**[Gain Complete Control of Any Android Phone with the AhMyth RAT](https://null-byte.wonderhowto.com/how-to/gain-complete-control-any-android-phone-with-ahmyth-rat-0180960/)**

* By [**Hoid**](https://creator.wonderhowto.com/hoid/)
* 11/15/2017 7:37 am

There are more than [2 billion Android devices](https://www.macrumors.com/2017/05/17/2-billion-active-android-devices/) active each month, any of which can be hacked with the use of a remote administration tool, more commonly known as a RAT. [AhMyth](https://github.com/AhMyth/AhMyth-Android-RAT), one of these powerful tools, can help outsiders monitor a device's location, see SMS messages, take camera snapshots, and even record with the microphone without the user knowing.

Remote administration tools were first programs intended to provide technical support to remote computers by allowing an administrator to log in and control the device directly. However, hackers quickly saw the potential of these tools and started using them for more nefarious deeds. Today, advanced RATs are used to remotely access and control a wide variety of devices, but today we'll focus on one of the world's most popular — [Android](https://android.gadgethacks.com/).

AhMyth is a new, up-and-coming, open-source Android RAT, currently in the beta stages of development, which uses a simple GUI interface. While Android RATs [aren't a new thing](https://null-byte.wonderhowto.com/how-to/setup-dendroid-android-rat-0167299/), what makes this one stand out from the crowd is the simple and easy-to-understand graphical user interface. Additionally, AhMyth is multi-platform, available on Linux, Windows, and macOS.

**Don't Miss:** [**How to Simulate a RAT on Your Network with ShinoBOT**](https://null-byte.wonderhowto.com/how-to/simulate-rat-your-network-with-shinobot-0179503/)

The RAT consists of two parts. The first is a server-side application based on [Electron framework](https://electron.atom.io/), in our case, just our desktop or laptop, but this could be scaled up to some degree if needed. This acts as a control panel which we use to create and connect to the RAT. The second part is client side, which is the infected Android application we'll use as a backdoor.

Below you can see a quick video demonstration of AhMyth in action, courtesy of the AhMyth team.

**Step 1Download & Install AhMyth**

There are two ways to download and install AhMyth. The first is to directly use the source code from GitHub. The second is to use the binaries they provide.

**Method 1From Source Code**

If you chose to start with the source code, then you'll need to check that you have a few prerequisites installed.

* **Java** — it's used to generate the APK backdoor.
* [**Electron**](https://github.com/electron/electron) — it's used to start the desktop application.
* [**Electron-builder**](https://github.com/electron-userland/electron-builder) **and** [**Electron-packer**](https://github.com/electron-userland/electron-packager) — they are used to build the binaries for macOS, Windows, and Linux.

Once you have those prerequisites, you're ready to proceed. First clone the code from GitHub with the following commands.

git clone <https://github.com/AhMyth/AhMyth-Android-RAT.git>

Then move to the AhMyth-Android-Rat directory with the following.

cd AhMyth-Android-RAT/AhMyth-Server

Once you're in, start AhMyth with the command below.

npm start

This program is still in beta development, and as such, it isn't as robust as it could be. Some users have gotten errors when attempting to start it. If you do, try again running it as root, as seen below.

sudo npm start --unsafe-perm

You'll know it's working when you see the GUI launch.

