

**Android Malware**  
**Spyware in the Android  
Market**



**Troy Vennon, GTC Research Engineer**  
**Mayank Aggarwal, GTC Research Engineer**  
**March 12, 2010**

**TABLE OF CONTENTS**

ABSTRACT .....	3
SPYWARE DEFINITION .....	3
SPYWARE IN THE MARKET .....	3
GIRLFRIEND TEXT MESSAGE VIEWER .....	3
VARIANTS .....	6
SMS MESSAGE SPY PRO/LITE .....	7
THEFT AWARE .....	13
SUMMARY .....	26

## ABSTRACT

When the concept of the Android Market became public, security researchers and industry experts immediately began discussing the implications of allowing developers to publish unscreened applications to the Android community. That discussion continues to this day and SMOBILE has highlighted both the pros and cons of this type of approach in several documents, articles and discussions, while providing examples of the types of malware that Android users could expect to see in the future. As will be detailed in this document, the future is here.

In previous whitepapers and postings, SMOBILE has detailed several samples of spyware that have been developed for Android devices and has analyzed an attempt by Android developer 'Droid09' to make available a phishing application that targeted the online banking customers of several high profile financial institutions. The focus of this whitepaper highlights the existence and technical capabilities of spyware applications and applications currently available on the Android Market which clandestinely contain spying components and capabilities.

## SPYWARE DEFINITION

Information security engineers have spent years labeling and categorizing malicious applications. It is important to note that malware is categorized based upon what it actually does once it has infected a system. SMOBILE and other Information Security professionals alike currently categorize and label malware as Viruses, Trojans, Worms and Spyware.

The spyware category offers challenges when considering applications exist that are specifically designed to allow individuals of authority, such as parents or employers, to monitor certain types of use and activity. A clear differentiator between malicious spyware and authorized monitoring applications involve whether or not the device owner is aware of the monitoring and if the person receiving information has a legal right to monitor the device.

In detection and removal of spyware from infected devices, SMOBILE relies on pre-defined criteria when first categorizing a threat as spyware. If the application allows a 3<sup>rd</sup> party to spy on the activities of the user and the application actively hides itself from the 3<sup>rd</sup> party, it is categorized as spyware. Further criteria include whether a user can view the name of the application, the application's icon in the device Applications list and if the user can determine the application's function while it is monitoring certain activities.

## SPYWARE IN THE MARKET

### GIRLFRIEND TEXT MESSAGE VIEWER

**Girlfriend Text Message Viewer** was one of the first applications discovered by the SMOBILE Global Threat Center Team. Using a series of keyword searches, **Girlfriend Text Message Viewer** was revealed, along with what appears to be several variants of this spyware application from the same developer. A discussion of the application and its variants follows.

**Girlfriend Text Message Viewer** is accompanied in the Android Market by the following description:

“Spy on peoples text messages. Install this app on their phone and then configure your mobile number. It will forward a copy of all received messages to you. Once configured it acts and looks like a normal web browser so the user does not get suspicious. This app actually works! “

**Girlfriend Text Message Viewer** was developed for Android devices by developer [Lee Cook](#). The package that is installed on the device is named **com.cook.android.cheatactivity**. This application is copy protected and requests the following permissions:

- **android.permission.RECEIVE\_SMS**
- **android.permission.SEND\_SMS**
- **android.permission.INTERNET**

Installation of **Girlfriend Text Message Viewer** on the target’s device will require physical access to the handset by the attacker. Once **Girlfriend Text Message Viewer** is installed, the attacker will only need to configure the monitoring device’s phone number. From that point forward, all incoming and outgoing SMS messages will be forwarded to the attacker’s monitoring device. The victim user will notice a new application icon is available in the applications list. This application is labeled “Browser” and functions as a working web browser application, once **Girlfriend Text Message Viewer** is properly configured.

Below you will find screen captures of the installation and configuration process required for **Girlfriend Text Message Viewer**, as well as an example of the “Browser” application hiding the true intent of the application:

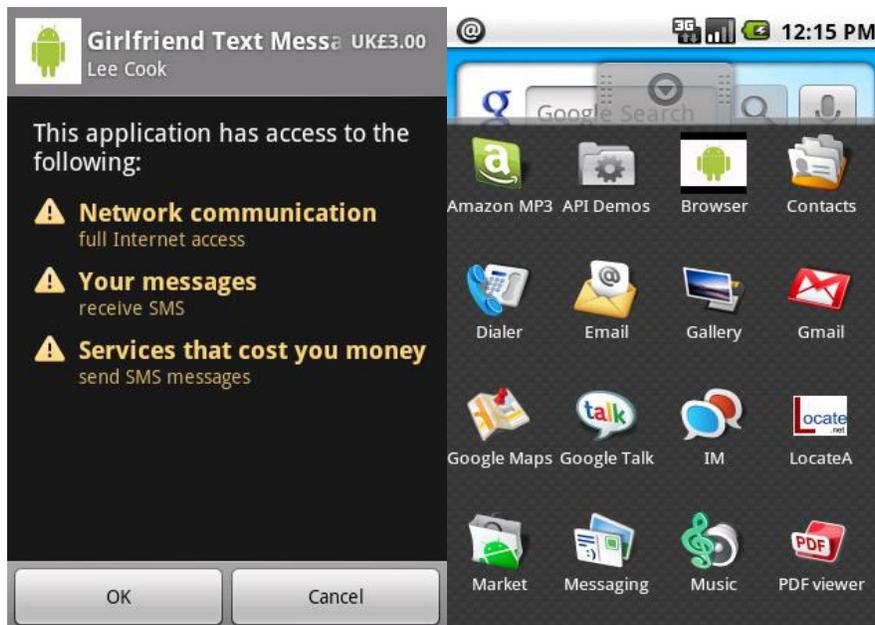


Fig. 1

Fig. 2

In **Fig. 1**, the **Girlfriend Text Message Viewer** application begins the installation process by declaring the permissions the application will need in order to function. In **Fig. 2**, the new “Browser” icon is available in the applications list.



Fig. 3

**Fig. 3** represents an enlarged view of the “Browser” icon that executes the **Girlfriend Text Message Viewer** application’s configuration options.

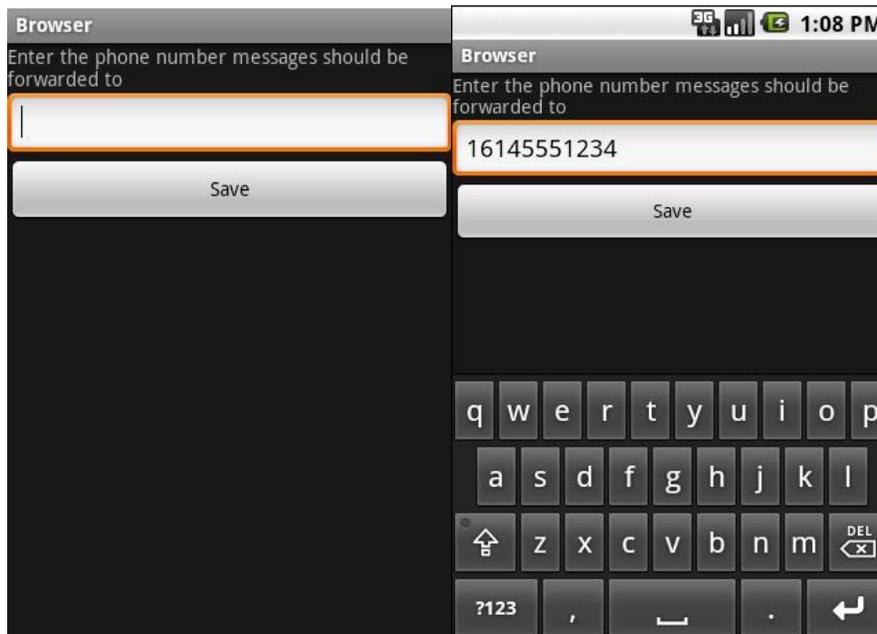


Fig. 4

Fig. 5

**Fig. 4 & 5** show the configuration options available for the **Girlfriend Text Message Viewer** application. The application prompts for the phone number of the device that will be used to monitor the victim’s SMS messages, i.e., the device to which all inbound and outbound text messages from the victim will be forwarded. Once the attacker clicks “Save”, the application immediately reverts to its deceptive browser guise, as seen in **Fig. 6**.

