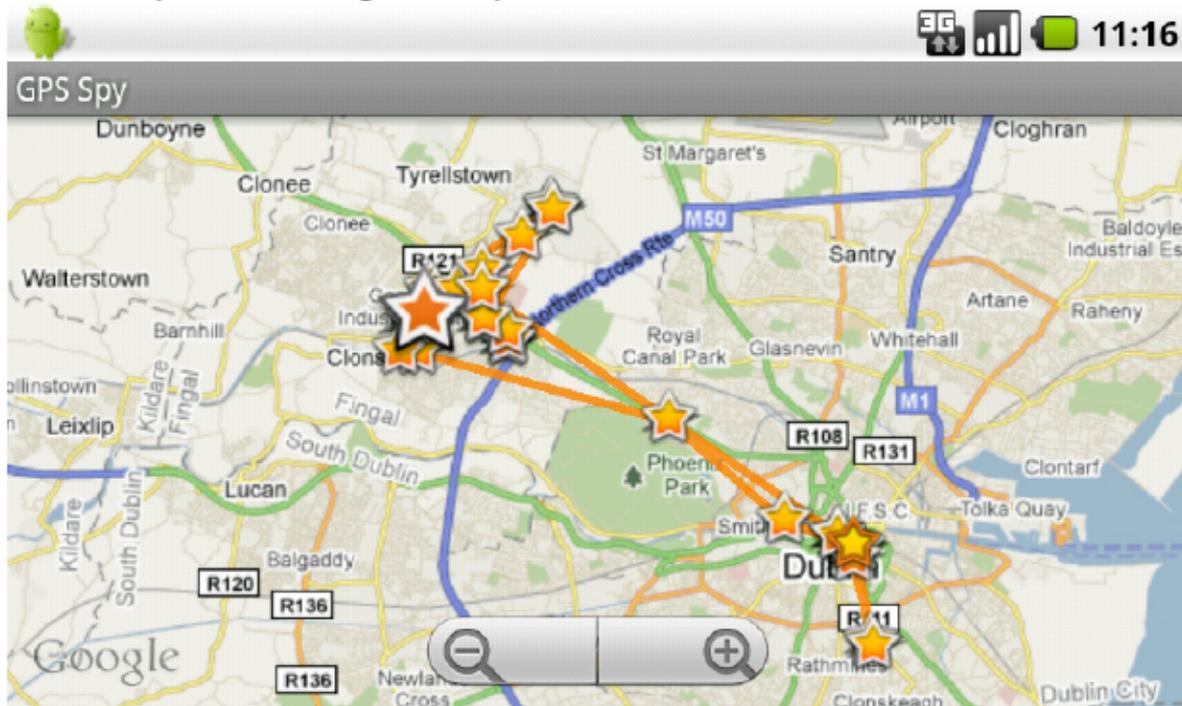


# Malicious Android Apps

Android.Tapsnake tracking the compromised device



*The Motivation is Money; the Opportunity is There, Why Aren't There More?*

Cybercriminals have wormed their way into everything from personal PCs to the financial system, so what's to stop them from taking hold of our smartphones and using them for nefarious ends? According to a recent [Symantec study](#), the answer lies in profitability.

For the last 10 years, the security industry has predicted a flood of mobile malware (specifically in the form of apps for Android) to hit the marketplace and begin wreaking havoc on consumers. Only a trickle ever appears-- why is this? Well, respect them or hate them, the majority of attackers are at their very core, businessmen. They either develop or purchase readymade malware with the goal of making money, and so far only a fraction of the available schemes generate enough revenue to make the risk worth the reward.

According to the recent Symantec study, there are three factors needed for malware attacks to flourish:

- An open platform
- A platform that is far-reaching and widely used
- Attacker motivation (usually monetary)

## The Perfect Petri Dish

The Android is an open platform and the most prolific smartphone operating system. It secured 43% of the worldwide market as of 2Q11, which gives cybercriminals ample opportunity for

corruption once they find a profitable scheme. Here is a list of the current seven most popular threats to mobile security, how they work and the likelihood they'll stick around.

### 1) Premium Rate Number Billing

In this instance, attackers register and activate a premium rate number (i.e., a phone number that charges an exorbitant amount to call or text it), and then they hardwire your phone to repeatedly text the number without your permission.

Typically, these premium rate numbers are registered in the form of short codes, which appear shorter than normal phone numbers (e.g. 123-4). Each country and carrier regulates them differently, and the revenue split between the attacker, the carrier and the SMS aggregator can vary. What doesn't vary? Every time your phone sends a text message to the short code, your phone bill goes up, and the thief gets a percentage of that.