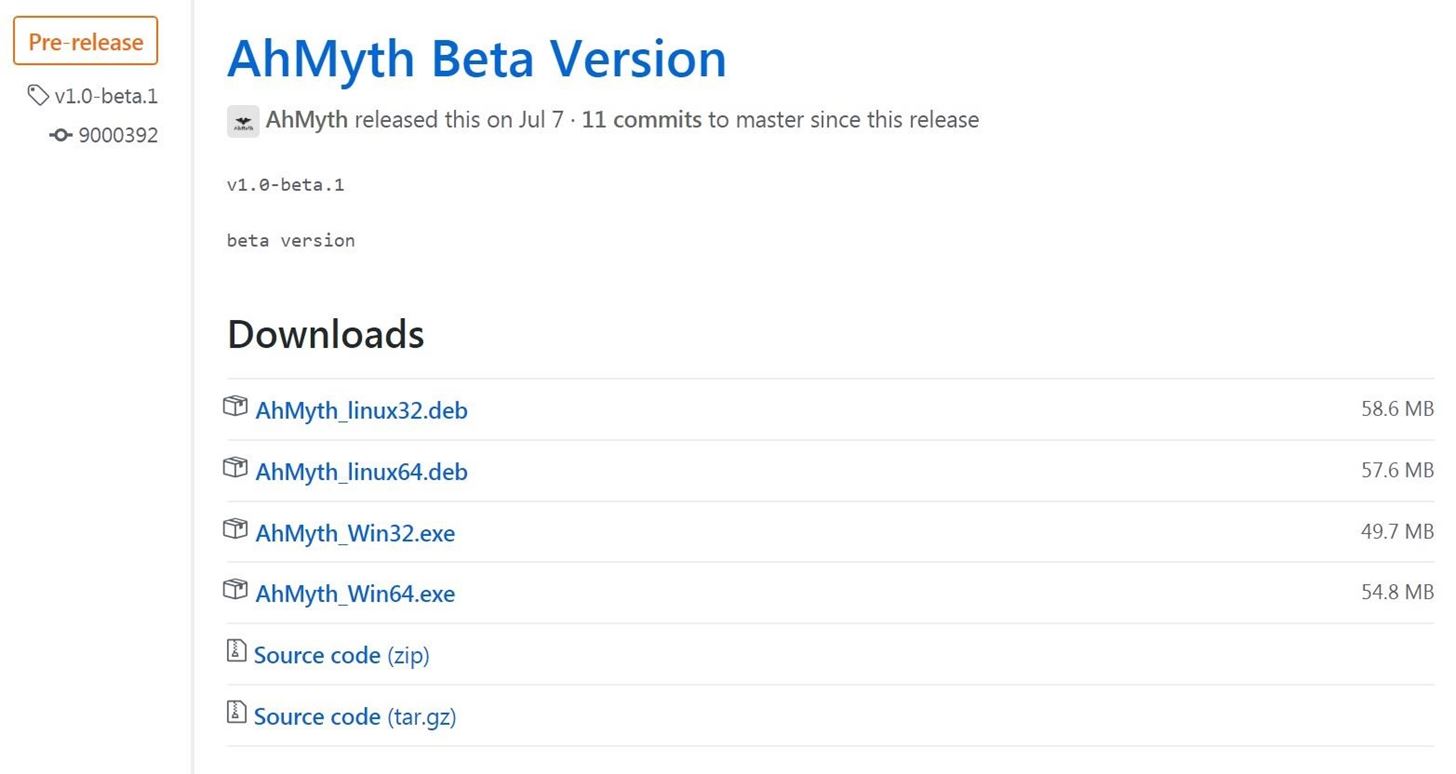
[](https://img.wonderhowto.com/img/original/24/43/63645728052087/0/636457280520872443.jpg)

**Don't Miss:** [**How to Program Your Own Little RAT**](https://null-byte.wonderhowto.com/how-to/program-your-own-little-rat-part-1-getting-server-working-0167490/)

**Method 2From Binaries**

The source code is one way to download it, but if you're lazy like me, there's a slightly easier way — use the binaries! It's particularly nice when you're working on a Windows computer and don't want to mess around with the command line. This shouldn't be a concern as most people will already have it, but do check that Java is updated on your computer.

Navigate to the [AhMyth release page](https://github.com/AhMyth/AhMyth-Android-RAT/releases) and download the release for your system. Currently, they only have Linux and Windows files uploaded.

[](https://img.wonderhowto.com/img/original/13/80/63645727511055/0/636457275110551380.jpg)

Once you download the right file, open it up on your computer, and [it should start installing](https://img.wonderhowto.com/img/original/85/10/63645727961819/0/636457279618198510.jpg). It will automatically open when it completes. After that, we should be ready to go!