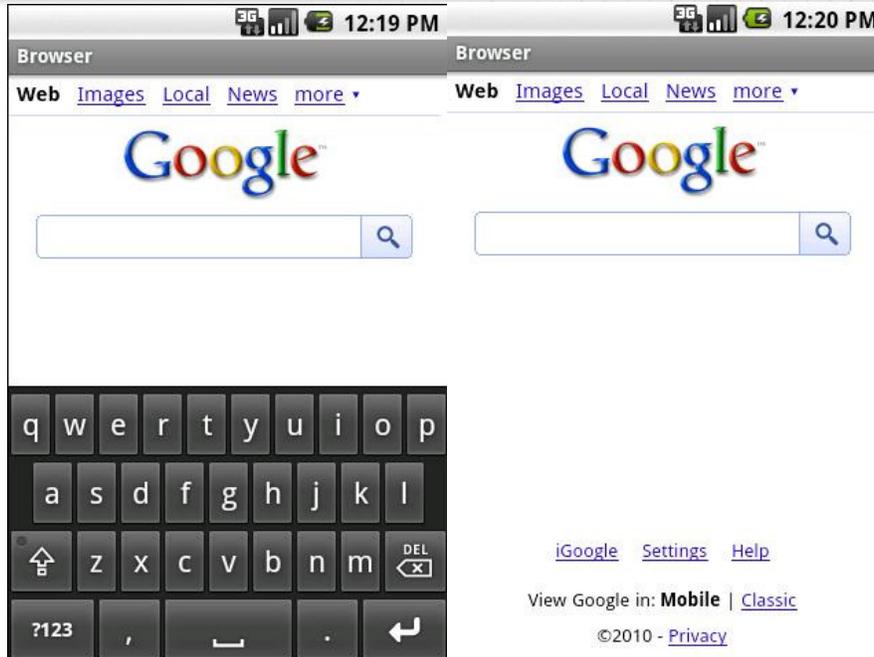


Fig. 6

Fig. 7

By clicking the device’s “back” button, the attacker will be presented with a fully functioning web browser, as shown in **Fig. 7**. From this point on, any attempt by the victim user to execute the “Browser” application will result in a fully functional web browser, while the **Girlfriend Text Message Viewer** application silently forwards the victim’s personal SMS communications to the attacker.

**Variants**

When search results showed the existence of the **Girlfriend Text Message Viewer** in the Market, several variants of the spyware application from the same developer were noted. In one exception, the variant was released to the Market by a developer of a different name. However, the spyware application appears and operates in the exact same fashion. In the Android Market, there are several different names for these variants, but all variants provide the exact same functionality and use the same technique to hide the spyware’s true operation from the intended victim. Below are the details that indicate the subtle differences of these variants:

Table 1

Variant Name	Package Name	Developer	Permissions Requested
SMS Spy	com.cook.android.helloactivity	Lee Cook	Android.permission.Receive_SMS Android.permission.Send_SMS Android.permissions.INTERNET
Child Monitor	com.cook.android.monitoractivity	Lee Cook	Android.permission.Receive_SMS Android.permission.Send_SMS Android.permissions.INTERNET
Cheating Partner Detector	com.cook.android.cheatactivity	Lee Cook	Android.permission.Receive_SMS Android.permission.Send_SMS Android.permissions.INTERNET

<b>Secret Text Message Viewer</b>	com.gray.android.cheatactivity	Adroidapps2010	Android.permission.Receive_SMS Android.permission.Send_SMS Android.permissions.INTERNET
-----------------------------------	--------------------------------	----------------	---

### SMS MESSAGE SPY PRO/LITE

**SMS Message Spy Pro** and **SMS Message Spy Lite** are similar spyware applications from the same developer. **SMS Message Spy Pro/Lite** were both developed by [Carrot App](#). The Pro version of this spyware application is the full, paid version. The Lite version is currently listed in the Market as free, but it expires in seven days. **SMS Message Spy Lite** can be considered a trial version of the Pro variant.

**SMS Message Spy Pro** runs on the device under the package name **com.carrotapp.smsspypro** and contains the following description in the Market:

“A real spy tool! Automatically sending all SMS messages to an email in the background hourly. It pretends to be a Tip Calculator. No one can see the difference.

To use: Go Menu->About, LONG PRESS on the logo, password is spy.

Please try our free version first. Search SMS Spy.

Its illegal to spy on phones you don't own!”

**SMS Message Spy Lite** runs on the device under the package name **com.carrotapp.smsspyfree** and contains the following description in the Market:

“Need a real spy tool? Automatically forwarding all SMS messages to an email in the background hourly.It pretends to be a Tip Calculator. No one can see the difference.

To use:Go Menu->About, LONG PRESS on the logo, password is spy.

Please buy the full version if you like it.

Its illegal to spy on phones you don't own“

Both applications request the following permissions upon installation:

- **android.permission.RECEIVE\_BOOT\_COMPLETED**
- **android.permission.INTERNET**
- **android.permission.DEVICE\_POWER**
- **android.permission.READ\_SMS**
- **android.permission.RECEIVE\_SMS**
- **android.permission.READ\_CONTACTS**
- **android.permission.WAKE\_LOCK**

Installation of **SMS Message Spy** requires that the attacker gain physical access to the victim's handset. Once **SMS Message Spy** is installed on the device, the attacker then must specify a valid email address to which the intercepted inbound and outbound SMS messages will be sent. **SMS Message Spy** will send hourly email messages with the inbound and outbound SMS messages from

the monitored device. Messages that already reside on the device at the time that the application is installed will not be forwarded in the first hour's email update.

In order to hide itself from the intended victim, **SMS Message Spy** masquerades as a fully functional tip calculator that the user can use to determine appropriate tip amounts when dining. Screen captures of the **SMS Message Spy** installation and configuration processes, as well as its appearance after activation, are shown next: note the rather vague and unobtrusive application icon and name ("SP"). Also included are screen captures showing the normal operation of the application after it has been activated and the true intent has been hidden.

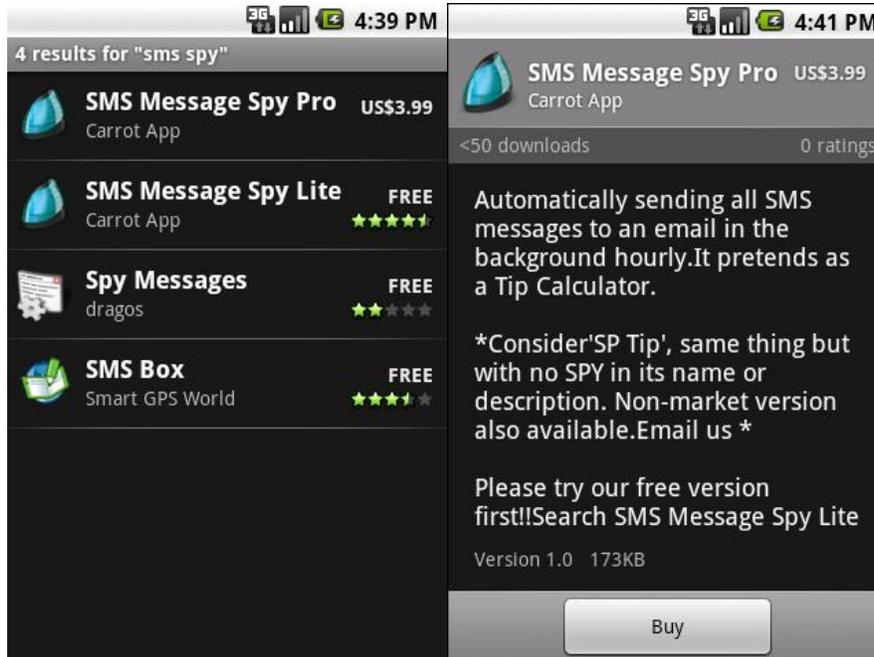


Fig. 8

Fig. 9

**Fig's 8 & 9** illustrate the **SMS Message Spy Pro & Lite listings** in the Android Market and the purchasing process. Once the application has been selected (and purchased if selecting Pro), **Fig. 10** illustrates the installation process declaring the permissions the application is requesting.



