
market.android.com	117.144.231.205	China - Beijing

Potentially Dangerous Operations

	Name	Description
Info Leakage	App_Get_Tasks	Retrieve running task information
	App_Info_Get	Retrieve package installation information (3 times)
	Call_Query	List phone call records (3 times)
	GPS_Get	Retrieve GPS information (4 times)
	Location_Get	Retrieve current phone location (5 times)
	Location_Last_Get	Retrieve last phone location
	Network_Provider_Get	Retrieve network provider information (3 times)
	Phone_IMEI_Get	Retrieve IMEI (7 times)
	Phone_IMSI_Get	Retrieve IMSI (2 times)
	Phone_Number_Get	Retrieve current phone number (3 times)
SMS Activities	Contact_Create	Create contact
	Notification_Send	Send notifications
	SMS_Create_Message	Create SMS Inbox
	SMS_Query	List SMS (3 times)
Monitor Activities	GPS_Spy	Spy GPS states
	Location_Spy	Spy location
File Operations	OS_Kill	Terminate a process
Network Activities	Network_Access	Access network (18 times)
	TAINT_IMEI	app.waps.cn:80 or alias (14 times)
Embedded Commands	unix-compress	Compress a file
	unix-cp	Copy a file
	unix-diff	Display line-by-line differences between pairs of text files
	unix-gzip	Compress a file and add the extension .gz
	unix-kill	Terminate a process
	unix-md	Make a directory
	unix-mkdir	Make a directory
	unix-sleep	Suspend execution for a specified interval
	unix-su	Set super-user mode



Info Leakage	32
SMS Activities	6
Monitor Activities	2
File Operations	1
Network Activities	32
Embedded Commands	9

DroidKungFu4 A

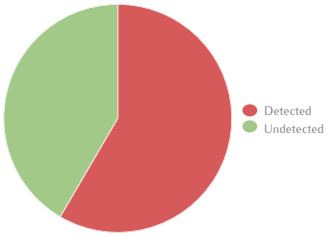
MD5	ebdb48da292198c0ebf4126f474ade0a
SHA-1	9fc39c43012cd921bbcbf042a504cda995a1d366
SHA-256	85043f962aad210bec8ba35266e3e9b8852eeeb38bd839bb4ca036488b79882a
API Level	3
File Dimension (MB)	0.23
Package Name	com.safetest.myapn
Other Names	9fc39c43012cd921bbcbf042a504cda995a1d366
Used Features	android.hardware.location android.hardware.location.network android.hardware.wifi android.hardware.telephony android.hardware.touchscreen

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.DroidKungFu.F
Adobe Malware Classifier	
Aegislab	DroidKungFu
Agnitum	
AhnLab-V3	Android-Malicious/KungFu
ALYac	
Anchivia	
Antiy-AVL	
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Other:Malware-gen, Android:KungFu-L
AVG	Android_mc.AQV
Avira	Android/Malmix.952, Android/DroidKungFu.D.Gen
AVware	Trojan.AndroidOS.DroidKungFu.e
Baidu	Backdoor.AndroidOS.KungFu.Auv
BitDefender	Android.Trojan.DroidKungFu.F
Bkav	
ByteHero	
ClamAV	Andr.Trojan.DroidKungFu
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.EBDB48DA!Olympus, AndroidOS/AdrAds.A
Digital Patrol	Backdoor.AndroidOS.KungFu.a
DrWeb	Android.Gongfu.3.origin
EmsiSoft	Android.Trojan.DroidKungFu.F (B)
Epoolsoft	
eScan	Android.Trojan.DroidKungFu.C[ZP], Android.Trojan.DroidKungFu.F
F-Mirc	
F-Prot	AndroidOS/AdrAds.A
F-Secure	Trojan:Android/DroidKungFu.L
FileMedic	
FilsecLab Twister	Android.M.bvre
Fortinet	Adware/Adswo.KK, Android/DroidKungFu.D
GData	Android.Trojan.DroidKungFu.F
GFI Vipre	Trojan.AndroidOS.DroidKungFu.e
Ikarus	Trojan.AndroidOS.DroidKungFu, Backdoor.AndroidOS.KungFu, AndroidOS.Suspect.Manifest
Immunos	Andr.Trojan.DroidKungFu
Jiangmin	Backdoor/AndroidOS.ys
K7 Antivirus	
K7GW Antivirus	Trojan (000001021)
Kaspersky	HEUR:Backdoor.AndroidOS.KungFu.a
Kingsoft	Android.Troj.KillAll.a.(kcloud), Android.Troj.Kongfu.op.(kcloud)
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!EBDB48DA2921
McAfee GW	
Microsoft	Trojan:AndroidOS/Legana.A
NANO AntiVirus	Riskware.Android.Wooboo.cthjxd, Trojan.Android.WqM
NOD32	Android/DroidKungFu.M.Gen, Android/DroidKungFu.M
NoraLabs NoraScan	
Norman	
Norton Symantec	Trojan.Gen.2
nProtect	
OfficeMalScanner	

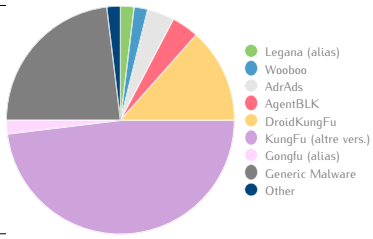
Antivirus	Result
Panda	
PathFinder	Malware
Preventon	Andr/KongFu-A
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Android.Kungfu.F
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Trojan.DroidKungFu.F
Segurmatica	
Segurmatica KE	HEUR:Backdoor.AndroidOS.KungFu.a
Solo	
Sophos	Andr/KongFu-A
SUPERAntiSpyware	
Team Cymru	Malware
The Cleaner	
The Hacker	
TotalDefense	Kugfu.XAVN!suspicious, AndroidOS/MalAndroid
TotalDefense Cloud	Heur/Backdoor!CedHEHB, Heur/TrojanHorse!CDeHEHB
Tencent	Trojan.Android.Agent.A6ECF066
Trend Micro	AndroidOS_AGENTBLK.135, Android.ADCC7A0C
Trend Micro-Housecall	AndroidOS_AGENTBLK.135
TrustPort	Android.Trojan.DroidKungFu.C
TT Livescan	
VBA32	Backdoor.AndroidOS.KungFu.a
Vexira	
VirIT eXplorer	Android.Trj.KungFu.GY
VIRobot	Android.Trojan.DroidKungFu.F[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.DroidKungFu.C

Detected	52
Undetected	37
Sum	89



Name Distribution

Name	Amount	Score
Legana (alias)	1	3
Wooboo	1	0
AdrAds	2	0
AgentBLK	2	0
DroidKungFu	7	3
KungFu (altre vers.)	25	2
Gongfu (alias)	1	3
Generic Malware	12	1
Other	1	1
Sum	**52**	



Average Score	0,60

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_COARSE_LOCATION	Allows an app to access approximate location derived from network location sources such as cell towers and WI-FI
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.ACCESS_WIFI_STATE	Allows applications to access information about WI-FI networks
android.permission.CHANGE_NETWORK_STATE	Allows applications to change network connectivity state
android.permission.CHANGE_WIFI_STATE	Allows applications to change Wi-Fi connectivity state
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.READ_SMS	Allows an application to read SMS messages
android.permission.WAKE_LOCK	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming
android.permission.WRITE_APN_SETTINGS	Allows applications to write the apn settings
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage
android.permission.WRITE_SMS	Allows an application to write SMS messages

Used Permissions	Description	API calls
android.permission.ACCESS_FINE_LOCATION		android/location/LocationManager;->getLastKnownLocation
android.permission.ACCESS_NETWORK_STATE		android/net/ConnectivityManager;->getActiveNetworkInfo
android.permission.ACCESS_WIFI_STATE		android/net/wifi/WifiManager;->getConnectionInfo
android.permission.CHANGE_WIFI_STATE		android/net/wifi/WifiManager;->setWifiEnabled
android.permission.FACTORY_TEST °	Run as a manufacturer test application, running as the root user	android/content/pm/ApplicationInfo/lflags
android.permission.INTERNET		java/net/NetworkInterface
android.permission.READ_CONTACTS °	Allows an application to read the user's contacts data	android/content/ContentResolver;->query
android.permission.READ_LOGS °	Allows an application to read the low-level system log files	java/lang/Runtime;->exec
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getDeviceId
android.permission.VIBRATE °	Allows access to the vibrator	android/app/NotificationManager;->notify
com.android.browser.permission.READ_HISTORY_BOOKMARKS °	Allows an application to read (but not write) the user's browsing history and bookmarks	android/provider/Browser;->getAllVisitedUrls

Used Intents
android.intent.action.BATTERY_CHANGED_ACTION
android.intent.action.BOOT_COMPLETED
android.intent.action.MAIN
android.intent.action.SIG_STR
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.adwo.adsdk.AdwoAdBrowserActivity	✕	✔	✕
com.safetest.common.app.ActivationActivity	✕	✔	✕
com.safetest.myapn.HelpActivity	✕	✔	✕
com.safetest.myapn.InitialActivity	✔	✔	✔
com.safetest.myapn.PreferenceActivity	✕	✔	✕
com.safetest.myapn.ShowTips	✔	✔	✕

Services	Used	Provided by Android	Provided by Third-Parties
com.google.update.UpdateService	✔	✔	✕
com.android.vending.util.WorkService	✔	✔	
com.android.music.MediaPlaybackService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
com.safetest.myapn.HiApnRotaterWidgetProvider	✕	✔	✔
com.safetest.myapn.HiApnSwitcherWidgetProvider	✕	✔	✔
com.safetest.myapn.HiApnWidgetProvider	✕	✔	✔
com.safetest.myapn.Receiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
android.appwidget.provider	✔	✔	

Used Networks
android.net.conn.CONNECTIVITY_CHANGE
android.net.wifi.WIFI_STATE_CHANGED

Toast Messages	
low_memory	
无备份文件	[No backup file]
您未选中任何运营商	[You have not selected any operator]

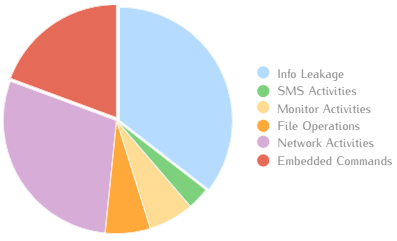
Network Analysis

Hardcoded URLs	IP	Region
market.android.com	117.144.231.205	China - Beijing
maps.google.com	74.125.235.164	United States - Mountain View
www.adwo.com	42.62.76.6	China - Beijing
www.hidroid.net	115.182.0.81	China - Beijing
proxy.youdraw.cn	114.255.171.253	China - Beijing
schemas.android.com	-	-
bbs.hidroid.net	115.182.0.81	China - Beijing
gad.ju6666.com	-	-
r2.adwo.com	42.62.76.8	China - Beijing

Request	IP	Region	Type
proxy.youdraw.cn	118.26.192.171	China - Beijing	HTTP POST / DNS
r2.adwo.com	42.62.76.8	China - Beijing	HTTP POST
r2.adwo.com	114.255.171.253	China - Beijing	HTTP POST / DNS
android.clients.google.com	173.194.116.164	United States - Mountain View	HTTP POST / DNS
-	164.116.194.173.in-addr.arpa	United States - Kent	DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	App_Get_Tasks	Retrieve running task information
	App_Info_Get	Retrieve package installation information
	Call_Query	List phone call records
	Contact_Query	List contacts
	GPS_Get	Retrieve GPS information
	Location_Get	Retrieve current phone location
	Location_Last_Get	Retrieve last phone location
	Network_Provider_Get	Retrieve network provider information
	Phone_IMEI_Get	Retrieve IMEI
	Phone_IMSI_Get	Retrieve IMSI
	Phone_Number_Get	Retrieve current phone number
	SMS_Query	List SMS
SMS Activities	Notification_Send	Send notifications
Monitor Activities	GPS_Spy	Spy GPS states
	Location_Spy	Spy location
File Operations	File_Erase	Delete file
	OS_Kill	Terminate a process
Network Activities	TAINT_PHONE_NUMBER, TAINT_IMEI	r2.adwo.com:80 (9 times)
Embedded Commands	unix-compress	Compress a file
	unix-gzip	Compress a file and add the extension .gz
	unix-md	Make a directory
	unix-mkdir	Make a directory
	unix-sleep	Suspend execution for a specified interval
	unix-su	Set super-user mode



Info Leakage	11
SMS Activities	1
Monitor Activities	2
File Operations	2
Network Activities	9
Embedded Commands	6

DroidKungFu4 B

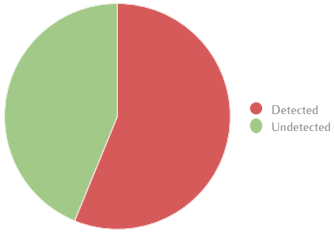
MD5	5c1f2f86c4e3c72267f6afd28a681de3
SHA-1	7237c992c69e4bd2ccb6e8a79bd87d90eb3fb37b
SHA-256	51bfb82709e927d65770e5c59ab6eb96b73b19525e127f60a25831cd2b8aee82
API Level	1
File Dimension (MB)	3.34
Package Name	com.glu.android.dinercn
Other Names	7237c992c69e4bd2ccb6e8a79bd87d90eb3fb37b
Used Features	android.hardware.location android.hardware.location.network android.hardware.wifi android.hardware.telephony android.hardware.touchscreen android.hardware.screen.landscape

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.DroidKungFu.F
Adobe Malware Classifier	
Aegislab	DroidKungFu
Agnitum	
AhnLab-V3	Android-Malicious/KungFu
ALYac	
Anchivia	
Antiy-AVL	
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Other:Malware-gen, Android:KungFu-GR *
AVG	Android_mc.A *, Android/AdWo
Avira	Android/Malmix.952, Android/DroidKungFu.D.Gen
AVware	Trojan.AndroidOS.DroidKungFu.e
Baidu	*NO MALWARE $*
BitDefender	Android.Trojan.DroidKungFu.F
Bkav	
ByteHero	
ClamAV	Andr.Trojan.DroidKungFu
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.5C1F2F86!Olympus *, AndroidOS/AdrAds.A
Digital Patrol	*NO MALWARE $*
DrWeb	Android.Gongfu.3.origin
EmsiSoft	Android.Trojan.DroidKungFu.F (B)
Epoolsoft	
eScan	Android.Trojan.DroidKungFu.C[ZP], Android.Trojan.DroidKungFu.F
F-Mirc	
F-Prot	AndroidOS/AdrAds.A
F-Secure	Trojan:Android/DroidKungFu.L
FileMedic	
FilsecLab Twister	Android.M.vwkc *
Fortinet	Adware/Adswo.KK, Android/DroidKungFu.D
GData	Android.Trojan.DroidKungFu.F
GFI Vipre	Trojan.AndroidOS.DroidKungFu.e
Ikarus	Trojan.AndroidOS.DroidKungFu
Immunos	Andr.Trojan.DroidKungFu
Jiangmin	Backdoor/AndroidOS.bqk *
K7 Antivirus	
K7GW Antivirus	Trojan (0048d55a1) *
Kaspersky	HEUR:Backdoor.AndroidOS.KungFu.a
Kingsoft	Android.Troj.KillAll.a.(kcloud), Android.Troj.Kongfu.op.(kcloud)
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!5C1F2F86C4E3 *
McAfee GW	
Microsoft	Trojan:AndroidOS/Legana.A
NANO AntiVirus	Riskware.Android.Wooboo.cthjxd, Trojan.Android.WqM
NOD32	Android/DroidKungFu.M.Gen, Android/DroidKungFu.M
NoraLabs NoraScan	
Norman	
Norton Symantec	Trojan.Gen.2
nProtect	
OfficeMalScanner	