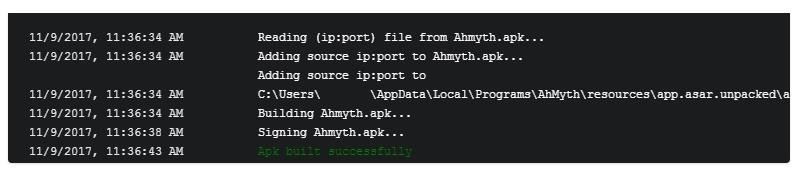
**Step 2Build an APK**

Now that we have the program up and running, it's time to build an Android application with a backdoor. At the top of the screen, select "APK Builder." The first thing to change is "Source IP." This needs to be the IP address of the computer you'll be sending and receiving commands from.

For testing purposes, I'll just be using my local Wi-Fi network. However, if you wanted it to work outside of the local network, you would need to port-forward your computer to the internet and use your public IP address.

AhMyth can build an APK two different ways. It can create a standalone APK or be used to infect another application in order to remain hidden on the target device. To do the latter, select the box beside "Bind With Another Apk" and then browse and select the APK you wish to use. Today I'll just be creating the default standalone APK, but if a malicious user were deploying this in the real, they would very likely be binding it with another APK.

Once you have all the settings selected you're ready to build the APK, just click on "Build."