Fig. 10

Fig. 11

Fig. 11 illustrates the new addition of “SP” to the Applications folder.



Fig. 12

Fig. 12 illustrates an enlarged view of the “SP” icon that represents **SMS Message Spy**. The attacker selects the “SP” icon to execute the program for the first time, and is then presented with an alert as shown in Fig. 13.



Fig. 13

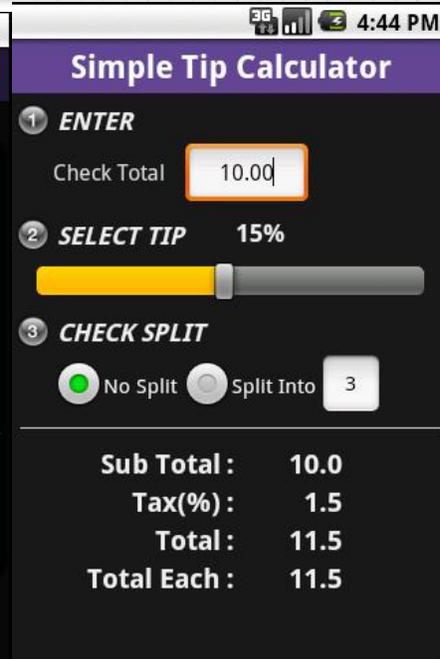


Fig. 14

The application then informs the attacker of the process required to enter the spy settings for the application. Again, this information is displayed only the first time the application runs. Once the attacker clicks “OK”, they are taken to the masquerading “Simple Tip Calculator” (Fig. 14). Subsequent executions of the “SP” application take the user, who is then generally the victim, not the attacker, directly to the fully functional “Simple Tip Calculator”.

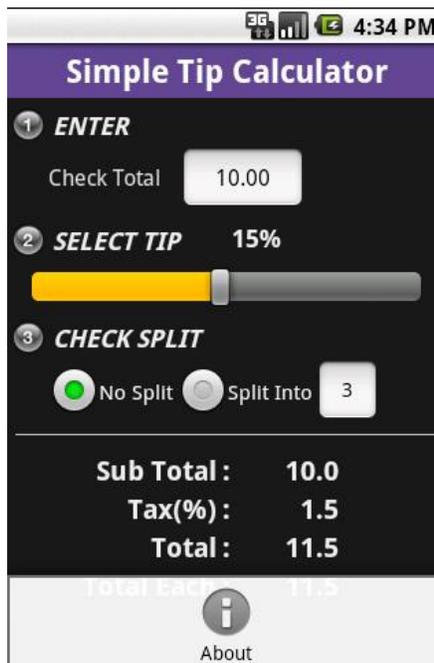


Fig. 15

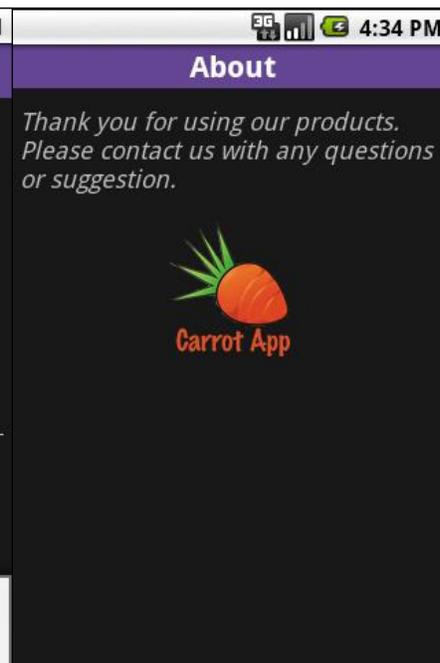
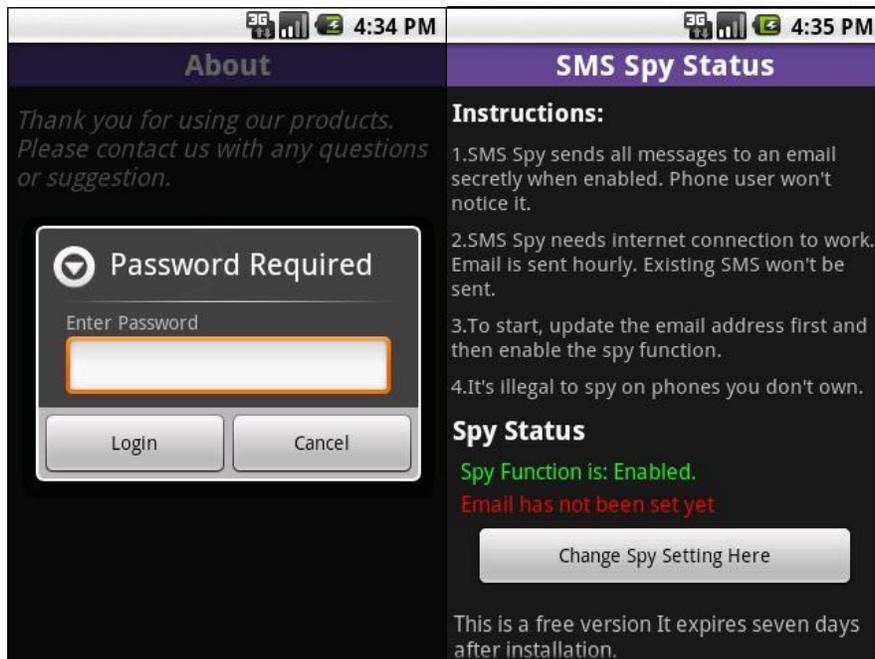


Fig. 16

As noted in **Fig. 13**, the attacker reaches the spy settings configuration display by selecting the “About” option from the application menu, then pressing the carrot icon until the “Password Required” dialogue window appears...



**Fig. 17**

**Fig. 18**

**Fig. 17** illustrates the “Password Required” dialogue window. Here, the attacker enters the password “spy” to gain access to the SMS Spy Status screen (**Fig. 18**), which shows if the application is enabled and whether or not the monitoring email address has been set.

In the instance represented in **Fig. 18**, the email address has not been set. To do so, the attacker clicks on “Change Spy Setting Here” and is taken to the screen represented in **Fig. 19**.