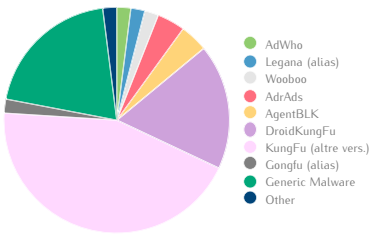
Antivirus	Result
Panda	
PathFinder	Malware
Preventon	Andr/KongFu-A
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Android.Kungfu.F
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Trojan.DroidKungFu.F
Segurmatica	
Segurmatica KE	HEUR:Backdoor.AndroidOS.KungFu.a
Solo	
Sophos	Andr/KongFu-A
SUPERAntiSpyware	
Team Cymru	Malware
The Cleaner	
The Hacker	
TotalDefense	Kugfu.XAVN!suspicious, AndroidOS/MalAndroid
TotalDefense Cloud	Heur/Backdoor!CdfGEHB *, Heur/TrojanHorse!CCAHEHB *
Tencent	Android.Trojan.Droidkungfu.Svrr *
Trend Micro	AndroidOS_AGENTBLK.935 *, Android.A3DF2BB4 *
Trend Micro-Housecall	AndroidOS_AGENTBLK.935 *
TrustPort	Android.Trojan.DroidKungFu.C
TT Livescan	
VBA32	Backdoor.AndroidOS.KungFu.a
Vexira	
VirIT eXplorer	Android.Trj.KungFu.GY
VIRobot	Android.Trojan.DroidKungFu.F[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.DroidKungFu.C

Detected	50
Undetected	39
Sum	89



Name Distribution

Name	Amount	Score
AdWho	1	2
Legana (alias)	1	3
Wooboo	1	0
AdrAds	2	0
AgentBLK	2	0
DroidKungFu	9	3
KungFu (altre vers.)	22	2
Gongfu (alias)	1	3
Generic Malware	10	1
Other	1	1
Sum	**50**	



Average Score	0,57

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_COARSE_LOCATION	Allows an app to access approximate location derived from network location sources such as cell towers and WI-FI
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.ACCESS_WIFI_STATE	Allows applications to access information about WI-FI networks
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.READ_SMS	Allows an application to read SMS messages
android.permission.VIBRATE	Allows access to the vibrator
android.permission.WRITE_SMS	Allows an application to write SMS messages

Used Permissions	Description	API calls
android.permission.ACCESS_FINE_LOCATION °	Allows an app to access precise location from location sources such as GPS, cell towers, and WI-FI	android/location/LocationManager;->getLastKnownLocation
android.permission.ACCESS_NETWORK_STATE		android/net/ConnectivityManager;->getActiveNetworkInfo
android.permission.ACCESS_WIFI_STATE		android/net/wifi/WifiManager;->getConnectionInfo
android.permission.FACTORY_TEST °	Run as a manufacturer test application, running as the root user	android/content/pm/ApplicationInfo/Iflags
android.permission.INTERNET		java/net/NetworkInterface
android.permission.READ_CONTACTS °	Allows an application to read the user's contacts data	android/content/ContentResolver;->query
android.permission.READ_LOGS °	Allows an application to read the low-level system log files	java/lang/Runtime;->exec
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getDeviceId
android.permission.VIBRATE		android/os/Vibrator;->cancel
android.permission.WAKE_LOCK °	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming	android/media/MediaPlayer;->start
com.android.browser.permission.READ_HISTORY_BOOKMARKS °	Allows an application to read (but not write) the user's browsing history and bookmarks	android/provider/Browser;->getAllVisitedUrls

Used Intents
android.intent.action.BATTERY_CHANGED_ACTION
android.intent.action.BOOT_COMPLETED
android.intent.action.MAIN
android.intent.action.SIG_STR
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.adwo.adsdk.AdwoAdBrowserActivity	✗	✓	✗
com.glu.android.dinercn.DinerDash2	✓	✓	✓
com.glu.android.dinercn.ShowTips	✓	✓	✗

Services	Used	Provided by Android	Provided by Third-Parties
com.glu.android.dinercn.UpdateService	✓	✓	✗
com.android.vending.util.WorkService	✓	✓	
com.android.music.MediaPlaybackService	✓	✓	

Receivers	Used	Provided by Android	Provided by Third-Parties
com.glu.android.dinercn.Receiver	✓	✓	✓

Providers	Used	Provided by Android	Provided by Third-Parties
-			

Used Networks

Toast Messages
low_memory

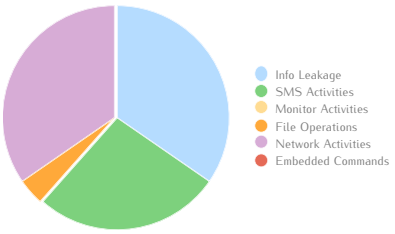
Network Analysis

Hardcoded URLs	IP	Region
proxy.youdraw.cn	114.255.171.253	China - Beijing
gad.ju6666.com	-	-
www.ss3.glu.com	-	-
mrc-stage.glu.com	64.75.10.61	United States - Chesterfield
gcs.glu.com	64.75.10.55	United States - Chesterfield
market.android.com	117.144.231.205	China - Beijing
maps.google.com	74.125.235.164	United States - Mountain View
www.adwo.com	42.62.76.6	China - Beijing
r2.adwo.com	42.62.76.8	China - Beijing
schemas.android.com	-	-
mrc.glu.com	64.75.10.11	United States - Chesterfield

Request	IP	Region	Type
proxy.youdraw.cn	118.26.192.171	China - Beijing	HTTP POST / DNS
r2.adwo.com	114.255.171.253	China - Beijing	HTTP POST / DNS
r2.adwo.com	42.62.76.8	China - Beijing	HTTP POST

Potentially Dangerous Operations

	Name	Description
Info Leakage	Call_Query	List phone call records
	Contact_Query	List contacts
	GPS_Get	Retrieve GPS information
	Location_Get	Retrieve current phone location
	Network_Provider_Get	Retrieve network provider information
	Phone_IMEI_Get	Retrieve IMEI
	Phone_IMSI_Get	Retrieve IMSI
	Phone_Number_Get	Retrieve current phone number
	SMS_Query	List SMS
SMS Activities	Contact_Create	Create contact
	Contact_Erase	Delete contact
	Database_Erase	Delete database
	Notification_Send	Send notifications
	SMS_Create_Message	Create SMS Inbox
	SMS_Delete_Message	Delete SMS Inbox
	SMS_Erase	Delete SMS
Monitor Activities	-	
File Operations	File_Erase	Delete file
Network Activities	TAINT_PHONE_NUMBER, TAINT_IMEI	r2.adwo.com:80 (9 times)
Embedded Commands	-	



Info Leakage	9
SMS Activities	7
Monitor Activities	0
File Operations	1
Network Activities	9
Embedded Commands	0

DroidKungFuSapp A

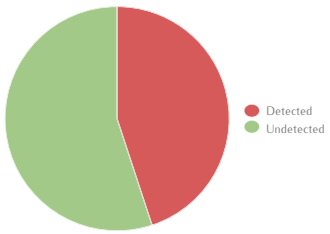
MD5	d27945202667cf6f588fed28d93562cd
SHA-1	8f85dbb8f3b58c40d1c5cabe2f72f7a9480a460f
SHA-256	4b9c844545e2463335822d041c647976ca30fcaf9152c1de2dc9a8e9b6046368
API Level	5
File Dimension (MB)	2.09
Package Name	com.aijiaoyou.android.sipphone
Other Names	8f85dbb8f3b58c40d1c5cabe2f72f7a9480a460f
Used Features	android.hardware.microphone android.hardware.wifi android.hardware.touchscreen android.hardware.screen.portrait

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.DroidKungFu.N
Adobe Malware Classifier	
Aegislab	DroidKungFu
Agnitum	
AhnLab-V3	Android-Malicious/KungFu
ALYac	
Anchivia	
Antiy-AVL	
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Other:Malware-gen, Android:KungFu-CD
AVG	Android_mc.AQX, Android_dc.AF.NY
Avira	Android/DroidKungFu.AP.3
AVware	Trojan.AndroidOS.Generic.A
Baidu	Trojan.Android.DroidKungFu.AP
BitDefender	Android.Trojan.DroidKungFu.N
Bkav	
ByteHero	
ClamAV	
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.D2794520!Olympus, AndroidOS/DroidKungFu.V
Digital Patrol	
DrWeb	
EmsiSoft	Android.Trojan.DroidKungFu.N (B)
Epoolsoft	
eScan	Android.Trojan.DroidKungFu.N
F-Mirc	
F-Prot	AndroidOS/DroidKungFu.V
F-Secure	Trojan:Android/DroidKungFu.A
FileMedic	
FilsecLab Twister	Android.DroidKungFu.Y.alvo, Android.M.ryym
Fortinet	Android/DroidKungFu.AP
GData	Android.Trojan.DroidKungFu.N
GFI Vipre	Trojan.AndroidOS.Generic.A
Ikarus	Trojan.AndroidOS.DroidKungFu, Backdoor.AndroidOS.KungFu, AndroidOS.Suspect.Manifest
Immunos	
Jiangmin	Backdoor/AndroidOS.ulv
K7 Antivirus	
K7GW Antivirus	Trojan (000001021)
Kaspersky	
Kingsoft	Android.Troj.at_KungFu.a.(kcloud)
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!D27945202667
McAfee GW	
Microsoft	
NANO AntiVirus	Trojan.Android.DroidKungFu.ddjjdf
NOD32	Android/DroidKungFu.W.Gen, Android/DroidKungFu.Y
NoraLabs NoraScan	
Norman	
Norton Symantec	
nProtect	
OfficeMalScanner	

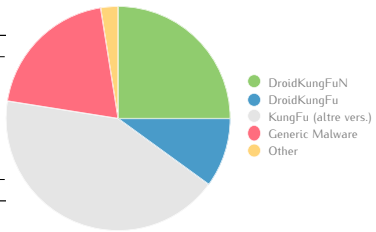
Antivirus	Result
Panda	
PathFinder	
Preventon	Andr/KongFu-N
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Exploit.Kongfu.N66, Android.Droidkungfu.AP1af8
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Trojan.DroidKungFu.N
Segurmatica	
Segurmatica KE	
Solo	
Sophos	Andr/KongFu-N
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	Kugfu.XAVM!suspicious
TotalDefense Cloud	
Tencent	Android.Trojan.Droidkungfu.Wpsz
Trend Micro	AndroidOS_TROJKungfu.A, Android.AB251B38
Trend Micro-Housecall	AndroidOS_TROJKungfu.A
TrustPort	
TT Livescan	
VBA32	Trojan.AndroidOS.KungFu.a
Vexira	
VirIT eXplorer	Android.Trj.KungFu.CT
VIRobot	Android.Trojan.DroidKungFu.N[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.DroidKungFu.A

Detected	40
Undetected	49
Sum	89



Name Distribution

Name	Amount	Score
DroidKungFuN	10	3
DroidKungFu	4	3
KungFu (altre vers.)	17	2
Generic Malware	8	1
Other	1	1
Sum	**40**	



Average Score	0,40

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.ACCESS_WIFI_STATE	Allows applications to access information about WI-FI networks
android.permission.BOOT_COMPLETED	-
android.permission.CHANGE_WIFI_STATE	Allows applications to change Wi-Fi connectivity state
android.permission.CLEAR_APP_CACHE	Allows an application to clear the caches of all installed applications on the device
android.permission.GET_TASKS	This constant was deprecated in API level 21
android.permission.INTERNET	Allows applications to open network sockets
android.permission.MODIFY_AUDIO_SETTINGS	Allows an application to modify global audio settings
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting
android.permission.RECORD_AUDIO	Allows an application to record audio
android.permission.SET_PREFERRED_APPLICATIONS	This constant was deprecated in API level 7
android.permission.WAKE_LOCK	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage

Used Permissions	Description	API calls
android.permission.ACCESS_NETWORK_STATE		android/net/ConnectivityManager;->getActiveNetworkInfo
android.permission.INTERNET		java/net/HttpURLConnection
android.permission.MODIFY_AUDIO_SETTINGS		android/media/AudioManager;->setSpeakerphoneOn
android.permission.READ_LOGS °	Allows an application to read the low-level system log files	java/lang/Runtime;->exec
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getDeviceId
android.permission.VIBRATE °	Allows access to the vibrator	android/app/NotificationManager;->notify
android.permission.WAKE_LOCK		android/media/MediaPlayer;->start

Used Intents
android.intent.action.BATTERY_CHANGED_ACTION
android.intent.action.BOOT_COMPLETED
android.intent.action.MAIN
android.intent.action.NEW_OUTGOING_CALL
android.intent.action.SIG_STR
android.intent.category.DEFAULT
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.aijiaoyou.android.sipphone.AgentDetialInfo	✔	✔	✘
com.aijiaoyou.android.sipphone.ChongZhiActivity	✔	✔	✘
com.aijiaoyou.android.sipphone.HistoryDetailActivity	✔	✔	✘
com.aijiaoyou.android.sipphone.InitOnlineActivity	✔	✔	✔
com.aijiaoyou.android.sipphone.OnlineActivity	✔	✔	✘
com.aijiaoyou.android.sipphone.SongListActivity	✔	✔	✘
com.aijiaoyou.android.sipphone.ZhiFuBaoChongZhiActivity	✔	✔	✘
org.linphone.LinphonePreferencesActivity11	✘	✔	✔

Services	Used	Provided by Android	Provided by Third-Parties
com.mjdc.sapp.service.BehindService	✔	✔	✘
com.mjdc.sapp.service.ConnectService	✔	✔	✘
org.linphone.LinphoneService	✔	✔	✘
com.android.vending.util.WorkService	✔	✔	
com.android.music.MediaPlaybackService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
com.mjdc.sapp.receiver.BootReceiver	✔	✔	✔
com.mjdc.sapp.receiver.SigChangeReceiver	✔	✔	✔
org.linphone.BootReceiver	✔	✔	✔
org.linphone.NetworkManager	✔	✔	✔
org.linphone.OutgoingCallReceiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
-			

Used Networks
android.net.conn.CONNECTIVITY_CHANGE

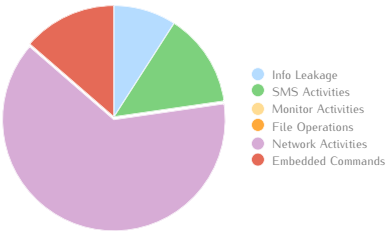
Network Analysis

Hardcoded URLs	IP	Region
msp.alipay.com	110.75.143.31	China - Hangzhou
-	219.238.160.86	China - Beijing
www.linphone.org	94.23.19.176	France
schemas.android.com	-	-

Request	IP	Region	Type
-	219.238.160.86	China - Beijing	HTTP GET
android.clients.google.com	173.194.116.165	United States - Mountain View	HTTP POST / DNS
-	86.160.238.219.in-addr.arpa	United Kingdom - Londra	DNS
-	165.116.194.173.in-addr.arpa	United States - Colorado Springs	DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	App_Info_Get	Retrieve package installation information
	Phone_IMEI_Get	Retrieve IMEI
SMS Activities	Notification_Send	Send notifications (3 times)
Monitor Activities	-	
File Operations	-	
Network Activities	Network_Access	Access network (9 times)
	TAINT_IMEI	219.238.160.86:80 (5 times)
Embedded Commands	unix-compress	Compress a file
	unix-mkdir	Make a directory
	unix-sleep	Suspend execution for a specified interval



Info Leakage	2
SMS Activities	3
Monitor Activities	0
File Operations	0
Network Activities	14
Embedded Commands	3

DroidKungFuSapp B

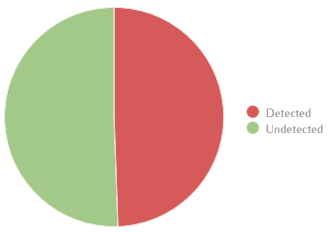
MD5	32e1eb3b5cd4dc64372bf6bb59370f08
SHA-1	f2b7ab8bbdc9cf07417cea4752e4b531c5d4b566
SHA-256	3ebb4c2bc959080eb9ba2328d10610b59e77892667f8cc5794479f0625e283ec
API Level	5
File Dimension (MB)	2.10
Package Name	com.aijiaoyou.android.sipphone
Other Names	f2b7ab8bbdc9cf07417cea4752e4b531c5d4b566
Used Features	android.hardware.microphone android.hardware.wifi android.hardware.touchscreen android.hardware.screen.portrait