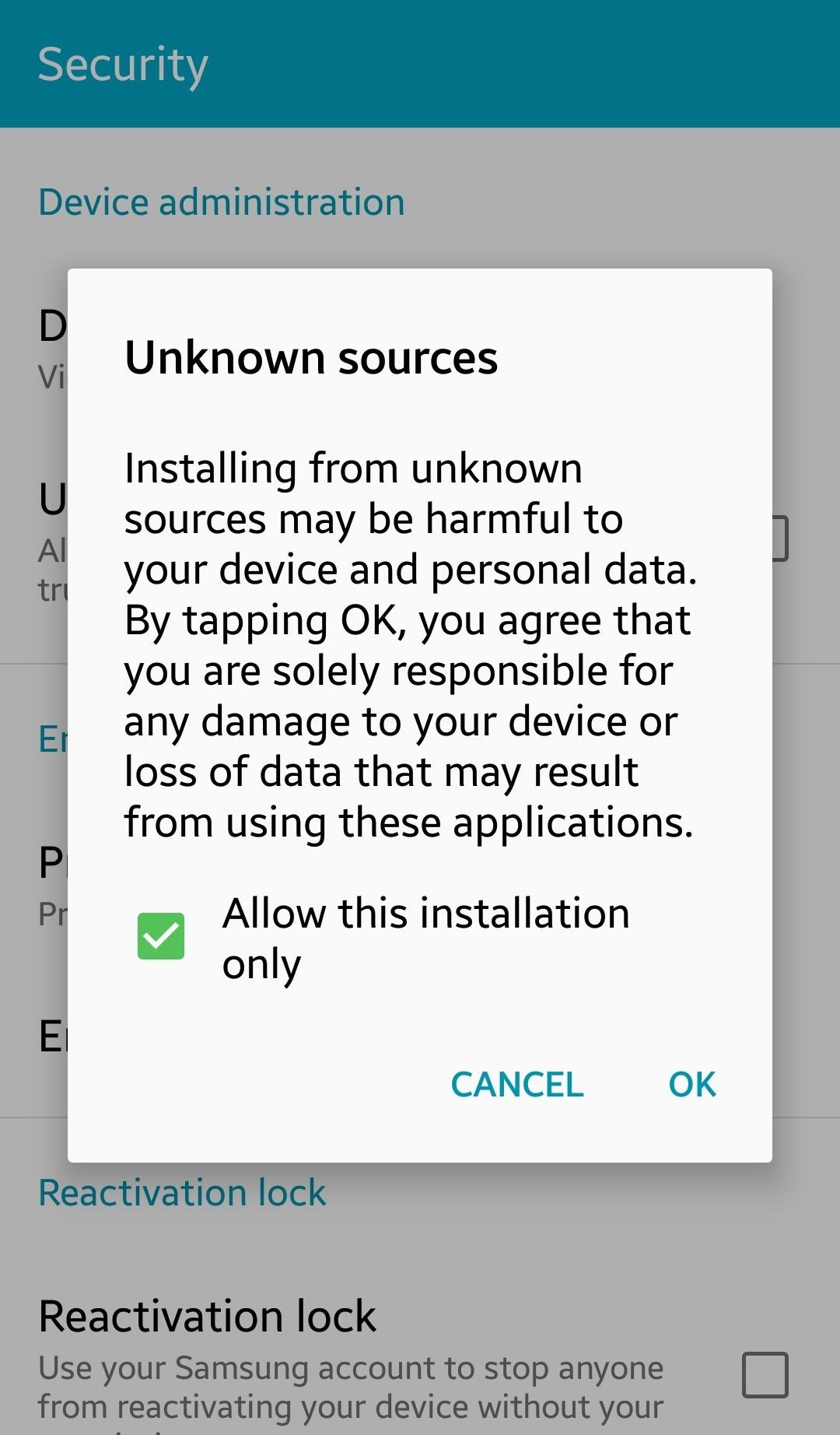
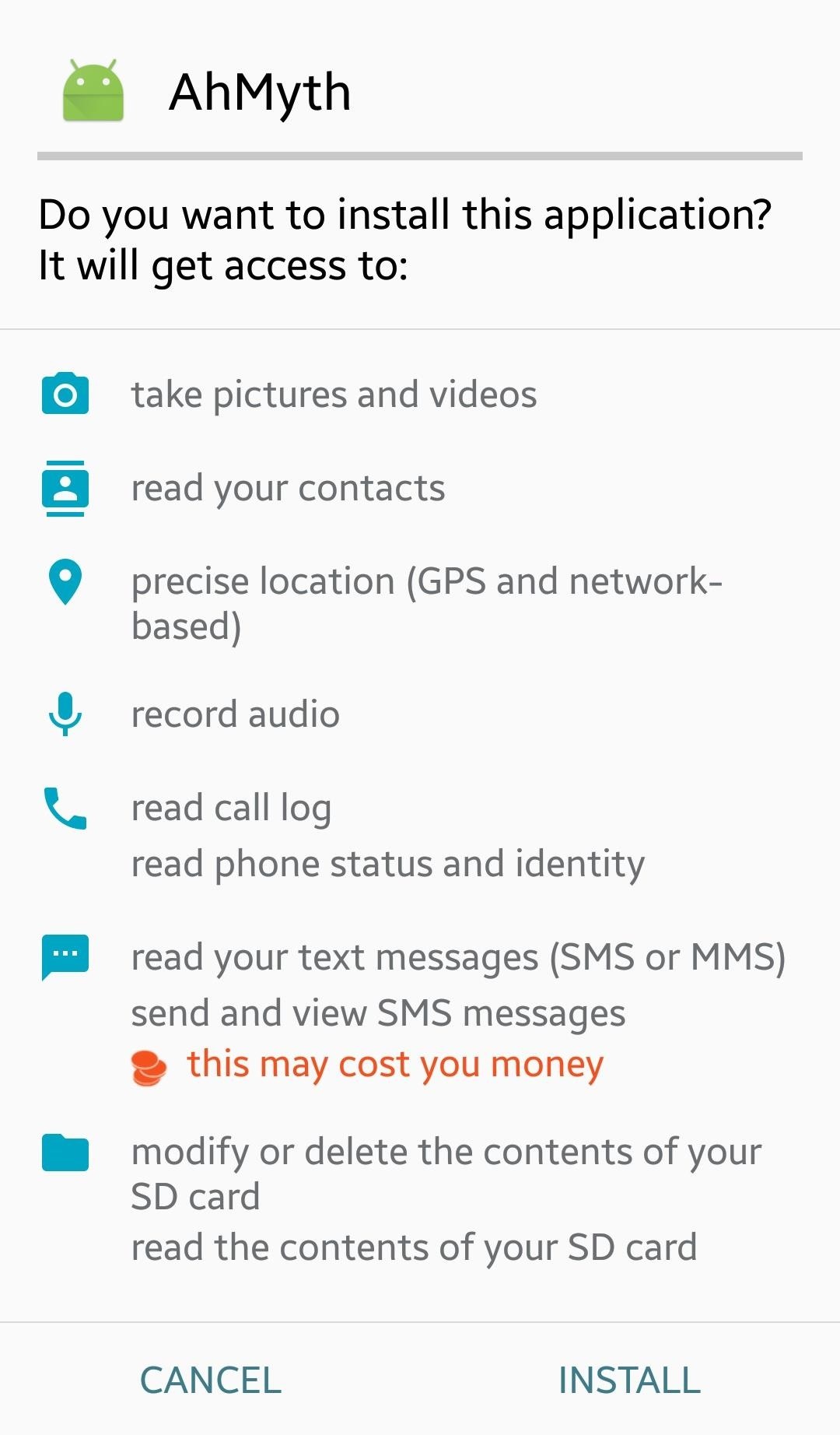
[](https://img.wonderhowto.com/img/original/33/06/63645817415421/0/636458174154213306.jpg)