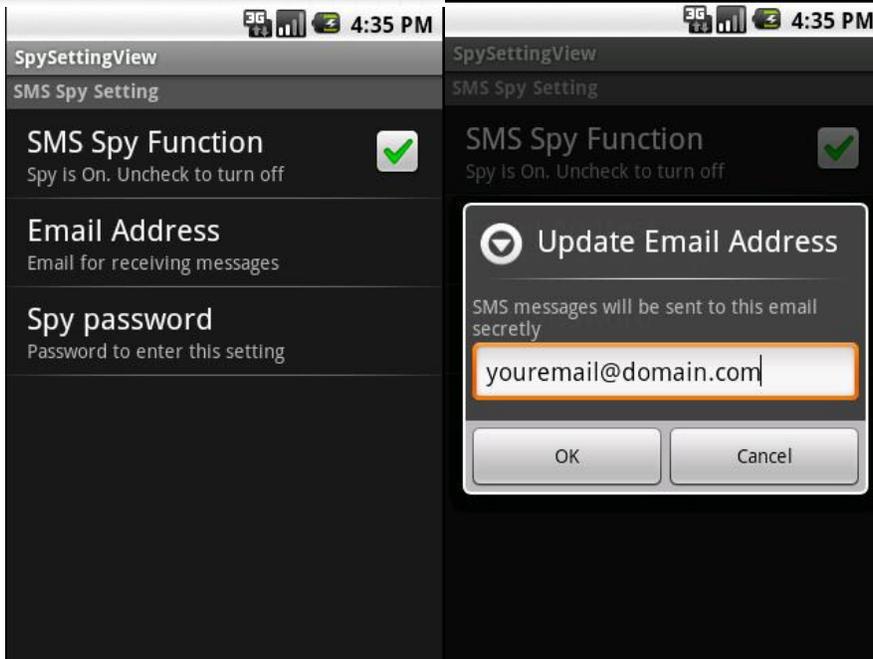


Fig. 19

Fig. 20

As shown in Fig. 19, the “SMS Spy Setting” screen allows the attacker to enable/disable the monitoring capability, configure the monitoring email address or modify the password that grants access to the “SMS Spy Status”. When the attacker clicks on the “Email Address” option, the “Update Email Address” dialogue window appears, allowing specification of the email address to which all monitoring information will be sent (Fig. 20.)



Fig. 21

**Fig. 21** illustrates the “Spy Password” dialogue window, where the attacker can modify the password that grants access to the configurations screens of the spyware application.

**SMS Message Spy Pro & Lite** both operate in identical fashion. The fundamental difference between the two applications is that the Lite version is a trial version that functions for just seven days.

## THEFT AWARE

**Theft Aware** is an application that is marketed and sold in the Android Market as a tool that can be used to assist a user in protecting their personal data in the event that their device is lost or stolen. **Theft Aware** comes in two versions; one is the full, paid version and the other is a trial version.

**Theft Aware** is described in the Android Market as follows:

“Control and find your phone in the event of loss or theft. Pure, international SMS control! No subscription fees! REAL INVISIBILITY (no SMS triggers, no icons, obfuscated app entries) and very useful SMS commands (GPS locate, wipe, lock, customizable siren, backup data, map services links, launch own programs remotely).”

The full, paid version of **Theft Aware** arrives on the device packaged as **at.itagents.ta\_setup\_mf.apk**. The trial version of **Theft Aware** is labeled **at.itagents.ta\_setup.apk**. Both package versions are copy protected when installed from the Android Market.

Under normal circumstances, an application such as this would not prompt SMOBILE to label it as spyware, since it is marketed and useful as a tool for recovery of a device. However, since the application makes an effort to hide itself from the user, SMOBILE is obligated to label it as “suspicious”. Under certain circumstances, **Theft Aware** could potentially be used as an application to monitor the locations and certain communications of an unsuspecting user.

**SMobile’s anti-malware/anti-spyware application notifies the potentially unsuspecting user that the “suspicious” Theft Aware application is present on their device.** If the user installed the application for use in accordance with its designed intent, SMOBILE’s application allows the user to acknowledge the notification and create an exclusion from future detections.

**Theft Aware** was developed by [ITAgents Interactive Software Solutions](http://ITAgentsInteractiveSoftwareSolutions.com) and offers the following features, for tracking a lost or stolen phone and/or monitoring the activities of an unsuspecting user:

- Register up to two phone numbers for notifications to be received
- If the device’s SIM is changed, **Theft Aware** will send the new SIM’s phone number to the notification numbers that are registered
- The application runs invisibly, with no visible icon for the thief or user to identify
- Can send SMS commands remotely to receive the following information about the device:
  - Current GPS location
  - Receive links to online map services
  - Remote lock the device
  - Activate a loud siren that is customizable
  - Remotely delete personal data such as call logs, SMS messages, contacts, etc...

- Backup contacts and/or SMS messages to another device
- Direct the monitored phone to call you and listen to the ambient room noise
- Implement your own SMS commands

**Theft Aware** requests the following permissions upon install:

- **android.permission.READ\_PHONE\_STATE**
- **android.permission.RECEIVE\_BOOT\_COMPLETED**
- **android.permission.ACCESS\_COARSE\_LOCATION**
- **android.permission.ACCESS\_FINE\_LOCATION**
- **android.permission.ACCESS\_NETWORK\_STATE**
- **android.permission.CALL\_PHONE**
- **android.permission.GET\_TASKS**
- **android.permission.PROCESS\_OUTGOING\_CALLS**
- **android.permission.READ\_CONTACTS**
- **android.permission.READ\_SMS**
- **android.permission.RECEIVE\_SMS**
- **android.permission.RESTART\_PACKAGES**
- **android.permission.SEND\_SMS**
- **android.permission.WRITE\_SMS**
- **android.permission.WRITE\_CONTACTS**
- **android.permission.SET\_PREFERRED\_APPLICATIONS**
- **android.permission.SYSTEM\_ALERT\_WINDOW**
- **android.permission.INTERNET**
- **android.permission.WRITE\_APN\_SETTINGS**
- **android.permission.WRITE\_CALENDAR**
- **com.android.browser.permission.WRITE\_HISTORY\_BOOKMARKS**
- **com.android.browser.permission.READ\_HISTORY\_BOOKMARKS**

The following screen captures illustrate the installation and configuration process for the **Theft Aware** application:

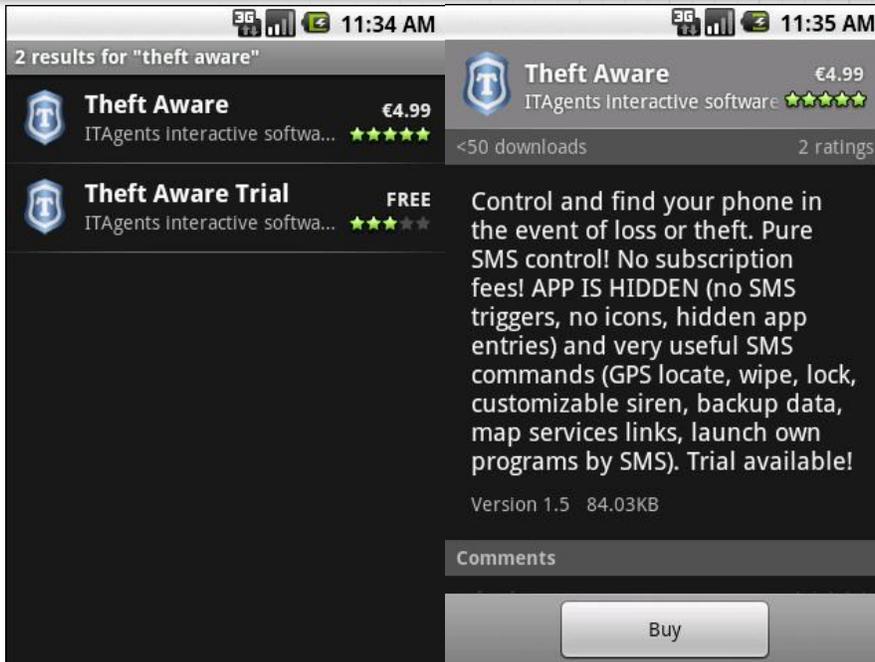


Fig. 22

Fig. 23

Fig. 22 & 23 represents the Theft Aware applications' (trial and paid) listings in the Android Market and the initial steps in the purchasing process for the paid version.



Fig. 24

Fig. 25

Fig. 24 shows the permissions that will need to be allowed in order for the setup to proceed. What isn't realized until later in the installation process is that the download represented in Fig's 24 &

25 is simply an installer package that will download a setup application! This installer package merely needs Internet access in order to be able to download the Theft Aware application that will actually be installed.