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.DroidKungFu.N
Adobe Malware Classifier	
Aegislab	DroidKungFu
Agnitum	
AhnLab-V3	Android-Malicious/KungFu
ALYac	
Anchivia	
Antiy-AVL	*Backdoor/AndroidOS.KungFu[:vcsii] #*
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Other:Malware-gen, Android:KungFu-CD
AVG	Android_mc.XB *
Avira	Android/DroidKungFu.AG *
AVware	Trojan.AndroidOS.Generic.A
Baidu	Trojan.Android.DroidKungFu.aNu *
BitDefender	Android.Trojan.DroidKungFu.N
Bkav	
ByteHero	
ClamAV	
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.32E1EB3B!Olympus *, AndroidOS/DroidKungFu.V
Digital Patrol	
DrWeb	
EmsiSoft	Android.Trojan.DroidKungFu.N (B)
Epoolsoft	
eScan	Android.Trojan.DroidKungFu.N
F-Mirc	
F-Prot	AndroidOS/DroidKungFu.V
F-Secure	Trojan:Android/DroidKungFu.A
FileMedic	
FilsecLab Twister	Android.DroidKungFu.Y.alvo, Android.M.qlpk *
Fortinet	Android/DroidKungFu.A!tr *
GData	Android.Trojan.DroidKungFu.N
GFI Vipre	Trojan.AndroidOS.Generic.A
Ikarus	Trojan.AndroidOS.DroidKungFu, Backdoor.AndroidOS.KungFu, AndroidOS.Suspect.Manifest
Immunos	
Jiangmin	Backdoor/AndroidOS.ulv
K7 Antivirus	
K7GW Antivirus	Trojan (000001021)
Kaspersky	*HEUR:Backdoor.AndroidOS.KungFu.a #*
Kingsoft	Android.Troj.at_KungFu.i.(kcloud) *
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!32E1EB3B5CD4 *
McAfee GW	
Microsoft	
NANO AntiVirus	Trojan.Android.KungFu.cvgvkg *
NOD32	Android/DroidKungFu.W.Gen, Android/DroidKungFu.Y
NoraLabs NoraScan	
Norman	
Norton Symantec	
nProtect	
OfficeMalScanner	

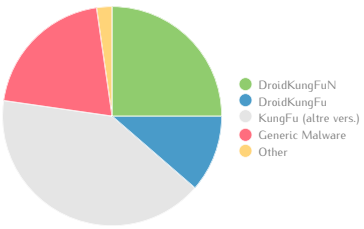
Antivirus	Result
Panda	
PathFinder	*Malware #*
Preventon	Andr/KongFu-N
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Exploit.Kongfu.N66, Android.Kungfu.A Suspicious *
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Trojan.DroidKungFu.N
Segurmatica	
Segurmatica KE	*HEUR:Backdoor.AndroidOS.KungFu.a #*
Solo	
Sophos	Andr/KongFu-N
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	Kugfu.XAVM!suspicious
TotalDefense Cloud	
Tencent	Android.Trojan.Droidkungfu.Wpsz
Trend Micro	AndroidOS_TROJKungfu.A, Android.AB251B38
Trend Micro-Housecall	AndroidOS_TROJKungfu.A
TrustPort	
TT Livescan	
VBA32	Trojan.AndroidOS.KungFu.a
Vexira	
VirIT eXplorer	Android.Trj.KungFu.LJ *
VIRobot	Android.Trojan.DroidKungFu.N[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.DroidKungFu.A

Detected	44
Undetected	45
Sum	89



Name Distribution

Name	Amount	Score
DroidKungFuN	11	3
DroidKungFu	5	3
KungFu (altre vers.)	18	2
Generic Malware	9	1
Other	1	1
Sum	**44**	



Average Score	0,55

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.ACCESS_WIFI_STATE	Allows applications to access information about WI-FI networks
android.permission.BOOT_COMPLETED	-
android.permission.CHANGE_WIFI_STATE	Allows applications to change Wi-Fi connectivity state
android.permission.CLEAR_APP_CACHE	Allows an application to clear the caches of all installed applications on the device
android.permission.GET_TASKS	This constant was deprecated in API level 21
android.permission.INTERNET	Allows applications to open network sockets
android.permission.MODIFY_AUDIO_SETTINGS	Allows an application to modify global audio settings
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting
android.permission.RECORD_AUDIO	Allows an application to record audio
android.permission.SET_PREFERRED_APPLICATIONS	This constant was deprecated in API level 7
android.permission.VIBRATE	Allows access to the vibrator
android.permission.WAKE_LOCK	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage

Used Permissions	Description	API calls
android.permission.ACCESS_NETWORK_STATE		android/net/ConnectivityManager;->getActiveNetworkInfo
android.permission.INTERNET		java/net/HttpURLConnection
android.permission.MODIFY_AUDIO_SETTINGS		android/media/AudioManager;->setSpeakerphoneOn
android.permission.READ_LOGS °	Allows an application to read the low-level system log files	java/lang/Runtime;->exec
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getDeviceId
android.permission.VIBRATE		android/app/NotificationManager;->notify
android.permission.WAKE_LOCK		android/media/MediaPlayer;->start

Used Intents
android.intent.action.BATTERY_CHANGED_ACTION
android.intent.action.BOOT_COMPLETED
android.intent.action.MAIN
android.intent.action.NEW_OUTGOING_CALL
android.intent.action.SIG_STR
android.intent.category.DEFAULT
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.aijiaoyou.android.sipphone.AgentDetialInfo	✔	✔	✘
com.aijiaoyou.android.sipphone.ChongZhiActivity	✔	✔	✘
com.aijiaoyou.android.sipphone.HistoryDetailActivity	✔	✔	✘
com.aijiaoyou.android.sipphone.InitOnlineActivity	✔	✔	✔
com.aijiaoyou.android.sipphone.OnlineActivity	✔	✔	✘
com.aijiaoyou.android.sipphone.SongListActivity	✔	✔	✘
com.aijiaoyou.android.sipphone. ZhiFuBaoChongZhiActivity	✔	✔	✘
org.linphone.LinphonePreferencesActivity11	✘	✔	✔

Services	Used	Provided by Android	Provided by Third-Parties
com.mjdc.sapp.service.BehindService	✔	✔	✘
com.mjdc.sapp.service.ConnectService	✔	✔	✘
org.linphone.LinphoneService	✔	✔	✘
com.android.vending.util.WorkService	✔	✔	
com.android.music.MediaPlaybackService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
com.mjdc.sapp.receiver.BootReceiver	✔	✔	✔
com.mjdc.sapp.receiver.SigChangeReceiver	✔	✔	✔
org.linphone.BootReceiver	✔	✔	✔
org.linphone.NetworkManager	✔	✔	✔
org.linphone.OutgoingCallReceiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
-			

Used Networks
android.net.conn.CONNECTIVITY_CHANGE

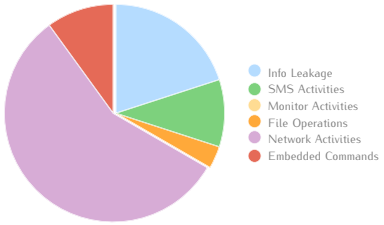
Network Analysis

Hardcoded URLs	IP	Region
msp.alipay.com	110.75.143.31	China - Hangzhou
219.238.160.86	219.238.160.86	China - Beijing
www.linphone.org	94.23.19.176	France

Request	IP	Region	Type
219.238.160.86	219.238.160.86	China - Beijing	HTTP GET
android.clients.google.com	173.194.116.165	United States - Mountain View	HTTP POST / DNS
-	86.160.238.219.in-addr.arpa	United Kingdom - Londra	DNS
-	165.116.194.173.in-addr.arpa	United States - Colorado Springs	DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	App_Info_Get	Retrieve package installation information (3 times)
	Phone_IMEI_Get	Retrieve IMEI (2 times)
	Phone_Number_Get	Retrieve current phone number del device
SMS Activities	Notification_Send	Send notifications (3 times)
Monitor Activities	-	
File Operations	Os_Kill	Terminate a process
Network Activities	Network_Access	Access network (12 times)
	TAINT_IMEI	219.238.160.86:80 (5 times)
Embedded Commands	unix-compress	Compress a file
	unix-mkdir	Make a directory
	unix-sleep	Suspend execution for a specified interval



Info Leakage	6
SMS Activities	3
Monitor Activities	0
File Operations	1
Network Activities	17
Embedded Commands	3

DroidKungFuUpdate

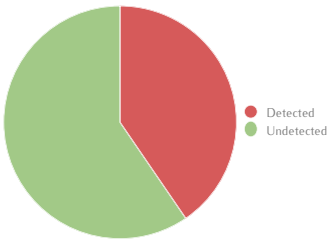
MD5	5e26403a5f7ec59479fb1009d875bcdb
SHA-1	5e2fb0bef9048f56e461c746b6a644762f0b0b54
SHA-256	37d382faafcaad6f8bf5da383cb8703b7094a045aeac5e13b5f4225c6272a615
API Level	5
File Dimension (MB)	0.21
Package Name	com.ps.keepaccount
Other Names	5e2fb0bef9048f56e461c746b6a644762f0b0b54
Used Features	android.hardware.touchscreen

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Adware.Wapsx.A
Adobe Malware Classifier	
Aegislab	SUSPICIOUS
Agnitum	
AhnLab-V3	Android-Malicious/KungFu
ALYac	
Anchivia	
Antiy-AVL	
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Android:DroidKungFuU-A
AVG	Android_mc.BCJ
Avira	Android/DroidKungFu.AN
AVware	Trojan.AndroidOS.Generic.A
Baidu	Trojan.Android.DroidKungFu.AN
BitDefender	Android.Adware.Wapsx.A
Bkav	
ByteHero	
ClamAV	
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.5E26403A!Olympus, AndroidOS/Wooboo.A.gen!Eldorado
Digital Patrol	
DrWeb	
EmsiSoft	Android.Adware.Wapsx.A (B)
Epoolsoft	
eScan	Android.Adware.Wapsx.A
F-Mirc	
F-Prot	AndroidOS/Wapsx.E
F-Secure	Trojan-Downloader:Android/DroidKungFu.E
FileMedic	
FilsecLab Twister	Android.M.xjkg
Fortinet	Android/DroidKungFu.AN, Android/DroidKungFu.O
GData	Android.Adware.Wapsx.A
GFI Vipre	Trojan.AndroidOS.Generic.A
Ikarus	AndroidOS.Suspect.Manifest
Immunos	
Jiangmin	
K7 Antivirus	
K7GW Antivirus	Trojan (0001140e1)
Kaspersky	
Kingsoft	Android.Troj.at_KungFu.d.(kcloud), Android.Troj.hh_kungfu.d.(kcloud)
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!5E26403A5F7E
McAfee GW	
Microsoft	
NANO AntiVirus	Trojan.Android.Waps.demevm
NOD32	Android/DroidKungFu.AN
NoraLabs NoraScan	
Norman	
Norton Symantec	
nProtect	
OfficeMalScanner	

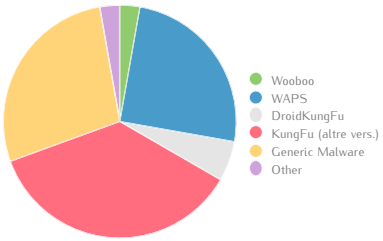
Antivirus	Result
Panda	
PathFinder	
Preventon	Andr/KongFu-O
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Adware.Wapsx.A
Segurmatica	
Segurmatica KE	
Solo	
Sophos	Andr/KongFu-O
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	
TotalDefense Cloud	
Tencent	Android.Trojan.Droidkungfu.Swuw
Trend Micro	AndroidOS_DROIDKUNGFU.CDE, Android.B235FAF9
Trend Micro-Housecall	AndroidOS_DROIDKUNGFU.CDE
TrustPort	
TT Livescan	
VBA32	
Vexira	
VirIT eXplorer	Android.Trj.KungFu.BN
VIRobot	Android.Adware.Wapsx.A[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.DroidKungFu.E

Detected	36
Undetected	53
Sum	89



Name Distribution

Name	Amount	Score
Wooboo	1	0
WAPS	9	2
DroidKungFu	2	3
KungFu (altre vers.)	13	2
Generic Malware	10	1
Other	1	1
Sum	**36**	



Average Score	0,09

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.GET_TASKS	This constant was deprecated in API level 21
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage

Used Permissions	Description	API calls
android.permission.ACCESS_FINE_LOCATION °	Allows an app to access precise location from location sources such as GPS, cell towers, and WI-FI	android/location/LocationManager;->getLastKnownLocation
android.permission.ACCESS_NETWORK_STATE		android/net/ConnectivityManager;->getActiveNetworkInfo
android.permission.FACTORY_TEST	Run as a manufacturer test application, running as the root user	android/content/pm/ApplicationInfo/lflags
android.permission.GET_TASKS		android/app/ActivityManager;->getRunningTasks
android.permission.INTERNET		java/net/HttpURLConnection
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getDeviceId
android.permission.VIBRATE °	Allows access to the vibrator	android/app/NotificationManager;->notify

Used Intents
android.intent.action.MAIN
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.ps.keepaccount.Main	✔	✔	✔
com.ps.keepaccount.activity.DemoApp	✔	✔	✘
com.ps.keepaccount.activity.HistoryAccount	✔	✔	✘
com.ps.keepaccount.activity.QueryAccount	✔	✔	✘
com.ps.keepaccount.activity.TodayAccount	✔	✔	✘
com.ps.keepaccount.activity.TypeAccount	✔	✔	✘
com.ps.keepaccount.activity.TypeAccountList	✔	✔	✘
com.ps.keepaccount.activity.WriteAccount	✔	✔	✘
com.ps.keepaccount.dialog.CanlendarDialog	✘	✔	✘
com.ps.keepaccount.dialog.DateSelectorDialog	✘	✔	✘
com.ps.keepaccount.tabbar.ButtonDemo	✔	✔	✘
com.waps.OffersWebView	✘	✔	✘
org.achartengine.GraphicalActivity	✘	✔	✘

Services	Used	Provided by Android	Provided by Third-Parties
com.android.vending.util.WorkService	✔	✔	
com.android.music.MediaPlaybackService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
-			

Providers	Used	Provided by Android	Provided by Third-Parties
-			

Used Networks
-

Toast Messages	
加载中,请稍候...	[Loading, please wait]
正在下载,请稍候...	[Loading, please wait]

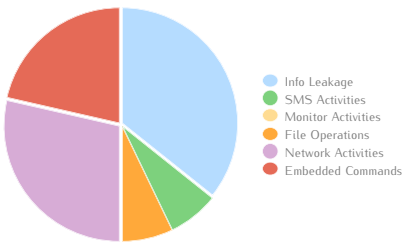
Network Analysis

Hardcoded URLs	IP	Region
app.waps.cn	219.234.85.243	China - Beijing
ads.waps.cn	117.144.231.205	China - Beijing
219.234.85.214	219.234.85.214	China - Beijing

Request	IP	Region	Type
app.waps.cn	219.234.85.216	China - Beijing	HTTP GET / DNS
ads.waps.cn	219.234.85.237	China - Beijing	HTTP GET / HTTP POST DNS
appcdn.wapx.cn	61.156.157.181	China - Jinan	HTTP GET / DNS
-	216.85.234.219.in-addr.arpa	United States - O' Fallon	DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	App_Get_Tasks	Retrieve running task information
	App_Info_Get	Retrieve package installation information
	GPS_Get	Retrieve GPS information
	Location_Get	Retrieve current phone location
	Phone_IMEI_Get	Retrieve IMEI
SMS Activities	Notification_Send	Send notifications
Monitor Activities	-	
File Operations	File_Erase	Delete file
Network Activities	TAINT_IMEI	app.waps.cn:80 (4 times)
Embedded Commands	unix-gzip	Compress a file and add the extension .gz
	unix-mkdir	Make a directory
	unix-sleep	Suspend execution for a specified interval