You can navigate to to "C:\Users\**UserName**\AhMyth\Output" to find the built APK.

**Step 3Deploy the RAT**

Now that you have a working APK, it's time to deploy it by downloading it on the target Android device. All of the standard attack methods apply — anything to get the user to download the APK. [Social engineering](https://null-byte.wonderhowto.com/how-to/social-engineering/) tends to work best. For example, if you know the person, then recommend an app to them and infect it.

By far the most effective method is if you have physical access to the phone, it only takes a few seconds to download and hide it. If you chose this method, then an easy way to do it is by saving the APK to Google Drive and sending the phone a link. On most phones, the download should only take a second or two.

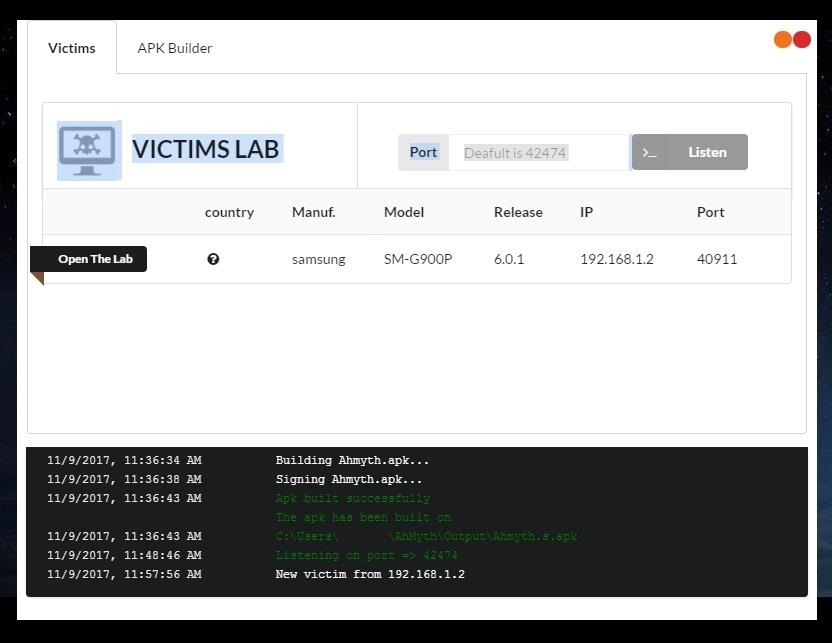
[](https://img.wonderhowto.com/img/original/41/49/63645818850054/0/636458188500544149.jpg)[](https://img.wonderhowto.com/img/original/25/98/63645819009601/0/636458190096012598.jpg)

If the Android phone doesn't want to install it, they probably never [enabled "Unknown sources"](https://android.gadgethacks.com/how-to/android-basics-enable-unknown-sources-sideload-apps-0161947/) in their settings. Open up the Settings, then go to "Security" and check "Unknown sources." This is how apps that come from outside the Google Play Store can be installed.