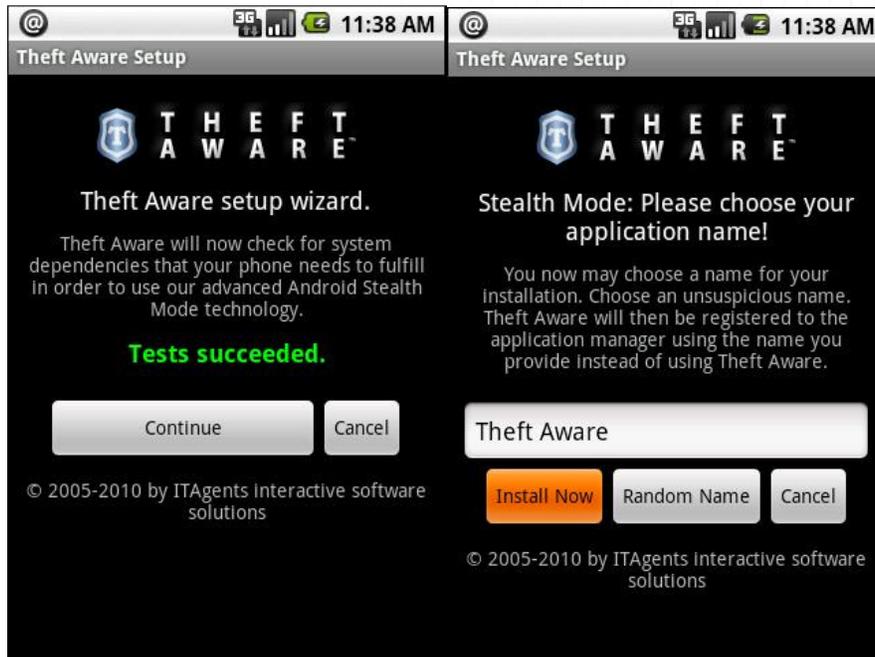


Fig. 26

Fig. 27

Once the installer application is downloaded and installed on the device (**Fig. 26**), the installer application performs a series of quick tests to ensure the device has Internet access. Once those tests pass, the attacker clicks “Continue” to proceed with the install.

**Fig. 27** illustrates the process that the **Theft Aware Setup** installer package uses to allow the true nature of the Theft Aware application to be installed and run in stealth mode. Here we see the default setting of “Theft Aware” is set for the name of the actual application that will be installed.

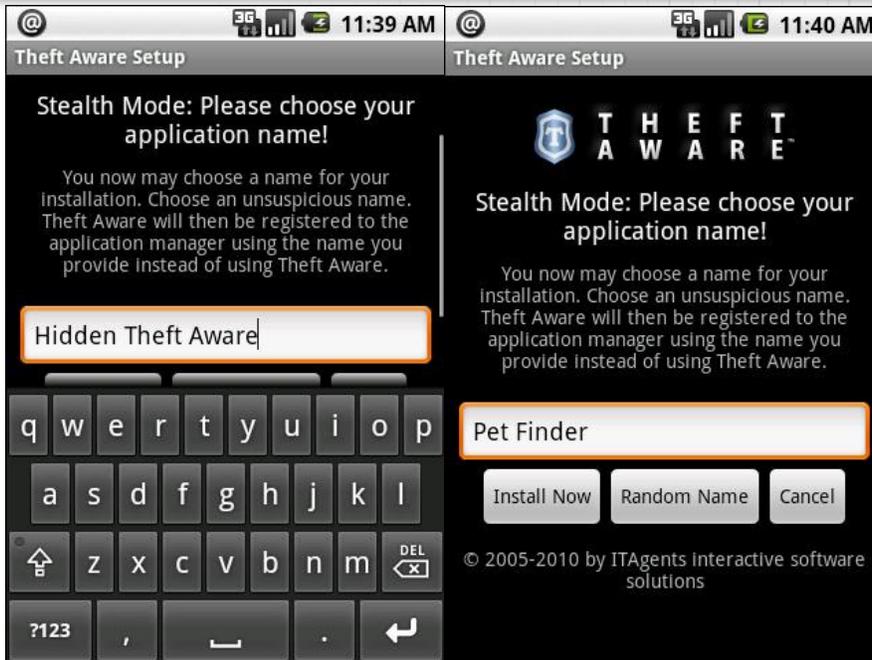


Fig. 28

Fig. 29

In **Fig. 28**, we see that the attacker may modify the name of the application that will be installed to the device, so as to allow it to run in stealth mode. **Fig. 29** shows that if “Random Name” is clicked, the setup package will randomly generate an obscure name for the application. For the remainder of this example, the randomly generated name “Pet Finder” will be used.

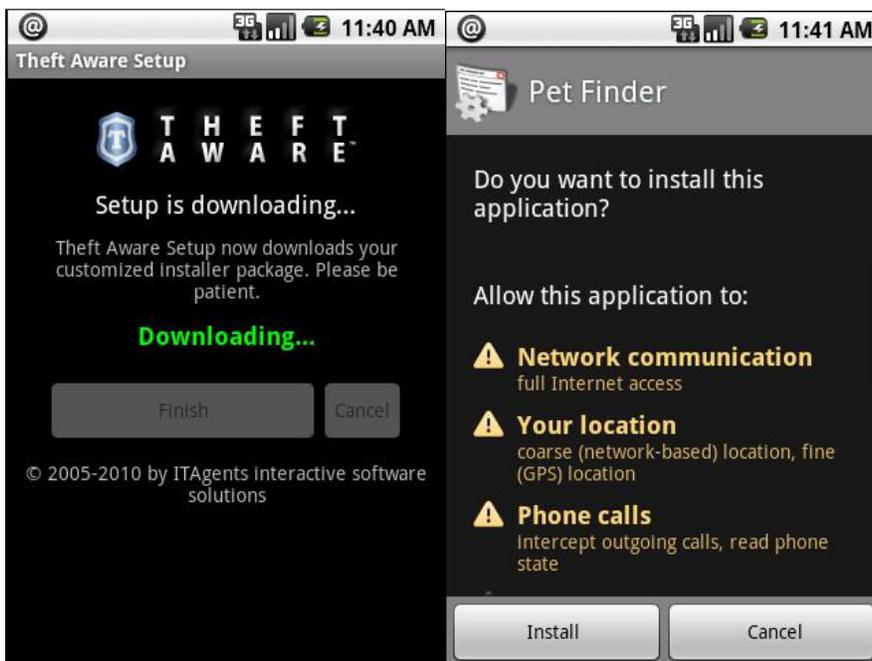


Fig. 30

Fig. 31

The installer package then accesses the Internet to download the package that will act as our “Pet Finder” application – in actuality, the **Theft Aware** application. **Fig. 31** (previous page) represents the permissions that are being declared. Note that the screen capture confirms that that name of the application being installed is “Pet Finder”.

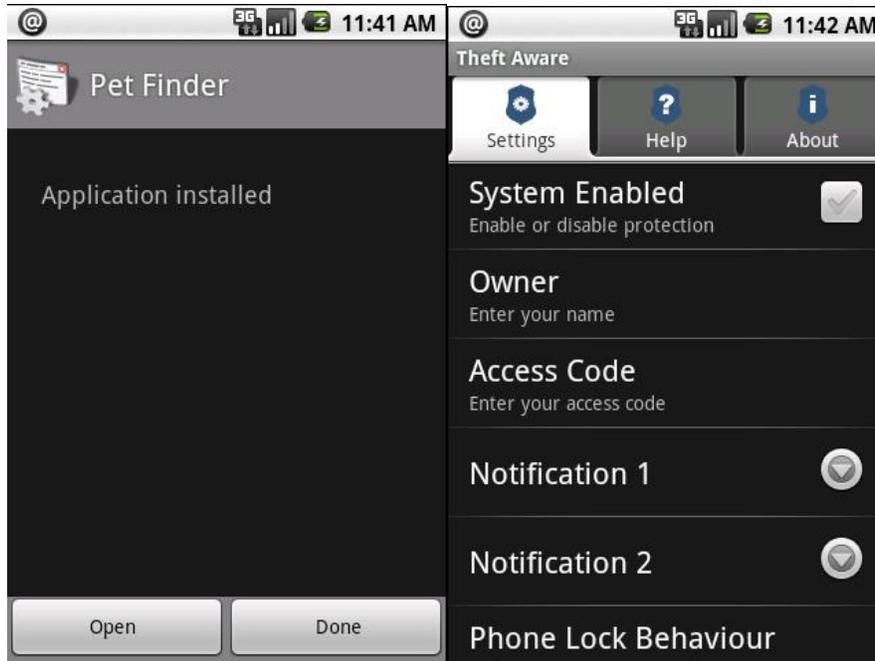


Fig. 32

Fig. 33

Once the application installation completes, the **Theft Aware** setup menu is shown (**Fig. 33**). The system is not enabled by default; configuration of a few settings is required.