Info Leakage	5
SMS Activities	1
Monitor Activities	0
File Operations	1
Network Activities	4
Embedded Commands	3

FakeMart A

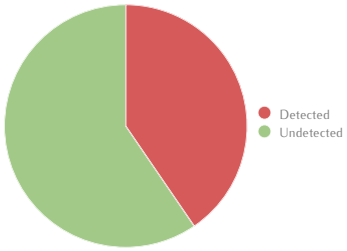
MD5	6a0e9ce340164af6f37a946df650b458
SHA-1	54855a5df15bc5d04310c06b9f34101acfa6a447
SHA-256	93ae0928d3ac4e1ef9b5fd737f6c7e3923b2afdb60040221107e34daf31fb3f9
API Level	0
File Dimension (MB)	0.25
Package Name	com.android.blackmarket
Other Names	Fakemart_6A0E9CE340164AF6F37A946DF650B458, 93ae0928d3ac4e1ef9b5fd737f6c7e3923b2afdb60040221107e34daf31fb3f9
Used Features	android.hardware.touchscreen android.hardware.telephony android.hardware.screen.portrait

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.FakeInst.AV
Adobe Malware Classifier	
Aegislab	Meds
Agnitum	
AhnLab-V3	Android-Malicious/FakeInst
ALYac	
Anchivia	
Antiy-AVL	
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Android:Jifake-G
AVG	Android/Fakeins
Avira	Android/MalCrypt.A.Gen
AVware	Trojan.AndroidOS.Generic.A
Baidu	Trojan.AndroidOS.Meds.Ayxe
BitDefender	Android.Trojan.FakeInst.AV
Bkav	
ByteHero	
ClamAV	
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.6A0E9CE3!Olympus, AndroidOS/FakeMart.A
Digital Patrol	
DrWeb	
EmsiSoft	Android.Trojan.FakeInst.AV (B)
Epoolsoft	
eScan	Android.Trojan.FakeInst.AV
F-Mirc	
F-Prot	AndroidOS/FakeMart.A
F-Secure	Trojan:Android/MalCrypt.A
FileMedic	
FilsecLab Twister	
Fortinet	Android/Fakemart.A!tr
GData	Android.Trojan.FakeInst.AV
GFI Vipre	Trojan.AndroidOS.Generic.A
Ikarus	AndroidOS.MalCrypt
Immunos	
Jiangmin	
K7 Antivirus	
K7GW Antivirus	
Kaspersky	HEUR:Trojan.AndroidOS.Meds.a
Kingsoft	Android.Troj.at_FakeMart.a.(kcloud)
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!6A0E9CE34016
McAfee GW	
Microsoft	
NANO AntiVirus	Trojan.Android.FakeInst.dgehia
NOD32	Android/MalCrypt.B
NoraLabs NoraScan	
Norman	
Norton Symantec	Trojan.Gen.2
nProtect	
OfficeMalScanner	

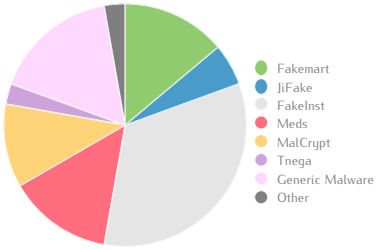
Antivirus	Result
Panda	
PathFinder	
Preventon	Andr/FakeIns-AH
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Trojan.FakeInst.AV
Segurmatica	
Segurmatica KE	HEUR:Trojan.AndroidOS.Meds.a
Solo	
Sophos	Andr/FakeIns-AH
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	AndroidOS/Tnega.cEVFZE
TotalDefense Cloud	
Tencent	Dos.Trojan.Meds.Wnms
Trend Micro	
Trend Micro-Housecall	
TrustPort	
TT Livescan	
VBA32	
Vexira	
VirIT eXplorer	Android.Trj.FakeMart.A
VIRobot	Android.Trojan.FakeInst.AV[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.Jifake.G

Detected	36
Undetected	53
Sum	89



Name Distribution

Name	Amount	Score
Fakemart	5	3
JiFake	2	0
FakeInst	12	2
Meds	5	0
MalCrypt	4	0
Tnega	1	0
Generic Malware	6	1
Other	1	1
Sum	**36**	



Average Score	-0,08

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.READ_SMS	Allows an application to read SMS messages
android.permission.RECEIVE_SMS	Allows an application to monitor incoming SMS messages, to record or perform processing on them
android.permission.SEND_SMS	Allows an application to send SMS messages
android.permission.WRITE_SMS	Allows an application to write SMS messages

Used Permissions	Description	API calls
android.permission.INTERNET		java/net/ServerSocket
android.permission.READ_CONTACTS °	Allows an application to read the user's contacts data	android/content/ContentResolver;->query
android.permission.SEND_SMS		android/telephony/gsm/SmsManager;->sendTextMessage
android.permission.VIBRATE °	Allows access to the vibrator	android/media/AudioManager/setRingerMode(I)

Used Intents
android.intent.action.MAIN
android.intent.action.NOTIFICATION_REMOVE
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.android.blackmarket.BlackMarketAlpha	✔	✔	✔

Services	Used	Provided by Android	Provided by Third-Parties
com.android.vending.util.WorkService	✔	✔	
com.android.music.MediaPlaybackService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
com.android.blackmarket.SmsReceiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
android.provider.Telephony.SMS_RECEIVED	✔	✔	

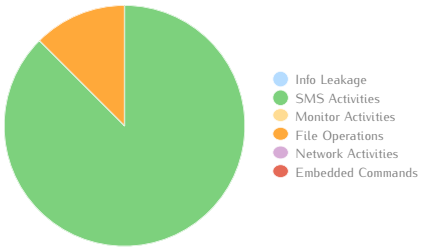
Used Networks
-

Network Analysis

Hardcoded URLs	IP	Region
ant.apache.org	192.87.106.229	Netherlands - Amsterdam
jakarta.apache.org	192.87.106.229	Netherlands - Amsterdam
marc.theaimsgroup.com	-	-
schemas.android.com	-	-
trill.cis.fordham.edu	150.108.68.29	United States - Bronx
www.apache.org	192.87.106.229	Netherlands - Amsterdam
www.jcraft.com	124.34.9.130	Japan - Tokyo

Potentially Dangerous Operations

	Name	Description
Info Leakage	-	
SMS Activities	Contact_Erase	Delete contact
	Database_Erase	Delete database
	SMS_Analysis	Analysis SMS messages
	SMS_Delete_Message	Delete Inbox SMS
	SMS_Erase	Delete SMS
	SMS_Intercept	Intercept SMS
	SMS_Send	Send SMS
Monitor Activities	-	
File Operations	File_Erase	Delete file
Network Activities	-	
Embedded Commands	-	



Info Leakage	0
SMS Activities	7
Monitor Activities	0
File Operations	1
Network Activities	0
Embedded Commands	0

FakeMart B

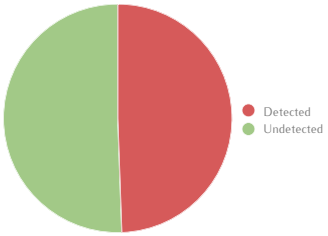
MD5	d002f0581a862373aa6c6c0070ec3156
SHA-1	b45d969a8fd1d3fb2a787cab8460b54088d89770
SHA-256	e6bbe679393e962ea5692bc7234f5ec6d475599299e34b2d6ad6a0a3304a62d1
API Level	0
File Dimension (MB)	0.24
Package Name	com.android.blackmarket
Other Names	Femrt_D002F0581A862373AA6C6C0070EC3156.apk e6bbe679393e962ea5692bc7234f5ec6d475599299e34b2d6ad6a0a3304a62d1 Recent14.apk Fakemart_D002F0581A862373AA6C6C0070EC3156
Used Features	android.hardware.touchscreen android.hardware.telephony android.hardware.screen.portrait

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.FakeInst.AV
Adobe Malware Classifier	
Aegislab	FakeMart *
Agnitum	
AhnLab-V3	Android-Malicious/FakeInst
ALYac	
Anchivia	
Antiy-AVL	
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Android:FakeInst-CJ *
AVG	Android/Fakeins
Avira	Android/Agent.O.Gen *£
AVware	Trojan.AndroidOS.Generic.A
Baidu	Trojan.AndroidOS.FakeMart.ao *
BitDefender	Android.Trojan.FakeInst.AV
Bkav	
ByteHero	
ClamAV	*Android.Trojan.Smssend-8 #*
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBLD002F058!Olympus *, AndroidOS/FakeMart.A
Digital Patrol	
DrWeb	
EmsiSoft	Android.Trojan.FakeInst.AV (B)
Epoolsoft	
eScan	Android.Trojan.FakeInst.AV
F-Mirc	
F-Prot	AndroidOS/FakeMart.A
F-Secure	Trojan:Android/FakeInst.gen!65232C *£
FileMedic	
FilsecLab Twister	*Android.M.vauv #*
Fortinet	Android/Fakemart.A!tr
GData	Android.Trojan.FakeInst.AV
GFI Vipre	Trojan.AndroidOS.Generic.A
Ikarus	PUA.AndroidOS.PrevGame *
Immunos	*Android.Trojan.Smssend-8 #*
Jiangmin	*Trojan/AndroidOS.wei #*
K7 Antivirus	*Trojan (0001140e1) #*
K7GW Antivirus	*Trojan (0001140e1) #*
Kaspersky	HEUR:Trojan-SMS.AndroidOS.FakeMart.a *£
Kingsoft	Android.Troj.hh_FakeMart.a.(kcloud) *, Android.Troj.Undef.a.(kcloud) *
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!D002F0581A86 *
McAfee GW	
Microsoft	
NANO AntiVirus	Trojan.Android.FakeInst.dgehia
NOD32	Android/TrojanSMS.Agent.OS *
NoraLabs NoraScan	
Norman	
Norton Symantec	Trojan.Gen.2
nProtect	
OfficeMalScanner	

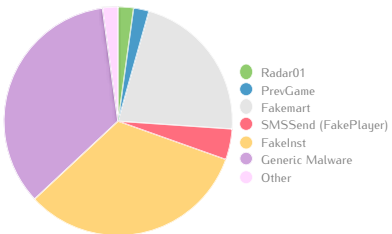
Antivirus	Result
Panda	
PathFinder	*Malware #*
Preventon	Andr/FakeIns-AH
Protector Plus	
PSafe Antivirus	
Qihoo 360	Malware.Radar01.Gen *^
Quick Heal (Cat)	*Android.FakeMart.A #*
RHBVS	
Rising	*NORMAL:Trojan.Agent.gcn!1612563 #*
Rising Cloud	
SecureIT	Android.Trojan.FakeInst.AV
Segurmatica	
Segurmatica KE	HEUR:Trojan-SMS.AndroidOS.FakeMart.a *£
Solo	
Sophos	Andr/FakeIns-AH
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	*NO MALWARE $*
TotalDefense Cloud	
Tencent	Trojan.Android.Agent.8DC685FF *£
Trend Micro	
Trend Micro-Housecall	
TrustPort	
TT Livescan	
VBA32	
Vexira	
VirIT eXplorer	Android.Trj.FakeMart.C *
VIRobot	Android.Trojan.FakeInst.AV[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.FakeInst.C *£

Detected	44
Undetected	45
Sum	89



Name Distribution

Name	Amount	Score
Radar01	1	0
PrevGame	1	0
Fakemart	10	3
SMSSend (FakePlayer)	2	0
FakeInst	15	2
Generic Malware	16	1
Other	1	1
Sum	44	



Average Score	0,36

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.INTERNET	Allows applications to open network sockets
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.READ_SMS	Allows an application to read SMS messages
android.permission.RECEIVE_SMS	Allows an application to monitor incoming SMS messages, to record or perform processing on them
android.permission.SEND_SMS	Allows an application to send SMS messages
android.permission.WRITE_SMS	Allows an application to write SMS messages

Used Permissions	Description	API calls
android.permission.INTERNET		java/net/ServerSocket
android.permission.READ_CONTACTS °	Allows an application to read the user's contacts data	android/content/ContentResolver;->query
android.permission.SEND_SMS		android/telephony/gsm/SmsManager;->sendTextMessage
android.permission.VIBRATE °	Allows access to the vibrator	android/media/AudioManager/setRingerMode(I)

Used Intents
android.intent.action.MAIN
android.intent.action.NOTIFICATION_REMOVE
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.android.blackmarket.BlackMarketAlpha	✔	✔	✔

Services	Used	Provided by Android	Provided by Third-Parties
com.android.vending.util.WorkService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
com.android.blackmarket.SmsReceiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
android.provider.Telephony.SMS_RECEIVED	✔	✔	

Used Networks
-

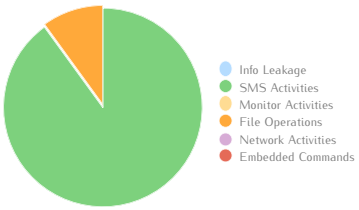
Network Analysis

Hardcoded URLs	IP	Region
www.gainpourtous.com	91.121.35.78	France - Lisses
mathissarox.myartsonline.com	83.125.22.184	Germany - Kiel
chateau-viranel.com	195.138.202.245	France
schemas.android.com	-	-
marc.theaimsgroup.com	-	-
jakarta.apache.org	192.87.106.229	Netherlands - Amsterdam
www.apache.org	192.87.106.229	Netherlands - Amsterdam
www.jcraft.com	124.34.9.130	Japan - Tokyo

Request	IP	Region	Type
www.gainpourtous.com	91.121.35.78	France - Lisses	HTTP GET / DNS
mathissarox.myartsonline.com	83.125.22.184	Germany - Kiel	HTTP GET / DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	-	
SMS Activities	Contact_Erase	Delete contact
	Database_Erase	Delete database
	SMS_Analysis	Analysis SMS messages
	SMS_Delete_Message	Delete Inbox SMS
	SMS_Erase	Delete SMS
	SMS_Intercept	Intercept SMS
	SMS_Send	Send "AP" to 81038 (3 times)
Monitor Activities	-	
File Operations	File_Erase	Delete file
Network Activities	-	
Embedded Commands	-	



Info Leakage	0
SMS Activities	9
Monitor Activities	0
File Operations	1
Network Activities	0
Embedded Commands	0

Geinimi A

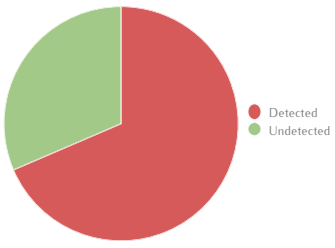
MD5	ae80c82e34278700886653a5e47f29c6
SHA-1	2ed1d46cd4f3aaaa20f079dd56aa52ecb5edc974
SHA-256	156ac7284eb536b413f469728448eb351ca952c4b6ebbbd1a0de158fab5b2fb6
API Level	3
File Dimension (MB)	0.83
Package Name	jp.co.kaku.spi.fs1006.Paid
Other Names	2ed1d46cd4f3aaaa20f079dd56aa52ecb5edc974
Used Features	android.hardware.location android.hardware.location.gps android.hardware.location.network android.hardware.telephony android.hardware.touchscreen android.hardware.screen.portrait