**More Info:** [**How to Enable Unknown Sources to Sideload Apps on Android**](https://android.gadgethacks.com/how-to/android-basics-enable-unknown-sources-sideload-apps-0161947/)

**Step 4Start to Listen**

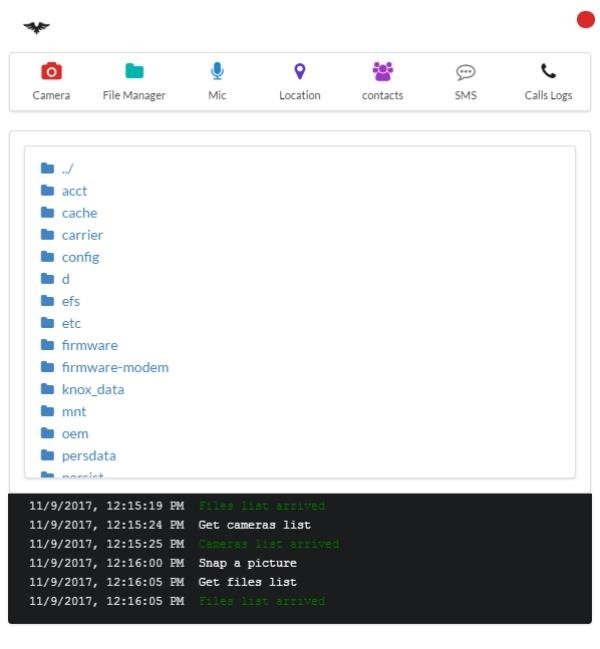
In the top left of the AhMyth screen, select the "Victims" tab, then change the *Port* number to the one you are using. You can also leave it blank for the default. Next, click on "Listen." Once this is done, and the RAT is running properly on the victim, then it should appear here along with some basic info.

[](https://img.wonderhowto.com/img/original/79/44/63645818442413/0/636458184424137944.jpg)

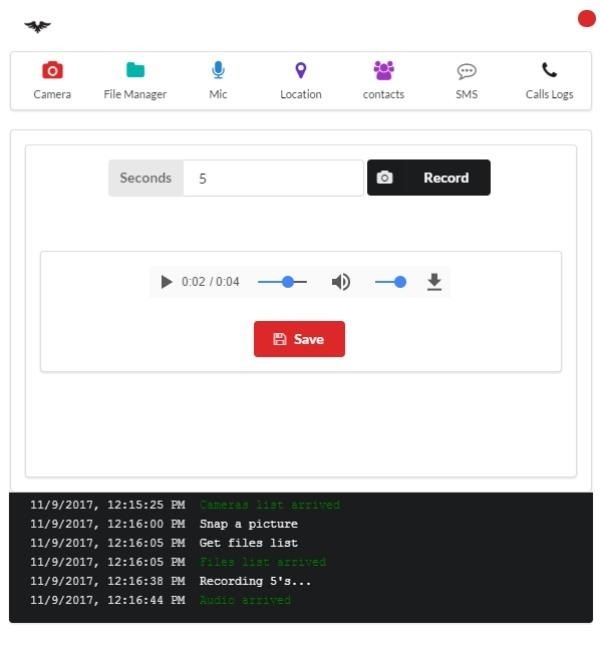
**Step 5Open the Lab**

Now that you have a RAT up and running on the target device, you can start doing remote administration. Click on "Open The Lab" button, and a new pop-up window will appear. If you're familiar with other Android RATs like [Cerberus](https://www.cerberusapp.com/), then you might be a little disappointed with how few features there are, but I would remind you that this is still only in the beta stages.