So how do criminals rig your phone to send the text messages? You give them permission. When you install Android applications, they can request permissions to send SMS messages, and these messages can be sent without user confirmation. So if you download android Android malware with this capability, it will send continual text messages to the short code in the background and unless you check your outbox with vigilance, you won't know about it until you get your phone bill.

One thing that prevents this scheme from becoming a larger problem is the fact that short codes are country and carrier specific. This means an attacker must register multiple numbers across various countries unless he or she only wants to target one region, which can be cost-prohibitive.

### 2) Spyware

Currently, multiple Android applications exist that allow someone to track and monitor smartphone users. They may record and export all SMS messages, emails, call logs, GPS locations, or they can turn on the mobile phone's microphone and record phone conversations. This scheme doesn't generate money directly for the attacker, but it can give them valuable information that can be used to access financial accounts or to steal identities.

In order for this malware to work, the attacker must purchase the Android application from a vendor (or develop one him or herself), and then gain access to the phone, usually by "rooting" it (i.e., removing the default security system).

Even without rooting the smartphone, thieves can obtain data by requesting standard permissions. One example is Android.Tapsnake, which masks itself as the popular snake game, and functions as such, but in the background, it's uploading the GPS coordinates of the device every 15 minutes.

### 3) Search Engine Poisoning

Search engines recommend sites or fluctuate rankings for sites based on their perceived relevance and users' visit rates, and when they're used on a mobile phone, the

recommendations and rankings are further customized.

Malware developers take advantage of this system by initiating multiple requests for their sites from a compromised smartphone. This poisons the hit rates monitored by search engines and artificially raises their search rank, allowing them to steer more prospective customers their way. They can also generate more revenue through pay-per-view or pay-per-click advertising.

Search engine poisoning also increases the percentage of the site owners' revenue sharing. Since search-related revenue sharing is paid on a sliding scale, (i.e., the more web traffic they generate, the higher the percentage of the revenue they get), it pays for them to send repeated hits to their site.

An additional way attackers raise revenue with this scheme is by offering a second search box on their specific site. If legitimate visitors use this box, owners of the site receive additional money from the search engine.

#### 4) Pay-per-Click

A variety of services, such as advertising networks, pay an affiliate each time they refer someone to their site. By using malicious Android applications, an attacker can generate artificial visits to these websites and receive a few cents per click. This scheme is not as lucrative as the payouts are relatively small and require high volumes to generate reasonable returns, but there are other options available to make money.

Many carriers provide value-added services such as ringtones, news releases, and mobile TV, and attackers can rig your phone to download their content surreptitiously without your permission, adding large amounts to your phone bill.

#### 5) Pay-per-Install

Pay-per-install means different things in the mobile phone and PC worlds. In the mobile marketplace, this refers to the legitimate distribution centers that host applications for download. They charge users to download the products and they charge vendors based on the number of downloads and installs.

In the PC space, this works in reverse as a distributor pays an affiliate every time they are able to install an application on a user's computer. This makes pay-per-install for PCs more attractive to attackers because they can force a compromised computer to download an app without the user knowing, and collect handsomely on the backend.

#### 6) Adware

Many advertising networks pay websites and other content providers like mobile phone applications, each time their ads display. Generally, the networks pay per view or click, so attackers will repackage or clone popular games sold in the Android marketplace, and then register the advertising library to themselves instead of the original content providers. Every time their application is used and the advertisement is viewed, the attacker generates revenue. The illegitimate application works as it was originally designed, so the user has no idea this is

going on.

## 7) mTAN Stealing

For the uninitiated, a “TAN” is a “transaction authorization number” used when logging into online banking or completing an online financial transaction. It’s one of the many security measures financial institutions have implemented in order to prevent “man-in-the-middle” attacks on their customers, and can be very effective.

The problem arises when an Android customer has spyware on their phone that tracks their keystrokes or reads their text messages and emails. Thieves can use the data they export to steal these numbers and authorize transactions without users’ knowledge.

### **It’s All About the Money**

It may seem like mobile malware is a huge problem, but relative to the continual attacks launched against PCs, it remains an undeveloped landscape. Most of the schemes represented above have a low revenue-per-infection ratio, so for consumers to see a rise in mobile malware incidents, infection rates must increase. And they could. As technology advances, more devices come on the market and the public increasingly embraces technology, more opportunities will present themselves and it is up users to protect themselves.

Mobilesecurity