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.Geinimi.B
Adobe Malware Classifier	
Aegislab	Geinimi
Agnitum	TrojanSpy.AndroidOS.Geinimi.C
AhnLab-V3	Android-Malicious/Geimini
ALYac	
Anchivia	
Antiy-AVL	Trojan/AndroidOS.Geinimi[SPY]
Anvisoft	
Anvisoft Cloud	
ArcaVir	Trojan.Spy.Androidos.geinimi.bq
Avast	Android:Geinim-A
AVG	Android/Geinim, Generic5_c.EVL
Avira	Android/Geinimi.D
AVware	Trojan.AndroidOS.Geimini.A
Baidu	Trojan.AndroidOS.Geinimi.AicX
BitDefender	Android.Trojan.Geinimi.B
Bkav	
ByteHero	
ClamAV	Andr.Trojan.Geinimi-1
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBLAE80C82E!Olympus, AndroidOS/Geimini.A
Digital Patrol	
DrWeb	Android.Geinimi.31
EmsiSoft	Android.Trojan.Geinimi.B (B)
Epoolsoft	
eScan	Android.Trojan.Geinimi.B[ZP]
F-Mirc	
F-Prot	ANDR/Geinimi.B, AndroidOS/Geimini.A
F-Secure	Trojan:Android/Geinimi.A
FileMedic	
FilsecLab Twister	Android.M.ppvk
Fortinet	W32/Malware_fam.NB
GData	Android.Trojan.Geinimi.B
GFI Vipre	Trojan.AndroidOS.Geimini.A
Ikarus	Trojan.AndroidOS.Geinimi
Immunos	Andr.Trojan.Geinimi-1
Jiangmin	TrojanSpy.AndroidOS.ce
K7 Antivirus	Trojan (00352b281)
K7GW Antivirus	Trojan (00352b281)
Kaspersky	HEUR:Trojan-Spy.AndroidOS.Geinimi.a
Kingsoft	Android.Troj.Geinimi.bq.v.(kcloud), Android.Troj.hh_Geinimi.e.(kcloud)
MalwareBytes	
McAfee	Generic.hu
McAfee Artemis	Artemis!AE80C82E3427
McAfee GW	Generic.hu
Microsoft	TrojanSpy:AndroidOS/Geimini.A
NANO AntiVirus	Trojan.Android.Geinimi.cwzgmg
NOD32	Android/Spy.Geinimi.D
NoraLabs NoraScan	
Norman	Suspicious_Gen3.ABJUU
Norton Symantec	Android.Geinimi
nProtect	
OfficeMalScanner	

Antivirus	Result
Panda	Generic Malware
PathFinder	
Preventon	Andr/BBridge-A
Protector Plus	TrojanSpy.AndroidOS.Geinimi.C
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Android.Geimini.B
RHBVS	
Rising	DEX:System.Geimini!1.9DA5
Rising Cloud	
SecureIT	Android.Trojan.Geinimi.B
Segurmatica	
Segurmatica KE	HEUR:Trojan-Spy.AndroidOS.Geinimi.a
Solo	
Sophos	Andr/BBridge-A
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	AndroidOS/Geinimi.B
TotalDefense Cloud	Win32/Trafog!CIEZec, AndroidOS/Trojan!CEDcKb
Tencent	Trojan.Android.Agent.B1C4884E
Trend Micro	ANDROIDOS_GEINIMI.HRXA, ANDROID.5A9F93A1
Trend Micro-Housecall	ANDROIDOS_GEINIMI.HRXA
TrustPort	Android.Trojan.Geinimi.B
TT Livescan	
VBA32	Trojan-Spy.AndroidOS.Geinimi.bq
Vexira	TrojanSpy.AndroidOS.Geinimi.C
VirIT eXplorer	Android.Bkd.Geinimi.H
VIRobot	Android.Trojan.Geinimi.B[b]
VirusBuster	TrojanSpy.AndroidOS.Geinimi.C
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.Geimini.B

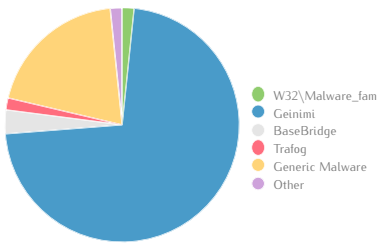
Detected	61
Undetected	28
Sum	89



Name Distribution

Name	Amount	Score
W32\Malware_fam	1	0
Geinimi	44	3
BaseBridge	2	0
Trafog	1	0
Generic Malware	12	1
Other	1	1
Sum	61	

Average Score	1,31



Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_COARSE_LOCATION	Allows an app to access approximate location derived from network location sources such as cell towers and WI-FI
android.permission.ACCESS_FINE_LOCATION	Allows an app to access precise location from location sources such as GPS, cell towers, and WI-FI
android.permission.ACCESS_GPS	-
android.permission.ACCESS_LOCATION	-
android.permission.CALL_PHONE	Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call being placed.
android.permission.INTERNET	Allows applications to open network sockets
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	Allows mounting and unmounting file systems for removable storage
android.permission.READ_CONTACTS	Allows an application to read the user's contacts data
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.READ_SMS	Allows an application to read SMS messages
android.permission.RECEIVE_SMS	Allows an application to monitor incoming SMS messages, to record or perform processing on them
android.permission.RESTART_PACKAGES	This constant was deprecated in API level 8
android.permission.SEND_SMS	Allows an application to send SMS messages
android.permission.SET_WALLPAPER	Allows applications to set the wallpaper
android.permission.VIBRATE	Allows access to the vibrator
android.permission.WRITE_CONTACTS	Allows an application to write (but not read) the user's contacts data
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage
android.permission.WRITE_SMS	Allows an application to write SMS messages
com.android.browser.permission.READ_HISTORY_BOOKMARKS	Allows an application to read (but not write) the user's browsing history and bookmarks
com.android.browser.permission.WRITE_HISTORY_BOOKMARKS	Allows an application to write (but not read) the user's browsing history and bookmarks
com.android.launcher.permission.INSTALL_SHORTCUT	Allows an application to install a shortcut in Launcher

Used Permissions	Description	API calls
android.permission.ACCESS_FINE_LOCATION		android/location/LocationManager;->getBestProvider
android.permission.ACCESS_NETWORK_STATE °	Allows applications to access information about networks	android/net/ConnectivityManager;->getActiveNetworkInfo
android.permission.FACTORY_TEST °	Run as a manufacturer test application, running as the root user	android/content/pm/ApplicationInfo/lflags
android.permission.INTERNET		java/net/Socket
android.permission.READ_CONTACTS °	Allows an application to read the user's contacts data	android/content/ContentResolver;->query
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getDeviceId
android.permission.RESTART_PACKAGES		android/app/ActivityManager;->restartPackage
android.permission.SEND_SMS		android/telephony/SmsManager;->sendTextMessage
android.permission.SET_WALLPAPER		android/content/Context;->setWallpaper
android.permission.VIBRATE		android/app/NotificationManager;->notify
android.permission.WAKE_LOCK °	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming	android/media/MediaPlayer;->start

Used Intents
android.intent.action.MAIN
android.intent.action.VIEW
android.intent.category.DEFAULT
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.mobclix.android.sdk.MobclixBrowserActivity	✘	✔	✘
jp.co.kaku.spi.fs1006.Paid.FS1006Activity	✔	✔	✔
jp.co.kaku.spi.fs1006.Paid.activity.c.rFrfhCvj	✔	✔	✔
jp.co.kaku.spi.fs1006.com.EntryScoreViewActivity	✔	✔	✔
jp.co.kaku.spi.fs1006.mobclix.MobclixAdvertisingView	✔	✔	✔

Services	Used	Provided by Android	Provided by Third-Parties
jp.co.kaku.spi.fs1006.Paid.activity.c.AndroidIME	✘	✔	✘
com.android.musicfx.Compatibility$Service	✔	✔	
com.android.vending.util.WorkService	✔	✔	
com.android.music.MediaPlaybackService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
com.android.blackmarket.SmsReceiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
-			

Used Networks
-

Toast Messages
loading...
not available...
Android SensorManager disabled, 1.5 SDK emulator crashes when using it... Make sure to connect SensorSimulator

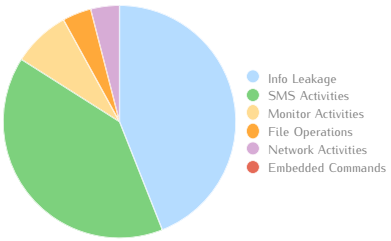
Network Analysis

Hardcoded URLs	IP	Region
kaku3.sakura.ne.jp	59.106.13.109	Japan - Osaka
data.mobclix.com	54.235.97.215	United States - Ashburn
schemas.android.com	-	-
vc.mobclix.com	75.101.131.215	United States - Ashburn
www.mobclix.com	75.101.131.215	United States - Ashburn
maps.google.com	74.125.235.164	United States - Mountain View
ads.mobclix.com	54.235.97.215	United States - Ashburn

Request	IP	Region	Type
data.mobclix.com	54.235.185.74	United States - Ashburn	HTTP GET
kaku3.sakura.ne.jp	59.106.13.109	Japan - Osaka	HTTP POST / DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	App_Info_Get	Retrieve package installation information
	Call_Query	List phone call records
	Contact_Query	List contacts
	GPS_Get	Retrieve GPS information
	Location_Get	Retrieve current phone location
	Location_Last_Get	Retrieve last phone location
	Network_NetProvider_Get	Retrieve network provider information
	Phone_IMEI_Get	Retrieve IMEI
	Phone_IMSI_Get	Retrieve IMSI
	Phone_Number_Get	Retrieve current phone number
	SMS_Query	List SMS
SMS Activities	App_Close	Close application
	Contact_Create	Create contact
	Contact_Erase	Delete contact
	Database_Erase	Delete database
	Notification_Send	Send notifications
	SMS_Analysis	Analysis SMS messages
	SMS_Create_Message	Create Inbox SMS
	SMS_Delete_Message	Delete Inbox SMS
	SMS_Erase	Delete SMS
	SMS_Send	Send SMS
Monitor Activities	GPS_Spy	Spy GPS states
	Location_Spy	Spy location
File Operations	File_Erase	Delete file
Network Activities	TAINT_ICCID	www.468.sakura.ne.jp:80
Embedded Commands	-	



Info Leakage	11
SMS Activities	10
Monitor Activities	2
File Operations	1
Network Activities	1
Embedded Commands	0

Geinimi B

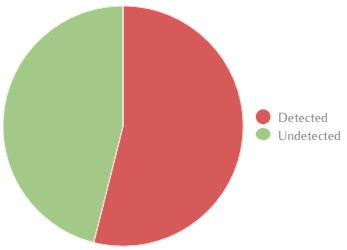
MD5	888cca6e0a62f5ff0564517d6c0d148c
SHA-1	043c690231c44de57fe05fff7cda5378b56ff0ad
SHA-256	a9530d0fb6e36dea0a157a6196cb36e46d8092218313284271 33b7aae83681fb
API Level	2
File Dimension (MB)	0.25
Package Name	cmp.netsentry
Other Names	043c690231c44de57fe05fff7cda5378b56ff0ad
Used Features	android.hardware.location android.hardware.location.gps android.hardware.location.network android.hardware.telephony android.hardware.touchscreen

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.Geinimi.B
Adobe Malware Classifier	
Aegislab	Geinimi
Agnitum	*NO MALWARE $*
AhnLab-V3	Android-Malicious/Geimini
ALYac	
Anchivia	
Antiy-AVL	*NO MALWARE $*
Anvisoft	
Anvisoft Cloud	
ArcaVir	*NO MALWARE $*
Avast	Android:Geinim-A
AVG	Android_mc.JBR *^
Avira	Android/Geinimi.B.Gen *
AVware	Trojan.AndroidOS.Generic.A *^
Baidu	Trojan.AndroidOS.Geinimi.ajHR *
BitDefender	Android.Trojan.Geinimi.B
Bkav	
ByteHero	
ClamAV	Andr.Trojan.Geinimi-1
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.888CCA6E!Olympus *, AndroidOS/Geimini.B *
Digital Patrol	
DrWeb	*NO MALWARE $*
EmsiSoft	Android.Trojan.Geinimi.B (B)
Epoolsoft	
eScan	Android.Trojan.Geinimi.B[ZP]
F-Mirc	
F-Prot	ANDR/Geinimi.B
F-Secure	Trojan:Android/Geinimi.A
FileMedic	
FilsecLab Twister	Android.M.qixz *
Fortinet	Android/Geinimi.H!tr *£
GData	Android.Trojan.Geinimi.B
GFI Vipre	*NO MALWARE $*
Ikarus	Trojan.AndroidOS.Geinimi, AndroidOS.Suspect.Manifest *
Immunos	Andr.Trojan.Geinimi-1
Jiangmin	TrojanSpy.AndroidOS.co *
K7 Antivirus	*NO MALWARE $*
K7GW Antivirus	Trojan (0001140e1) *
Kaspersky	HEUR:Trojan-Spy.AndroidOS.Geinimi.a
Kingsoft	Android.Troj.Geinimi.h.v.(kcloud) *, Android.Troj.hh_Geinimi.c.(kcloud) *
MalwareBytes	
McAfee	*NO MALWARE $*
McAfee Artemis	Artemis!888CCA6E0A62 *
McAfee GW	*NO MALWARE $*
Microsoft	TrojanSpy:AndroidOS/Geimini.A
NANO AntiVirus	Trojan.Android.Geinimi.cwzgmg
NOD32	Android/Spy.Geinimi.D
NoraLabs NoraScan	
Norman	Suspicious_Gen2.PXNEV *
Norton Symantec	Android.Geinimi
nProtect	
OfficeMalScanner	

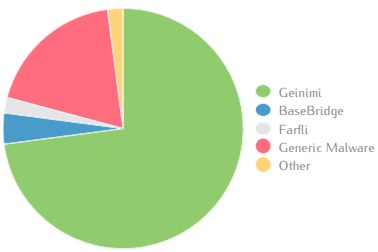
Antivirus	Result
Panda	*NO MALWARE $*
PathFinder	
Preventon	Andr/BBridge-A
Protector Plus	*NO MALWARE $*
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Android.Geimini.B
RHBVS	
Rising	DEX:System.Geimini!1.9DA5
Rising Cloud	
SecureIT	Android.Trojan.Geinimi.B
Segurmatica	
Segurmatica KE	HEUR:Trojan-Spy.AndroidOS.Geinimi.a
Solo	
Sophos	Andr/BBridge-A
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	*NO MALWARE $*
TotalDefense Cloud	Win32/Farfli!CSlYXe *, Win32/Farfli!COaLPb *
Tencent	Dos.Trojan-spy.Geinimi.Ebqy *£
Trend Micro	ANDROIDOS_GEINIMI.MJ *, Android.9AEDA42F *
Trend Micro-Housecall	ANDROIDOS_GEINIMI.MJ *
TrustPort	Android.Trojan.Geinimi.B
TT Livescan	
VBA32	Trojan-Spy.AndroidOS.Geinimi.h *
Vexira	*NO MALWARE $*
VirIT eXplorer	Android.Bkd.Geinimi.AD *
VIRobot	Android.Trojan.Geinimi.B[b]
VirusBuster	*NO MALWARE $*
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.Geimini.B

Detected	48
Undetected	41
Sum	89



Name Distribution

Name	Amount	Score
Geinimi	35	3
BaseBridge	2	3
Farfli	1	0
Generic Malware	9	1
Other	1	1
Sum	48	



Average Score	0,90

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_COARSE_LOCATION	Allows an app to access approximate location derived from network location sources such as cell towers and WI-FI
android.permission.ACCESS_FINE_LOCATION	Allows an app to access precise location from location sources such as GPS, cell towers, and WI-FI
android.permission.ACCESS_GPS	-
android.permission.ACCESS_LOCATION	-
android.permission.CALL_PHONE	Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call being placed.
android.permission.INTERNET	Allows applications to open network sockets
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	Allows mounting and unmounting file systems for removable storage
android.permission.READ_CONTACTS	Allows an application to read the user's contacts data
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.READ_SMS	Allows an application to read SMS messages
android.permission.RECEIVE_SMS	Allows an application to monitor incoming SMS messages, to record or perform processing on them
android.permission.RESTART_PACKAGES	This constant was deprecated in API level 8
android.permission.SEND_SMS	Allows an application to send SMS messages
android.permission.SET_WALLPAPER	Allows applications to set the wallpaper
android.permission.VIBRATE	Allows access to the vibrator
android.permission.WRITE_CONTACTS	Allows an application to write (but not read) the user's contacts data
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage
android.permission.WRITE_SMS	Allows an application to write SMS messages
com.android.browser.permission.READ_HISTORY_BOOKMARKS	Allows an application to read (but not write) the user's browsing history and bookmarks
com.android.browser.permission.WRITE_HISTORY_BOOKMARKS	Allows an application to write (but not read) the user's browsing history and bookmarks
com.android.launcher.permission.INSTALL_SHORTCUT	Allows an application to install a shortcut in Launcher