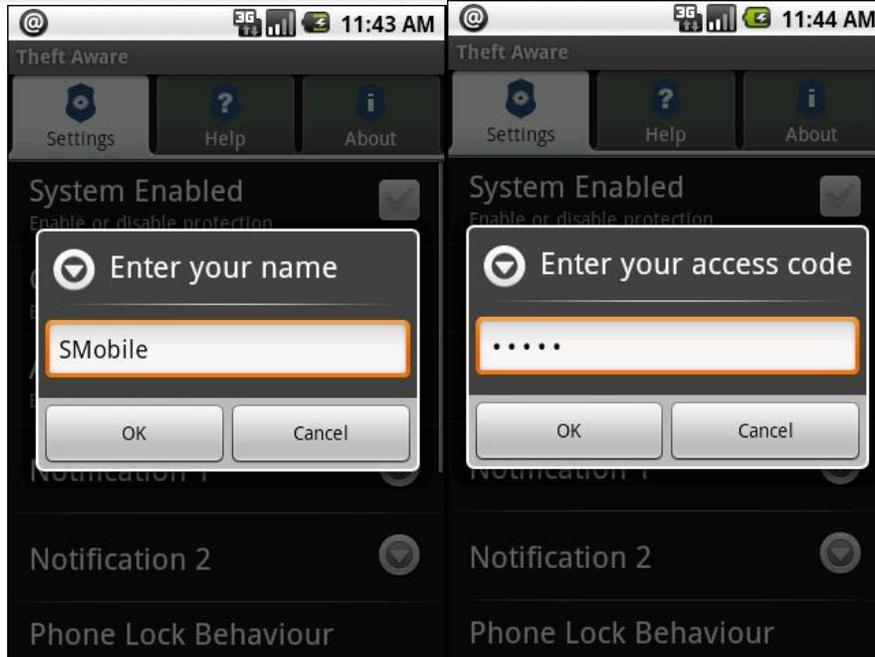


Fig. 34

Fig. 35

**Fig's. 34 & 35** represent the attacker setting the name of the device owner and the access code required to gain access to the configuration menu, once they have been initialized. For this example, we chose "SMobile" as the owner and set the access code as "12345". This access code will come into play later in this analysis.

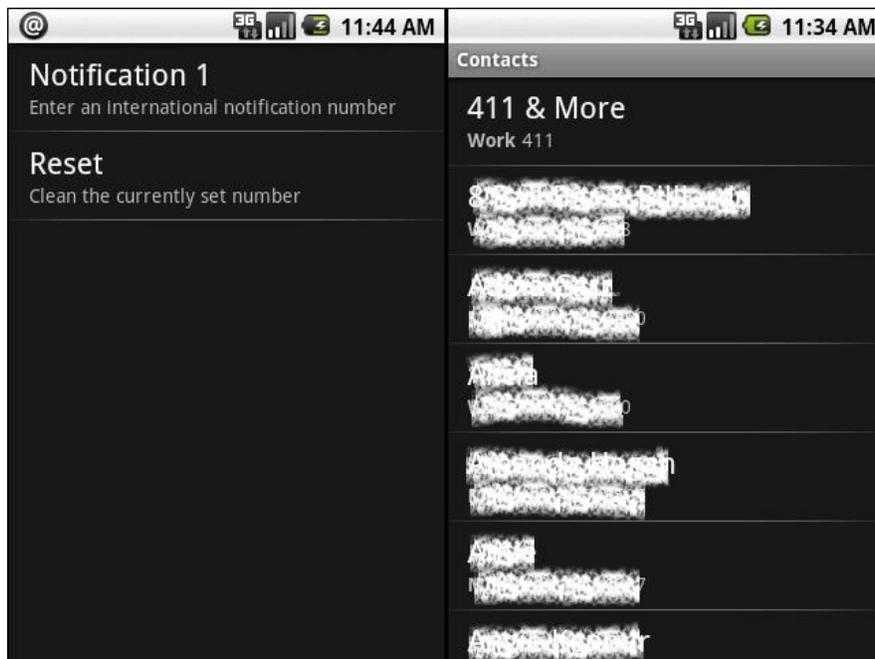
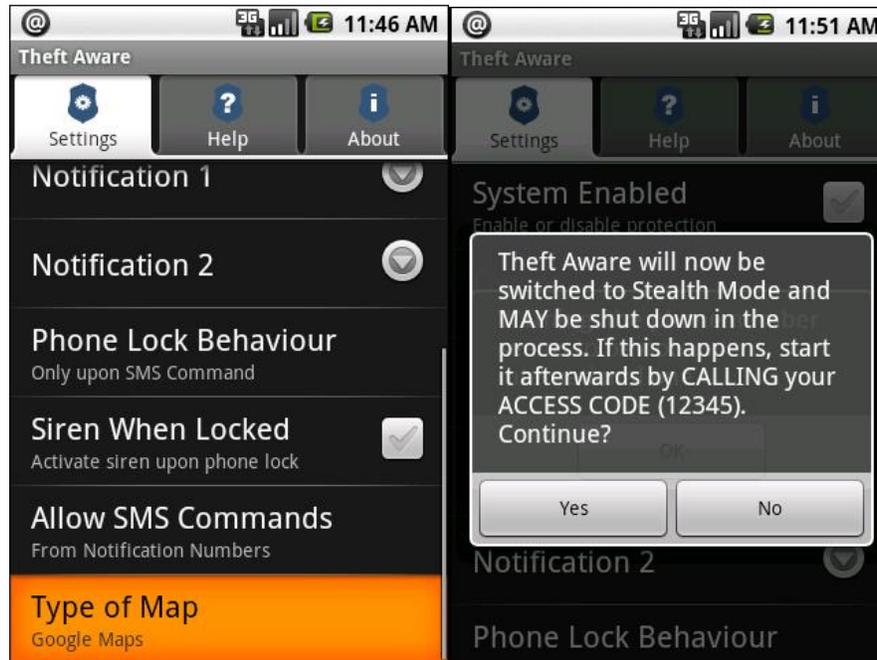


Fig. 36

Fig. 37

The final step in configuration of the application is to set a notification number. As the application's description indicated, this is where the user would choose up to two friends who would receive notifications in the event the device is lost or stolen. The user could then use that friend's device to monitor all of the possible services that **Theft Aware** allows. **Fig. 37** shows that the application forces the user to select a contact from the device's Contacts database.