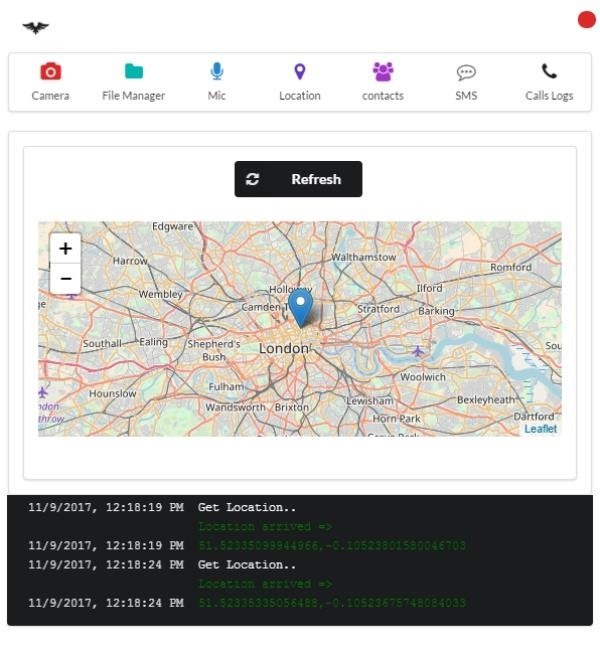
The features it does currently have are quite powerful. Let's take a look at a few of them. The "File Manager" is great because it lets you see everything on the device right down to the firmware. With this, you could potentially uncover all sorts of sensitive information, whether that be passwords and session cookies or compromising photos.

[](https://img.wonderhowto.com/img/original/54/99/63645820117132/0/636458201171325499.jpg)

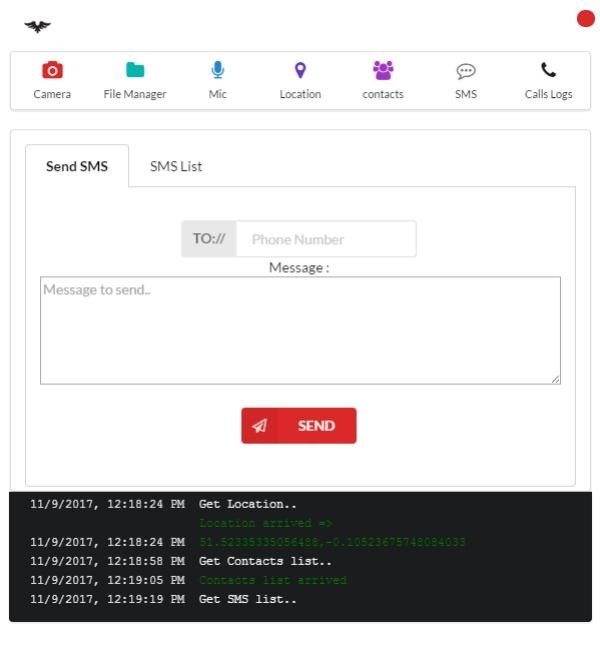
Another feature is the ability to record audio via "Mic." Since people take their phones with them everywhere they go, you, in effect, have a bug, or listening device, on them at all times.

[](https://img.wonderhowto.com/img/original/34/41/63645820390273/0/636458203902733441.jpg)