Used Permissions	Description	API calls
android.permission.ACCESS_FINE_LOCATION		android/location/LocationManager;->requestLocationUpdates
android.permission.ACCESS_NETWORK_STATE		android/net/ConnectivityManager;->getActiveNetworkInfo
android.permission.INTERNET		java/net/Socket
android.permission.READ_CONTACTS °	Allows an application to read the user's contacts data	android/content/ContentResolver;->query
android.permission.READ_PHONE_STATE		android/telephony/TelephonyManager;->getDeviceId
android.permission.RESTART_PACKAGES		android/app/ActivityManager;->restartPackage
android.permission.SEND_SMS		android/telephony/SmsManager;->sendTextMessage
android.permission.SET_WALLPAPER		android/content/Context;->setWallpaper
android.permission.VIBRATE		android/app/NotificationManager;->notify
android.permission.WAKE_LOCK °	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming	android/media/MediaPlayer;->start
com.android.browser.permission.WRITE_HISTORY_BOOKMARKS		android/provider/Browser/Landroid/net/Uri;BOOKMARKS_URI

Used Intents
android.intent.action.MAIN
android.intent.action.VIEW
android.intent.category.DEFAULT
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
cmp.netsentry.list.c.f	✔	✔	✔
cmp.netsentry.ui.ApplicationPreferences	✔	✔	✔
cmp.netsentry.ui.ChartInterfaceStats	✘	✔	✔
cmp.netsentry.ui.InterfaceStatsEditor	✔	✔	✔
cmp.netsentry.ui.InterfaceStatsList	✔	✔	✔

Services	Used	Provided by Android	Provided by Third-Parties
cmp.netsentry.list.c.AndroidIME	✘	✔	✘
com.android.vending.util.WorkService	✔	✔	
com.android.music.MediaPlaybackService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
cmp.netsentry.backend.Bootstrapper	✔	✔	✔
cmp.netsentry.backend.Resetter	✔	✔	✔
cmp.netsentry.backend.Updater	✔	✔	✔
cmp.netsentry.backend.scheduler.CronScheduler	✔	✔	✔
cmp.netsentry.list.f	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
cmp.netsentry.backend.InterfaceStatsProvider	✔		

Used Networks
-

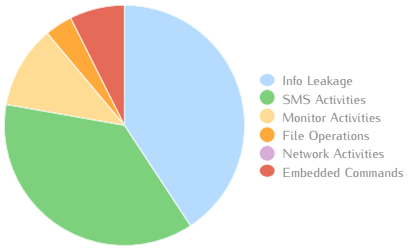
Network Analysis

Hardcoded URLs	IP	Region
schemas.android.com	-	-
maps.google.com	74.125.235.164	United States - Mountain View

Request	IP	Region	Type
android.clients.google.com	173.194.116.167	United States - Mountain View	HTTP POST / DNS
-	167.116.194.173.in-addr.arpa	-	DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	App_Info_Get	Retrieve package installation information
	Call_Query	List phone call records
	Contact_Query	List contacts
	GPS_Get	Retrieve GPS information
	Location_Get	Retrieve current phone location
	Location_Last_Get	Retrieve last phone location
	Network_NetProvider_Get	Retrieve network provider information
	Phone_IMEI_Get	Retrieve IMEI
	Phone_IMSI_Get	Retrieve IMSI
	Phone_Number_Get	Retrieve current phone number
	SMS_Query	List SMS
SMS Activities	App_Close	Close application
	Contact_Create	Create contact
	Contact_Erase	Delete contact
	Database_Erase	Delete database
	Notification_Send	Send notifications
	SMS_Analysis	Analysis SMS messages
	SMS_Create_Message	Create Inbox SMS
	SMS_Delete_Message	Delete Inbox SMS
	SMS_Erase	Delete SMS
	SMS_Send	Send SMS
Monitor Activities	Database_Spy	Spy database
	GPS_Spy	Spy GPS states
	Location_Spy	Spy location
File Operations	File_Erase	Delete file
Network Activities	-	
Embedded Commands	unix-compress	Compress file
	unix-mkdir	Make a directory
	unix-sleep	Suspend execution for a specified interval



Info Leakage	11
SMS Activities	10
Monitor Activities	3
File Operations	1
Network Activities	0
Embedded Commands	2

Jifake

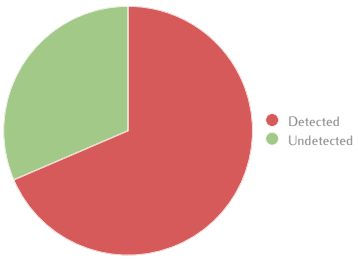
MD5	37a46aec9aa86831faa3ddb6b05a05f8
SHA-1	9440bb3da5e1ad862f357248b5da0c59dc7fc96b
SHA-256	16071d0a064cdca39672dcea0055aaa29750d4c5ba068b5d7b6df8922c5cfc93
API Level	3
File Dimension (MB)	1.19
Package Name	appinventor.ai_russ_support.JimmRussia
Other Names	9440bb3da5e1ad862f357248b5da0c59dc7fc96b
Used Features	android.hardware.touchscreen android.hardware.telephony

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.Jifake.A
Adobe Malware Classifier	
Aegislab	Jifake
Agnitum	Trojan.AndroidOS.Jifake.B
AhnLab-V3	Android-Malicious/FakeInst
ALYac	
Anchivia	
Antiy-AVL	
Anvisoft	
Anvisoft Cloud	
ArcaVir	Trojan.SMS.AndroidOS.Jifake.f
Avast	Android:SMSSend-X
AVG	Android_dc.AFOA
Avira	Android/Agent.CJ
AVware	Trojan.AndroidOS.Jifake.a
Baidu	Trojan.AndroidOS.FakeInst.avm
BitDefender	Android.Trojan.Jifake.A
Bkav	
ByteHero	
ClamAV	Andr.Jifake-9
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.37A46AEC!Olympus, AndroidOS/Steek.C
Digital Patrol	Trojan-SMS.AndroidOS.Jifake.f
DrWeb	Android.SmsSend.26
EmsiSoft	Android.Trojan.Jifake.A (B)
Epoolsoft	
eScan	Android.Trojan.Jifake.A[ZP]
F-Mirc	
F-Prot	AndroidOS/Steek.C
F-Secure	Trojan:Android/JiFake.gen!65232C
FileMedic	
FilsecLab Twister	Android.M.rlmd
Fortinet	Android/JiFake.A!tr.dial
GData	Android.Trojan.Jifake.A
GFI Vipre	Trojan.AndroidOS.Jifake.a
Ikarus	Trojan.AndroidOS.Jifake
Immunos	Andr.Jifake-9
Jiangmin	Backdoor/AndroidOS.cpv
K7 Antivirus	
K7GW Antivirus	Trojan (0049697d1)
Kaspersky	HEUR:Trojan-SMS.AndroidOS.FakeInst.a
Kingsoft	Win32.Troj.Undef.(kcloud), Android.Troj.at_jifake.b.(kcloud)
MalwareBytes	
McAfee	Android/SMS.gen
McAfee Artemis	Artemis!37A46AEC9AA8
McAfee GW	Android/SMS.gen
Microsoft	Trojan:AndroidOS/Jifake.B
NANO AntiVirus	Trojan.Android.FakeInst.cxcmjj
NOD32	Android/TrojanSMS.Agent.E
NoraLabs NoraScan	
Norman	
Norton Symantec	Android.Premiumtext
nProtect	
OfficeMalScanner	

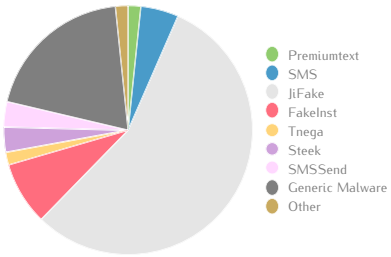
Antivirus	Result
Panda	Trj/Jifake.A
PathFinder	Malware
Preventon	Andr/Jifake-C
Protector Plus	Trojan.AndroidOS.Jifake.B
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Android.Jifake.F
RHBVS	
Rising	NORMAL:Trojan.Agent.gar!1612501
Rising Cloud	
SecureIT	Android.Trojan.Jifake.A
Segurmatica	
Segurmatica KE	HEUR:Trojan-SMS.AndroidOS.FakeInst.a
Solo	
Sophos	Andr/Jifake-C
SUPERAntiSpyware	
Team Cymru	Malware
The Cleaner	
The Hacker	
TotalDefense	AndroidOS/Tnega.cEVFZE
TotalDefense Cloud	Java/Jifake!CKbJIW
Tencent	Trojan.Android.Agent.CB4631F0
Trend Micro	AndroidOS_JIFAKE.E, Android.041E7BDC
Trend Micro-Housecall	AndroidOS_JIFAKE.E
TrustPort	Android.Trojan.Jifake.A
TT Livescan	
VBA32	Trojan-SMS.AndroidOS.Jifake.f
Vexira	Trojan.AndroidOS.Jifake.B
VirIT eXplorer	Android.Trj.JiFake.A
VIRobot	Android.Trojan.Jifake.A[b]
VirusBuster	Trojan.AndroidOS.Jifake.B
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.Jifake.F

Detected	61
Undetected	28
Sum	89



Name Distribution

Name	Amount	Score
Premiumtext	1	0
SMS	3	1
JiFake	34	3
FakeInst	5	2
Tnega	1	0
Steek	2	0
SMSSend	2	0
Generic Malware	12	1
Other	1	1
Sum	**61**	



Average Score	1,12

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.INTERNET	Allows applications to open network sockets
android.permission.RECEIVE_SMS	Allows an application to monitor incoming SMS messages, to record or perform processing on them
android.permission.SEND_SMS	Allows an application to send SMS messages

Used Permissions	Description	API calls
android.permission.ACCESS_FINE_LOCATION °	Allows an app to access precise location from location sources such as GPS, cell towers, and WI-FI	android/location/LocationManager;->requestLocationUpdates
android.permission.CHANGE_COMPONENT_ENABLED_STATE °	Allows an application to change whether an application component (other than its own) is enabled or not	android/content/pm/PackageManager;->setComponentEnabledSetting
android.permission.GET_ACCOUNTS °	Allows access to the list of accounts in the Accounts Service	android/accounts/AccountManager;->getAccounts
android.permission.INTERNET		java/net/ServerSocket
android.permission.MANAGE_ACCOUNTS °	Allows an application to manage the list of accounts in the AccountManager	android/accounts/AccountManager;->invalidateAuthToken
android.permission.READ_CONTACTS °	Allows an application to read the user's contacts data	android/content/ContentResolver;->query
android.permission.READ_LOGS °	Allows an application to read the low-level system log files	java/lang/Runtime;->exec
android.permission.RECORD_AUDIO °	Allows an application to record audio	android/media/MediaRecorder;->setAudioSource
android.permission.SEND_SMS		android/telephony/gsm/SmsManager;->sendTextMessage
android.permission.USE_CREDENTIALS °	Allows an application to request authtokens from the AccountManager	android/accounts/AccountManager;->getAuthToken
android.permission.VIBRATE °	Allows access to the vibrator	android/app/NotificationManager;->notify
android.permission.WAKE_LOCK °	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming	android/media/MediaPlayer;->start

Used Intents
android.intent.action.MAIN
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
appinventor.ai_russ_support.JimmRussia.Screen1	✔	✔	✔
com.google.devtools.simple.runtime.components.android.ListPickerActivity	✘	✔	✘
com.google.devtools.simple.runtime.components.android.WebViewActivity	✘	✔	✔

Services	Used	Provided by Android	Provided by Third-Parties
com.android.vending.util.WorkService	✔	✔	
com.android.musicfx.Compatibility$Service	✔	✔	
com.android.music.MediaPlaybackService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
-			

Providers	Used	Provided by Android	Provided by Third-Parties
-			

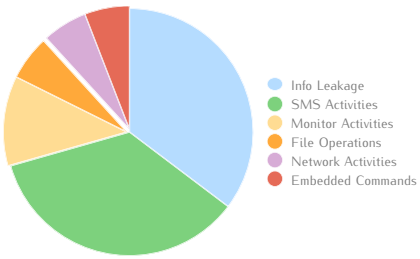
Used Networks
-

Network Analysis

Hardcoded URLs	IP	Region
www.gnu.org	208.118.235.148	United States - Boston
kawa.gnu.org	-	-
www.w3.org	128.30.52.45	United States - Cambridge
twitter.com	199.16.156.198	United States - San Francisco
appinvtingwebdb.appspot.com	173.194.67.141	United States - Mountain View
developer.android.com	74.125.232.128	United States - Mountain View
www.google.com	74.125.232.142	United States - Mountain View
appinvgameserver.appspot.com	173.194.67.141	United States - Mountain View
www.facebook.com	173.252.120.6	United States - Palo Alto
androvote.appspot.com	173.194.767.141	United States - Mountain View
smshelp.su	144.76.40.132	Germany - Kiez
Jimm5.ru	109.70.26.37	Russian Federation
stream.twitter.com	199.16.156.217	United States - San Francisco
status.twitter.com	66.6.44.4	United States - New York
yusuke.homeip.net	124.213.71.220	Japan
www.cs.caltech.edu	131.215.140.26	United States - Pasadena
schemas.xmlsoap.org	65.52.103.126	United States - Redmond

Potentially Dangerous Operations

	Name	Description
Info Leakage	Call_Query	List phone call records
	Contact_Get	Get contact
	Contact_Query	List contacts
	GPS_Get	Retrieve GPS information
	Location_Get	Retrieve current phone location
	Location_Last_Get	Retrieve last phone location
SMS Activities	Contact_Create	Create contact
	SMS_Analysis	Analysis SMS messages
	SMS_Create_Message	Create Inbox SMS
	SMS_Query	List SMS
	SMS_Send	Send "744155jimm" to 2476 (2 times)
Monitor Activities	GPS_Spy	Spy GPS states
	Location_Spy	Spy location
File Operations	File_Erase	Delete file
Network Activities	Network_Access	Access network
Embedded Commands	unix-sleep	Suspend execution for a specified interval



Info Leakage	6
SMS Activities	6
Monitor Activities	2
File Operations	1
Network Activities	1
Embedded Commands	1

OBad A

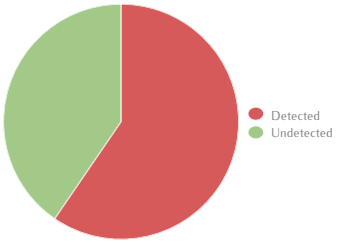
MD5	e1064bfd836e4c895b569b2de4700284
SHA-1	40b3abcc27be12e6d091fd4db83e15f9e06fa027
SHA-256	b65c352d44fa1c73841c929757b3ae808522aa2ee3fd0a3591d4ab6759ff8d17
API Level	1
File Dimension (MB)	0.08
Package Name	com.android.system.admin
Other Names	mms1 E1064BFD836E4C895B569B2DE4700284 b65c352d44fa1c73841c929757b3ae808522aa2ee3fd0a3591d4ab6759ff8d17 2
Used Features	android.hardware.bluetooth android.hardware.wifi android.hardware.telephony android.hardware.touchscreen