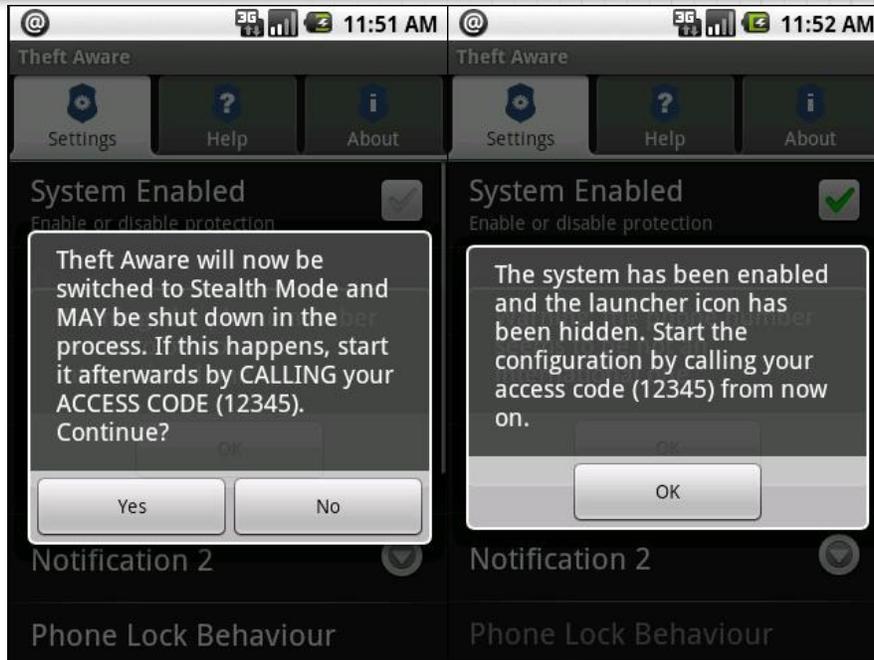


**Fig. 38**

**Fig. 39**

Once at least one notification number has been set, the application can be enabled. **Fig. 38** shows the remaining optional settings that can be configured. **Fig. 39** illustrates the alert that is given, once the user clicks the check mark next to "System Enabled", enabling the application.

As shown in the next screen capture, an alert informs the user/attacker that the application will be placed into "Stealth Mode", and details the process required for subsequent access to the configuration menu, once "Stealth Mode" has been enabled.



**Fig. 40**

**Fig. 41**

When the user/attacker clicks “Yes” to allow the application to enter “Stealth Mode”, **Fig. 41** alerts the user that the system has been enabled and also tells the user/attacker that the launcher icon has been hidden from the applications list. Thus, there is no icon available to the user for launch of the application. This singular activity is the determining factor in SMobile labeling **Theft Aware** as suspicious. It is logical to state that if the application is installed and configured by the device owner, the application would not be considered spyware and functions as intended by the device owner. Conversely, if the application is installed onto the device of an unsuspecting device owner without their knowledge and the application is hidden from detection, the application would be considered spyware. The SMobile Ant-Spyware application will inform the user of the application’s presence and the device owner can act accordingly.

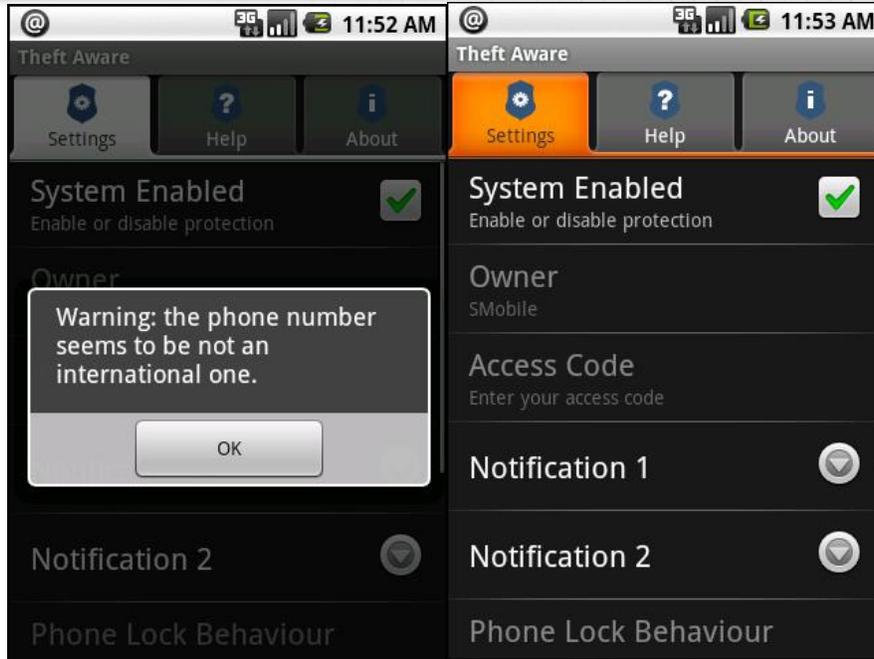


Fig. 42

Fig. 43

(Fig. 42 on the previous page shows an alert displayed to the user/attacker stating that the phone number set for notification is not an international phone number. This warning was able to be ignored. Fig. 43 simply shows the reader that the system has been enabled.)

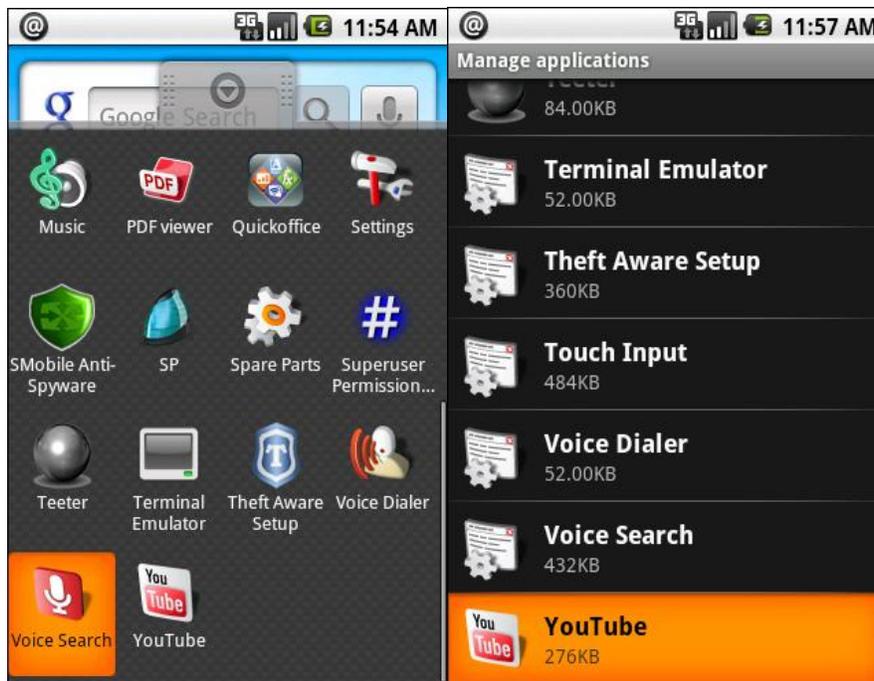


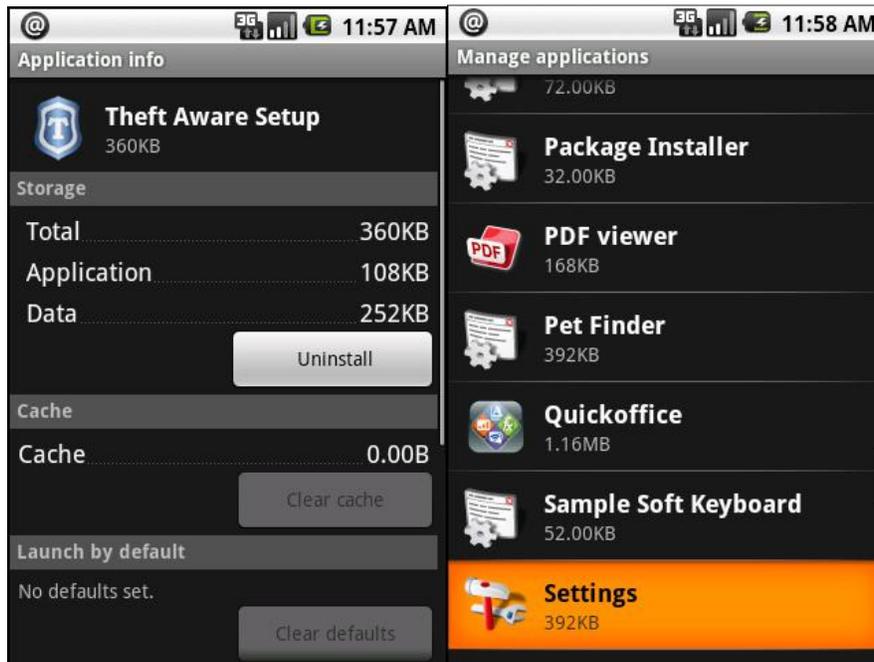
Fig. 44

Fig. 45

As was illustrated in Fig. 41, it is known that there is not a launcher icon for the “Pet Finder” application that **Theft Aware** is currently masquerading as. However, as in Fig. 44, the **Theft**

**Aware Setup** application that was originally downloaded from the Android Market is certainly visible to the user. This application serves absolutely no purpose from this point forward, except as a means to means to inform the user that Theft Aware has already been successfully installed.