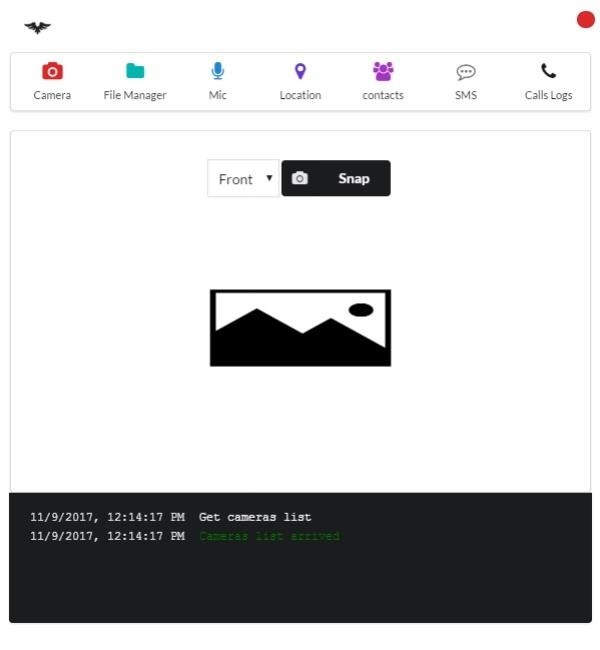
Along the same lines as the last one, you also have a tracking function ("Location") so you can not only know what they said, but also where they said it. One note on this, however, is that it can be fooled by a simple GPS spoofer application. I used one on the victim device to take the screenshot below.

[](https://img.wonderhowto.com/img/original/66/42/63645820326585/0/636458203265856642.jpg)

If you really like to sow chaos, then you'll love this next feature: the ability to not only read but also send "SMS" messages. A simple way to use this would be to [hack someone's Facebook](https://null-byte.wonderhowto.com/how-to/4-ways-crack-facebook-password-protect-yourself-from-them-0139532/) by resetting their password with an SMS text, then use the code that is sent. You can use your own imagination for all the things you can do by sending messages from the target's phone.

[](https://img.wonderhowto.com/img/original/32/12/63645820479726/0/636458204797263212.jpg)

Now you may have noticed that I skipped over the "Camera" feature. I did that because I was unable to get it working on my device, which could just be a problem with the old Android I was using for testing. In principle, it's supposed to allow you to send commands to take pictures with the front or rear camera and have them sent back to you.

[](https://img.wonderhowto.com/img/original/28/05/63645819960476/0/636458199604762805.jpg)

**Protecting Yourself from Android RATs**

There's not a whole lot you can do to protect yourself from RATs in general, but one thing you can do is not install Android apps that aren't from the Google Play Store. This doesn't mean that all the Google Play apps are safe, but they are much safer than some random app found online since Google does scan them for malware to the best of their abilities.

[Installing from "Unknown sources" is disabled by default in Android](https://android.gadgethacks.com/how-to/android-basics-enable-unknown-sources-sideload-apps-0161947), but if you allow this, you also greatly increase your risk as you will no longer get the security prompt. If you do ever have a legitimate reason to download an APK from outside Google Play, be sure to tap "Allow this installation only," otherwise you could accidentally permanently enable "Unknown sources."

Another way to protect yourself is to not take your phone to important meetings or anywhere you don't want people listening. Also, be careful who you let have your phone, as it only takes a few seconds to download one of these RATs. An example of this can be found in [*Mr. Robot*](https://null-byte.wonderhowto.com/how-to/mr-robot-hacks/), when Tyrell Wellick [installed malware on an employee's Android phone in seconds](https://null-byte.wonderhowto.com/how-to/hacks-mr-robot-spy-anyones-smartphone-activity-0163905/).

**Don't Miss:** [How to Spy on Anyone's Smartphone Activity Like in Mr. Robot](https://null-byte.wonderhowto.com/how-to/hacks-mr-robot-spy-anyones-smartphone-activity-0163905/)

One more probably obvious way to help prevent malicious software from installing on your Android device: keep it up to date. Install software updated when they come out, as Google and OEMs push on security fixes in almost every update, not just new features.

And last but not least, you can consider installing antivirus software on your Android device. This will not help you out all of the time, but it's better than nothing. You can find [a good list of antivirus apps for Android over on Gadget Hacks](https://android.gadgethacks.com/news/best-android-antivirus-avast-vs-avg-vs-kaspersky-vs-mcafee-0162518/).