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.Obad.A
Adobe Malware Classifier	
Aegislab	Obad
Agnitum	
AhnLab-V3	Android-Malicious/Obad
ALYac	
Anchivia	
Antiy-AVL	Backdoor/AndroidOS.Obad[:vcsii]
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Android:Obad-A
AVG	Android/Deng.OD
Avira	Android/Obad.a.3
AVware	Trojan.AndroidOS.Generic.A
Baidu	Backdoor.AndroidOS.Obad.aLb
BitDefender	Android.Trojan.Obad.A
Bkav	
ByteHero	
ClamAV	Andr.Trojan.Obad
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/Obad.A
Digital Patrol	Backdoor.AndroidOS.Obad.a
DrWeb	Android.Siggen.1.origin
EmsiSoft	Trojan.Android.Obad (A)
Epoolsoft	
eScan	Android.Trojan.Obad.A
F-Mirc	
F-Prot	AndroidOS/Obad.A
F-Secure	Trojan:Android/Obad.A
FileMedic	
FilsecLab Twister	Android.Obad.A.vxtr
Fortinet	Android/Obad.A
GData	Android.Trojan.Obad.A
GFI Vipre	Trojan.AndroidOS.Generic.A
Ikarus	Backdoor.AndroidOS.Obad
Immunos	Andr.Trojan.Obad
Jiangmin	
K7 Antivirus	Trojan (0001140e1)
K7GW Antivirus	Trojan (0001140e1)
Kaspersky	HEUR:Backdoor.AndroidOS.Obad.a
Kingsoft	Android.Troj.Obad.a.(kcloud)
MalwareBytes	
McAfee	Android/Obad
McAfee Artemis	Android/Obad
McAfee GW	Android/Obad
Microsoft	
NANO AntiVirus	Trojan.Android.Obad.dfttjr
NOD32	Android/Obad.A
NoraLabs NoraScan	
Norman	Obad.B
Norton Symantec	Android.Obad
nProtect	
OfficeMalScanner	

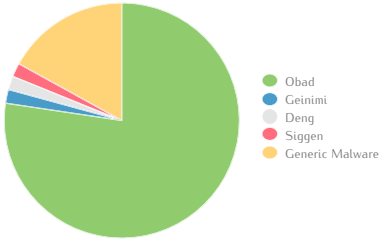
Antivirus	Result
Panda	
PathFinder	Malware
Preventon	Andr/Obad-A
Protector Plus	
PSafe Antivirus	Android.Trojan.Obad.A
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Android.Obad.A
RHBVS	
Rising	DEX:System.Geimini!1.9DA5
Rising Cloud	
SecureIT	Android.Trojan.Obad.A
Segurmatica	
Segurmatica KE	HEUR:Backdoor.AndroidOS.Obad.a
Solo	
Sophos	Andr/Obad-A
SUPERAntiSpyware	
Team Cymru	Malware
The Cleaner	
The Hacker	
TotalDefense	
TotalDefense Cloud	
Tencent	Dos.Backdoor.Obad.Afqs
Trend Micro	AndroidOS_OBAD.A
Trend Micro-Housecall	AndroidOS_OBAD.A
TrustPort	
TT Livescan	
VBA32	
Vexira	
VirIT eXplorer	Android.Bkd.Obad.A
VIRobot	Android.Trojan.Obad.A[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.Obad.A

Detected	53
Undetected	36
Sum	89



Name Distribution

Name	Amount	Score
Obad	41	3
Geinimi	1	0
Deng	1	0
Siggen	1	0
Generic Malware	9	1
Sum	**53**	



Average Score	1,08

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_BLUETOOTH_SHARE	-
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.ACCESS_WIFI_STATE	Allows applications to access information about WI-FI networks
android.permission.BLUETOOTH	Allows applications to connect to paired bluetooth devices
android.permission.BLUETOOTH_ADMIN	Allows applications to discover and pair bluetooth devices
android.permission.CALL_PHONE	Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call being placed.
android.permission.CHANGE_NETWORK_STATE	Allows applications to change network connectivity state
android.permission.CHANGE_WIFI_STATE	Allows applications to change Wi-Fi connectivity state
android.permission.INTERNET	Allows applications to open network sockets
android.permission.MODIFY_PHONE_STATE	Allows modification of the telephony state - power on, mmi, etc.
android.permission.PROCESS_OUTGOING_CALLS	Allows an application to see the number being dialed during an outgoing call with the option to redirect the call to a different number or abort the call altogether
android.permission.READ_CONTACTS	Allows an application to read the user's contacts data
android.permission.READ_EXTERNAL_STORAGE	Allows an application to read from external storage
android.permission.READ_LOGS	Allows an application to read the low-level system log files
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.READ_SMS	Allows an application to read SMS messages
android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting
android.permission.RECEIVE_SMS	Allows an application to monitor incoming SMS messages, to record or perform processing on them
android.permission.SEND_SMS	Allows an application to send SMS messages
android.permission.WAKE_LOCK	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage
android.permission.WRITE_SECURE_SETTINGS	Allows an application to read or write the secure system settings
android.permission.WRITE_SETTINGS	Allows an application to read or write the system settings
android.permission.WRITE_SMS	Allows an application to write SMS messages

Used Permissions	Description	API calls
android.permission.READ_LOGS		java/lang/Runtime;->exec

Used Intents
android.intent.action.BOOT_COMPLETED
android.intent.action.DATE_CHANGED
android.intent.action.MAIN
android.intent.action.NEW_OUTGOING_CALL
android.intent.action.PHONE_STATE
android.intent.action.QUICKBOOT_POWERON
android.intent.action.TIME_CHANGED
android.intent.action.TIME_SET
android.intent.action.TIMEZONE_CHANGED
android.intent.action.USER_PRESENT
android.intent.category.DEFAULT
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.android.system.admin.CCOloll	✔	✔	✔
com.android.system.admin.cCoIOlOo	✔	✔	✘

Services	Used	Provided by Android	Provided by Third-Parties
com.android.system.admin.MainService	✔	✔	✘
com.android.system.admin.OCICooCl	✔	✔	✔
com.android.system.admin.OCOcCOll	✔	✔	✘
com.android.vending.util.WorkService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
com.android.system.admin.ClCoICCo	✔	✔	✔
com.android.system.admin.CoccOlo	✔	✔	✔
com.android.system.admin.ICcIllo	✔	✔	✔
com.android.system.admin.IOOICOcl	✔	✔	✔
com.android.system.admin.OCllCoO	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
android.provider.Telephony.SMS_RECEIVED	✔	✔	

Used Networks
-

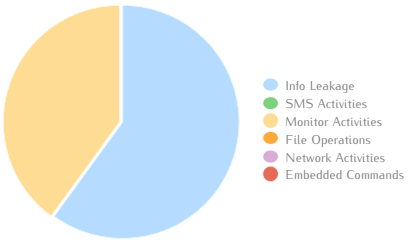
Network Analysis

Hardcoded URLs	IP	Region
schemas.android.com	-	-

Request	IP	Region	Type
www.google.com	173.194.112.212	United States - Mountain View	DNS
www.androfox.com	91.216.163.131	Lithuania	HTTP POST / DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	Call_Query	List phone call records
	Contact_Query	List contacts
	SMS_Query	List SMS
SMS Activities	-	
Monitor Activities	Database_Spy	Spy database
	SMS_Spy	Spy SMS
File Operations	-	
Network Activities	-	
Embedded Commands	-	



Info Leakage	3
SMS Activities	0
Monitor Activities	2
File Operations	0
Network Activities	0
Embedded Commands	0

OBad B

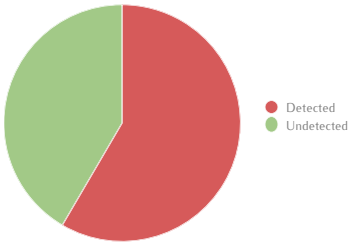
MD5	f7be25e4f19a3a82d2e206de8ac979c8
SHA-1	a2ba1bacc996b90b37a2c93089692bf5f30f1d68
SHA-256	ba1d6f317214d318b2a4e9a9663bc7ec867a6c845affecad1290fd717cc74f29
API Level	1
File Dimension (MB)	0.08
Package Name	com.android.system.admin
Other Names	F7BE25E4F19A3A82D2E206DE8AC979C8 ba1d6f317214d318b2a4e9a9663bc7ec867a6c845affecad1290fd717cc74f29
Used Features	android.hardware.bluetooth android.hardware.wifi android.hardware.telephony android.hardware.touchscreen

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.Obad.A
Adobe Malware Classifier	
Aegislab	Obad
Agnitum	
AhnLab-V3	Android-Malicious/Obad
ALYac	
Anchivia	
Antiy-AVL	Backdoor/AndroidOS.Obad[:vcsii]
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Android:Obad-A
AVG	Android/Deng.OD
Avira	Android/Obad.a.2 *
AVware	Trojan.AndroidOS.Generic.A
Baidu	Backdoor.AndroidOS.Obad.AdT *, Trojan.Android.Obad.b
BitDefender	Android.Trojan.Obad.A
Bkav	
ByteHero	
ClamAV	Andr.Trojan.Obad
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.F7BE25E4!Olympus *, AndroidOS/Obad.B *
Digital Patrol	Backdoor.AndroidOS.Obad.a
DrWeb	Android.Siggen.1.origin
EmsiSoft	Trojan.Android.Obad (A)
Epoolsoft	
eScan	Android.Trojan.Obad.A
F-Mirc	
F-Prot	AndroidOS/Obad.B *
F-Secure	Trojan:Android/Obad.A
FileMedic	
FilsecLab Twister	Backdoor.AndroidOS.Obad.a.qvfl *
Fortinet	Android/Obad.A
GData	Android.Trojan.Obad.A
GFI Vipre	Trojan.AndroidOS.Generic.A
Ikarus	Backdoor.AndroidOS.Obad
Immunos	Andr.Trojan.Obad
Jiangmin	
K7 Antivirus	Trojan (0001140e1)
K7GW Antivirus	Trojan (0001140e1)
Kaspersky	HEUR:Backdoor.AndroidOS.Obad.a
Kingsoft	Android.Troj.Obad.a.(kcloud)
MalwareBytes	
McAfee	Android/Obad
McAfee Artemis	Android/Obad
McAfee GW	Android/Obad
Microsoft	
NANO AntiVirus	Trojan.Android.Obad.dfttmg *
NOD32	Android/Obad.B *
NoraLabs NoraScan	
Norman	Obad.B
Norton Symantec	Android.Obad
nProtect	
OfficeMalScanner	

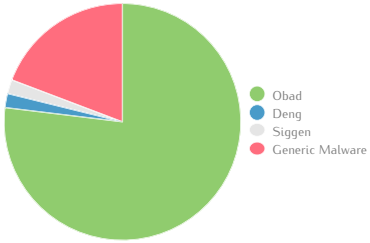
Antivirus	Result
Panda	
PathFinder	Malware
Preventon	Andr/Obad-A
Protector Plus	
PSafe Antivirus	Android.Trojan.Obad.A
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Android.Obad.A
RHBVS	
Rising	NORMAL:Trojan.Agent.fxr!1612421 *£
Rising Cloud	
SecureIT	*NO MALWARE $*
Segurmatica	
Segurmatica KE	HEUR:Backdoor.AndroidOS.Obad.a
Solo	
Sophos	Andr/Obad-A
SUPERAntiSpyware	
Team Cymru	Malware
The Cleaner	
The Hacker	
TotalDefense	
TotalDefense Cloud	
Tencent	Dos.Backdoor.Obad.Efba *
Trend Micro	AndroidOS_OBAD.A
Trend Micro-Housecall	AndroidOS_OBAD.A
TrustPort	
TT Livescan	
VBA32	
Vexira	
VirIT eXplorer	Android.Bkd.Obad.B *
VIRobot	Android.Trojan.Obad.A[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.Obad.A

Detected	52
Undetected	37
Sum	89



Name Distribution

Name	Amount	Score
Obad	40	3
Deng	1	0
Siggen	1	0
Generic Malware	10	1
Sum	**52**	



Average Score	1,04

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_BLUETOOTH_SHARE	-
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks
android.permission.ACCESS_WIFI_STATE	Allows applications to access information about WI-FI networks
android.permission.BLUETOOTH	Allows applications to connect to paired bluetooth devices
android.permission.BLUETOOTH_ADMIN	Allows applications to discover and pair bluetooth devices
android.permission.CALL_PHONE	Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call being placed.
android.permission.CHANGE_NETWORK_STATE	Allows applications to change network connectivity state
android.permission.CHANGE_WIFI_STATE	Allows applications to change Wi-Fi connectivity state
android.permission.INTERNET	Allows applications to open network sockets
android.permission.MODIFY_PHONE_STATE	Allows modification of the telephony state - power on, mmi, etc.
android.permission.PROCESS_OUTGOING_CALLS	Allows an application to see the number being dialed during an outgoing call with the option to redirect the call to a different number or abort the call altogether
android.permission.RAISED_THREAD_PRIORITY	-
android.permission.READ_CONTACTS	Allows an application to read the user's contacts data
android.permission.READ_EXTERNAL_STORAGE	Allows an application to read from external storage
android.permission.READ_LOGS	Allows an application to read the low-level system log files
android.permission.READ_PHONE_STATE	Allows read only access to phone state
android.permission.READ_SMS	Allows an application to read SMS messages
android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting
android.permission.RECEIVE_SMS	Allows an application to monitor incoming SMS messages, to record or perform processing on them
android.permission.SEND_SMS	Allows an application to send SMS messages
android.permission.WAKE_LOCK	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage
android.permission.WRITE_SECURE_SETTINGS	Allows an application to read or write the secure system settings
android.permission.WRITE_SETTINGS	Allows an application to read or write the system settings
android.permission.WRITE_SMS	Allows an application to write SMS messages

Used Permissions	Description	API calls
android.permission.READ_LOGS		java/lang/Runtime;->exec

Used Intents
android.intent.action.BOOT_COMPLETED
android.intent.action.DATE_CHANGED
android.intent.action.MAIN
android.intent.action.NEW_OUTGOING_CALL
android.intent.action.PHONE_STATE
android.intent.action.QUICKBOOT_POWERON
android.intent.action.TIME_CHANGED
android.intent.action.TIME_SET
android.intent.action.TIMEZONE_CHANGED
android.intent.action.USER_PRESENT
android.intent.category.DEFAULT
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.android.system.admin.CCOIoll	✔	✔	✔
com.android.system.admin.cCoIOlOo	✔	✔	✘

Services	Used	Provided by Android	Provided by Third-Parties
com.android.system.admin.AdminService	✔	✔	✘
com.android.system.admin.CCOIoCco	✔	✔	✔
com.android.system.admin.MainService	✔	✔	✘
com.android.music.MediaPlaybackService	✔	✔	
com.android.vending.util.WorkService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
com.android.system.admin.AdminReceiver	✔	✔	✔
com.android.system.admin.CIcIoICo	✔	✔	✔
com.android.system.admin.OOOOIIO	✔	✔	✔
com.android.system.admin.OIOCIICI	✔	✔	✔
com.android.system.admin.OooOOOo	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
android.provider.Telephony.SMS_RECEIVED	✔	✔	

Used Networks
-

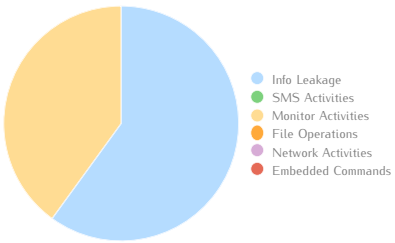
Network Analysis

Hardcoded URLs	IP	Region
schemas.android.com	-	-

Request	IP	Region	Type
www.google.com	173.194.112.212	United States - Mountain View	DNS
www.androfox.com	91.216.163.131	Lithuania	HTTP POST / DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	Call_Query	List phone call records
	Contact_Query	List contacts
	SMS_Query	List SMS
SMS Activities	-	
Monitor Activities	Database_Spy	Spy database
	SMS_Spy	Spy SMS
File Operations	-	
Network Activities	-	
Embedded Commands	-	



Info Leakage	3
SMS Activities	0
Monitor Activities	2
File Operations	0
Network Activities	0
Embedded Commands	0

Zsone A

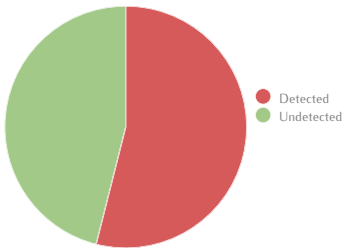
MD5	944cbd53a174dcbb0e1e3d0832cac465
SHA-1	14f5c14af60b5930f9dfbeed30f5529ba814c0e6
SHA-256	00f4fa52f37037efb710c18b7d7ae7708a27ab1bea333e99cdcbd680eb32408b
API Level	3
File Dimension (MB)	0.23
Package Name	com.mj.iMatch
Other Names	14f5c14af60b5930f9dfbeed30f5529ba814c0e6
Used Features	android.hardware.location android.hardware.location.network android.hardware.telephony android.hardware.touchscreen android.hardware.screen.portrait