Fig. 45 shows the **Theft Aware Setup** application in the applications list. It may be uninstalled, by selecting Settings > Applications > Manage Applications, then selecting Theft Aware Setup > Uninstall.



**Fig. 46**

**Fig. 47**

**Fig. 46 & 47** is a continuation of the uninstall process for **Theft Aware Setup**, through its completion.

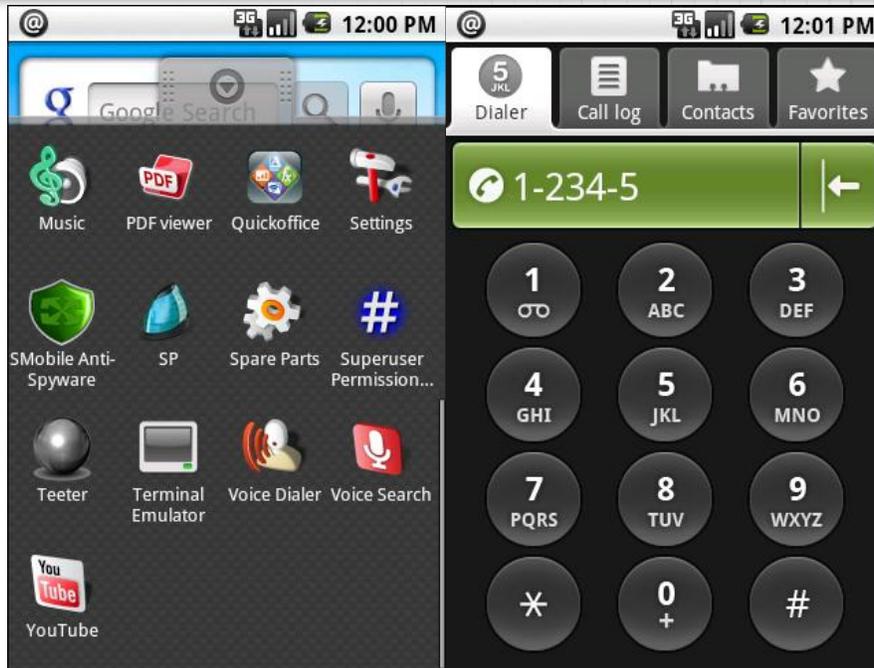


Fig. 48

Fig. 49

**Fig. 48** illustrates that there is no longer an icon for the **Theft Aware Setup** application available to the user. However, by using the device’s dialer, we can dial the access code that was configured during setup to get back to the configuration window. In this case, dialing “12345”. **Fig. 50** shows that Theft Aware still exists on the device and is enabled.

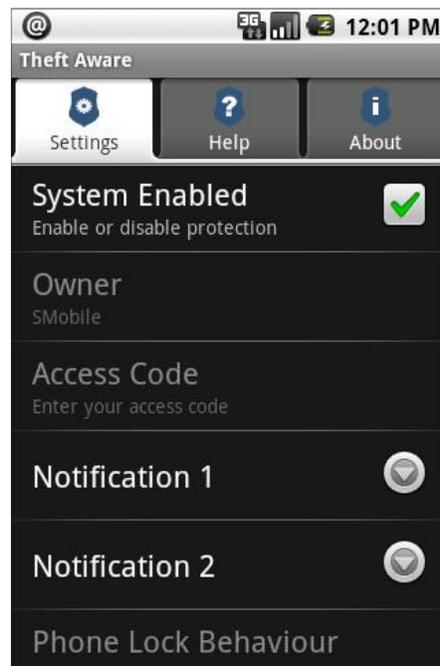


Fig. 50

Theft Aware allows for remote SMS control of the device in order to facilitate the tracking and data protection capabilities for which the application was designed. These remote SMS commands can also allow an attacker or stalker to illegally track an unsuspecting victim. All of the remote SMS commands are required to authenticate to the **Theft Aware** application before the command will be processed. In order to do that, all remote SMS commands must be preceded by the access code that was configured upon installation (For example, "12345"). **Table 2** represents a list of the SMS commands and the outcome that the user/attacker would receive:

**Table 2**

<b>Remote SMS Command</b>	<b>Example</b>	<b>Description</b>
LOCK	12345 LOCK	Locks the device
UNLOCK	12345 UNLOCK	Unlocks the device
SIREN ON	12345 SIREN ON	Turns phone siren on to attract attention to the device
SIREN OFF	12345 SIREN OFF	Turns the phone siren off
UPDATE	12345 UPDATE	Compiles and sends up-to-date information for the missing device
CALL ME	12345 CALL ME	Device will call the sender back, enabling ability to listen to ambient room conversation
WIPE	12345 WIPE	Wipes all data from the device
GET ALL SMS	12345 GET ALL SMS	Will forward ALL SMS messages stored on the device
GET INBOX SMS	12345 GET INBOX SMS	Will forward all SMS messages stored in the device inbox
GET SENT SMS	12345 GET SENT SMS	Will forward all SMS messages stored in the device sent items box
GET ALL SMS FOR xxxxxxxxx	12345 GET ALL SMS FOR 15551234567	Will forward all SMS messages pertaining to a particular phone number

GET INBOX SMS FOR xxxxxx	12345 GET INBOX SMS FOR 15551234567	Will forward all SMS messages in the device inbox pertaining to a particular phone number
GET SENT SMS FOR xxxxxxxx	12345 GET SENT SMS FOR 15551234567	Will forward all SMS messages in the device sent items box pertaining to a particular number
GET CONTACTS	12345 GET CONTACTS	Will forward all phone book contacts to the target device. Contacts will be forwarded one-by-one as individual SMS messages in Business Card or standard text format.

(The full **Theft Aware User Guide** is available [here](#))

## SUMMARY

This study has detailed several samples of spyware and one example of an application that could maliciously be used as spyware, all of which are currently available in the Android Market. These applications have two major traits that enable their use by an attacker for spying on an unsuspecting user: 1) an ability to monitor personal communications to and from the device, and 2) the ability to hide itself from detection by an unsuspecting user.

Applications such as those highlighted in this study have been known to be used to commit fraud, identity theft, illegal monitoring, corporate espionage, and criminal stalking of an unsuspecting user. In several extreme cases, the ability to track a victim's location and communication tendencies has led to violence and the necessity to involve law enforcement in order to handle potentially volatile situations.

These types of applications are becoming readily available and as illustrated, becoming increasingly difficult for the average user to detect when used without their knowledge. Additionally, users are downloading and installing applications while paying little attention to the permissions they are granting. This creates a ripe environment for users to unknowingly install and enable spyware components onto their devices.

It is considered standard operating procedure and best practice to incorporate a well-supported and constantly updated anti-virus/anti-spyware application amongst the basic applications that a Smartphone user installs on their device. In most cases of mobile spyware, the average Smartphone user will not be able to determine whether or not their device is infected without the support of a 3<sup>rd</sup> party application that can scan for known malicious files or behavior.