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.Zsone.A
Adobe Malware Classifier	
Aegislab	zsone
Agnitum	
AhnLab-V3	Android-Malicious/Zsone
ALYac	
Anchivia	
Antiy-AVL	Trojan/AndroidOS.Raden[SMS]
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Android:Zsone-B
AVG	Android_dc.AFXT
Avira	Android/Malmix.8
AVware	Trojan.AndroidOS.Raden.a
Baidu	Trojan.AndroidOS.Raden.aP
BitDefender	Android.Trojan.Zsone.A
Bkav	
ByteHero	
ClamAV	Andr.Zsone-5
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.944CBD53!Olympus, AndroidOS/Raden.A
Digital Patrol	Trojan-SMS.AndroidOS.Raden.f
DrWeb	
EmsiSoft	Android.Trojan.Zsone.A (B)
Epoolsoft	
eScan	Android.Trojan.Zsone.A[ZP]
F-Mirc	
F-Prot	AndroidOS/Raden.A
F-Secure	
FileMedic	
FilsecLab Twister	Android.M.dmsw
Fortinet	W32/Malware_fam.NB
GData	Android.Trojan.Zsone.A
GFI Vipre	Trojan.AndroidOS.Raden.a
Ikarus	Trojan.AndroidOS.Zsone
Immunos	Andr.Trojan.Zsone
Jiangmin	Trojan/AndroidOS.ar
K7 Antivirus	
K7GW Antivirus	Trojan (0001140e1)
Kaspersky	HEUR:Trojan-SMS.AndroidOS.Raden.v
Kingsoft	Android.Troj.hh_Raden.a.(kcloud), Troj.Randen.a.(kcloud)
MalwareBytes	
McAfee	
McAfee Artemis	Artemis!944CBD53A174
McAfee GW	
Microsoft	
NANO AntiVirus	
NOD32	Android/Zsone.A
NoraLabs NoraScan	
Norman	Suspicious_Gen3.ABWRO
Norton Symantec	
nProtect	
OfficeMalScanner	

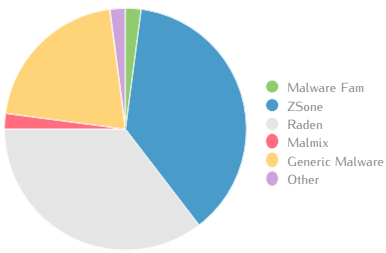
Antivirus	Result
Panda	
PathFinder	Malware
Preventon	Andr/Raden-A
Protector Plus	
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Android.Raden.B
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Trojan.Zsone.A
Segurmatica	
Segurmatica KE	HEUR:Trojan-SMS.AndroidOS.Raden.v
Solo	
Sophos	Andr/Raden-A
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	AndroidOS/Raden.VGDbHEC
TotalDefense Cloud	AndroidOS/Trojan!CVcEGV
Tencent	Dos.Trojan-sms.Raden.Hrou
Trend Micro	AndroidOS_ZSONE.A, Android.0427E578
Trend Micro-Housecall	AndroidOS_ZSONE.A
TrustPort	Android.Trojan.Zsone.A
TT Livescan	
VBA32	Trojan-SMS.AndroidOS.Raden.f
Vexira	
VirIT eXplorer	Android.Trj.Raden.B
VIRobot	Android.Trojan.Zsone.A[b]
VirusBuster	
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.Zsone.A

Detected	48
Undetected	41
Sum	89



Name Distribution

Name	Amount	Score
Malware Fam	1	0
ZSone	18	3
Raden	17	2
Malmix	1	0
Generic Malware	10	1
Other	1	1
Sum	**48**	



Average Score	0,65

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_COARSE_LOCATION	Allows an app to access approximate location derived from network location sources such as cell towers and WI-FI
android.permission.INTERNET	Allows applications to open network sockets
android.permission.RECEIVE_SMS	Allows an application to monitor incoming SMS messages, to record or perform processing on them
android.permission.RESTART_PACKAGES	This constant was deprecated in API level 8
android.permission.SEND_SMS	Allows an application to send SMS messages

Used Permissions	Description	API calls
android.permission.ACCESS_FINE_LOCATION °	Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.	android/location/LocationManager;->getBestProvider
android.permission.INTERNET		java/net/HttpURLConnection
android.permission.SEND_SMS		android/telephony/gsm/SmsManager;->sendTextMessage
android.permission.VIBRATE °	Allows access to the vibrator	android/media/AudioManager/getRingerMode()

Used Intents
android.intent.action.MAIN
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.admob.android.ads.AdMobActivity	✔	✔	✘
com.mj.iMatch.IMatch	✔	✔	✔

Services	Used	Provided by Android	Provided by Third-Parties
com.android.music.MediaPlaybackService	✔	✔	
com.android.vending.util.WorkService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
com.admob.android.ads.analytics.InstallReceiver	✔	✔	✔
com.mj.utils.MJReceiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
android.provider.Telephony.SMS_RECEIVED	✔	✔	

Used Networks
-

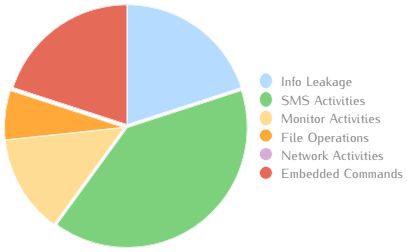
Network Analysis

Hardcoded URLs	IP	Region
schemas.android.com	-	-
mm.admob.com	70.32.132.54	United States - Mountain View
a.admob.com	165.193.245.52	United States - Mountain View
api.admob.com	165.193.245.41	United States - Mountain View
r.admob.com	-	-

Request	IP	Region	Type
api.admob.com	165.193.245.41	United States - Mountain View	HTTP GET / DNS
r.admob.com	-	-	DNS
mm.admob.com	70.32.132.54	United States - Mountain View	HTTP GET / DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	GPS_Get	Retrieve GPS information
	Location_Get	Retrieve current phone location
	Location_Last_get	Retrieve last phone location
SMS Activities	SMS_Analysis	Analysis SMS messages
	SMS_Intercept	Intercept SMS
	SMS_Send	Send "M6307AHD" to 10621900
		Send "aAHD" to 10626213
		Send "95pAHD" to 106691819
		Send "58#28AHD" to 10665123085
Monitor Activities	GPS_Spy	Spy GPS states
	Location_Spy	Spy location
File Operations	File_Erase	Delete file
Network Activities	-	
Embedded Commands	-	



Info Leakage	3
SMS Activities	6
Monitor Activities	2
File Operations	1
Network Activities	0
Embedded Commands	3

Zsone B

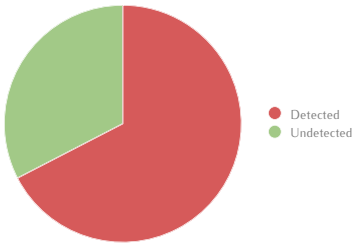
MD5	16c69031a4891c34f0458402de268975
SHA-1	c6e0d09385ee631b4245a1dd9c2e74c4772c026b
SHA-256	cd6ed0f9c19d71274b8b068f73d7188adbfce27ea6a5f4f71a2e3ac558dc1e57
API Level	3
File Dimension (MB)	0.35
Package Name	com.RZStudio.iMine
Other Names	c6e0d09385ee631b4245a1dd9c2e74c4772c026b
Used Features	android.hardware.location android.hardware.location.network android.hardware.telephony android.hardware.touchscreen android.hardware.screen.portrait

Antivirus Scan

Antivirus	Result
Ad-Aware	Android.Trojan.Zsone.A
Adobe Malware Classifier	
Aegislab	zsone
Agnitum	*Trojan.AndroidOS.Zsone.A #*
AhnLab-V3	Android-Malicious/Zsone
ALYac	
Anchivia	
Antiy-AVL	*NO MALWARE $*
Anvisoft	
Anvisoft Cloud	
ArcaVir	
Avast	Android:Raden-D [Trj] *^
AVG	Generic5_c.EVK *, Android_mc.GEB *
Avira	Android/Malmix.16 *
AVware	Trojan.AndroidOS.Raden.a
Baidu	Trojan.AndroidOS.Raden.AF *
BitDefender	Android.Trojan.Zsone.A
Bkav	
ByteHero	
ClamAV	Andr.Trojan.Zsone *
CMC	
Comodo	Malware
Comodo Cloud	Malware
Cyren	AndroidOS/GenBl.16C69031!Olympus, * AndroidOS/Zsone.A *£
Digital Patrol	Trojan-SMS.AndroidOS.Zsone.a *£
DrWeb	*Android.SmsSend.110.origin #*
EmsiSoft	Android.Trojan.Zsone.A (B)
Epoolsoft	
eScan	Android.Trojan.Zsone.A[ZP]
F-Mirc	
F-Prot	AndroidOS/Zsone.A *£
F-Secure	*Trojan:Android/Zsone.A #*
FileMedic	
FilsecLab Twister	Android.M.dltm *
Fortinet	Android/Smstibook.A!tr *
GData	Android.Trojan.Zsone.A
GFI Vipre	Trojan.AndroidOS.Raden.a
Ikarus	Trojan.AndroidOS.Zsone, AndroidOS.Suspect.Manifest *
Immunos	Andr.Trojan.Zsone
Jiangmin	Trojan/AndroidOS.ao *
K7 Antivirus	*Trojan (00352b231) #*
K7GW Antivirus	Trojan (00352b231) *
Kaspersky	HEUR:Trojan-SMS.AndroidOS.Raden.v
Kingsoft	Android.Troj.hh_Raden.a.(kcloud), Troj.Randen.a.(kcloud)
MalwareBytes	
McAfee	*Generic.hu #*
McAfee Artemis	Artemis!16C69031A489 *
McAfee GW	*Generic.hu #*
Microsoft	*Trojan:AndroidOS/Raden.A #*
NANO AntiVirus	*Trojan.Android.Raden.dgeliw #*
NOD32	Android/Zsone.A
NoraLabs NoraScan	
Norman	Suspicious_Gen3.ACPZY *
Norton Symantec	*Android.Hippo #*
nProtect	
OfficeMalScanner	

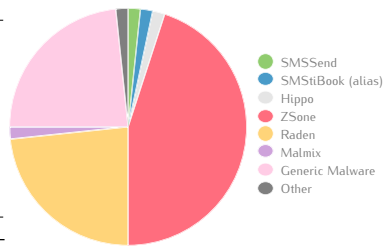
Antivirus	Result
Panda	*Generic Malware #*
PathFinder	Malware
Preventon	Andr/Raden-A
Protector Plus	*Trojan.AndroidOS.Zsone.A #*
PSafe Antivirus	
Qihoo 360	Trojan.Generic
Quick Heal (Cat)	Android.Raden.A *
RHBVS	
Rising	
Rising Cloud	
SecureIT	Android.Trojan.Zsone.A
Segurmatica	
Segurmatica KE	HEUR:Trojan-SMS.AndroidOS.Raden.v
Solo	
Sophos	Andr/Raden-A
SUPERAntiSpyware	
Team Cymru	
The Cleaner	
The Hacker	
TotalDefense	AndroidOS/Zsone.A *£
TotalDefense Cloud	AndroidOS/Trojan!CYaEGV *, AndroidOS/Trojan!CbaEGV *
Tencent	Dos.Trojan-sms.Raden.Dzuc *
Trend Micro	AndroidOS_ZSONE.A, Android.0427E578
Trend Micro-Housecall	AndroidOS_ZSONE.A
TrustPort	Android.Trojan.Zsone.A
TT Livescan	
VBA32	Trojan-SMS.AndroidOS.Zsone.a *£
Vexira	*Trojan.AndroidOS.Zsone.A #*
VirIT eXplorer	Android.Trj.Raden.M *
VIRobot	Android.Trojan.Zsone.A[b]
VirusBuster	*Trojan.AndroidOS.Zsone.A #*
Zillya!	
Zoner Antivirus	Trojan.AndroidOS.Zsone.A

Detected	60
Undetected	29
Sum	89



Name Distribution

Name	Amount	Score
SMSSend	1	0
SMStiBook (alias)	1	3
Hippo	1	0
ZSone	27	3
Raden	14	2
Malmix	1	0
Generic Malware	14	1
Other	1	1
Sum	**60**	



Average Score	1,10

Used Elements Analysis

AndroidManifest.xml Permissions	Description
android.permission.ACCESS_COARSE_LOCATION	Allows an app to access approximate location derived from network location sources such as cell towers and WI-FI
android.permission.INTERNET	Allows applications to open network sockets
android.permission.RECEIVE_SMS	Allows an application to monitor incoming SMS messages, to record or perform processing on them
android.permission.RESTART_PACKAGES	This constant was deprecated in API level 8
android.permission.SEND_SMS	Allows an application to send SMS messages

Used Permissions	Description	API calls
android.permission.ACCESS_FINE_LOCATION °	Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.	android/location/LocationManager;->getBestProvider
android.permission.INTERNET		java/net/HttpURLConnection
android.permission.SEND_SMS		android/telephony/gsm/SmsManager;->sendTextMessage
android.permission.VIBRATE °	Allows access to the vibrator	android/media/AudioManager/getRingerMode()

Used Intents
android.intent.action.MAIN
android.intent.category.LAUNCHER

Activities	Used	Provided by Android	Provided by Third-Parties
com.admob.android.ads.AdMobActivity	✔	✔	✘
com.RZStudio.iMine.Mine	✔	✔	✔

Services	Used	Provided by Android	Provided by Third-Parties
com.android.music.MediaPlaybackService	✔	✔	
com.android.vending.util.WorkService	✔	✔	

Receivers	Used	Provided by Android	Provided by Third-Parties
com.admob.android.ads.analytics.InstallReceiver	✔	✔	✔
com.RZStudio.iMine.SmsReceiver	✔	✔	✔

Providers	Used	Provided by Android	Provided by Third-Parties
android.provider.Telephony.SMS_RECEIVED	✔	✔	

Used Networks
-

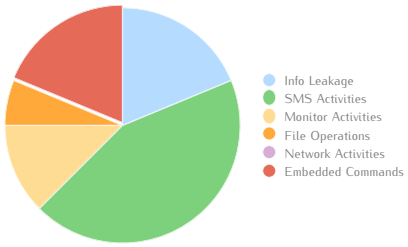
Network Analysis

Hardcoded URLs	IP	Region
schemas.android.com	-	-
mm.admob.com	70.32.132.54	United States - Mountain View
a.admob.com	165.193.245.52	United States - Mountain View
api.admob.com	165.193.245.41	United States - Mountain View
r.admob.com	-	-

Request	IP	Region	Type
api.admob.com	165.193.245.41	United States - Mountain View	HTTP GET / DNS
r.admob.com	-	-	DNS
mm.admob.com	70.32.132.54	United States - Mountain View	HTTP GET / DNS

Potentially Dangerous Operations

	Name	Description
Info Leakage	GPS_Get	Retrieve GPS information
	Location_Get	Retrieve current phone location
	Location_Last_get	Retrieve last phone location
SMS Activities	SMS_Analysis	Analysis SMS messages
	SMS_Intercept	Intercept SMS
	SMS_Send	Send "YXX1" to 106601412004 (2 times)
		Send "921X1" to 1066185829 (2 times)
		Send "C "X1" to 1066953930
Monitor Activities	GPS_Spy	Spy GPS states
	Location_Spy	Spy location
File Operations	File_Erase	Delete file
Network Activities	-	
Embedded Commands	unix-compress	Compress a file
	unix-mkdir	Make a directory
	unix-su	Set super-user mode



Info Leakage	3
SMS Activities	7
Monitor Activities	2
File Operations	1
Network Activities	0
Embedded Commands	3

University of Verona
Department of Computer Science
Strada Le Grazie, 15
I-37134 Verona
Italy

http://www.di.univr.it