Creating a safe dummy C&C to test Android bots

cryptax.medium.com/creating-a-safe-dummy-c-c-to-test-android-bots-ffa6e7a3dce5

@cryptax January 21, 2022

@cryptax

Jan 21

·

2 min read

To explain what a malware does, there’s no such good thing as showing in a video. But how can you do that safely? This is how I did it for Android/*BianLian*.

Thanks to *al1foobar* for his help with iptables ;-)

The bot

Simply use an Android emulator. The BianLian sample installs fine on Android 8.

The (fake) server

BianLian communicates to a C&C via HTTP. So, I created a quick Flask application to act as the web server.

At first, you don’t know all routes you need to serve. That’s not an issue, we’ll find them: run the fake server and notice all the HTTP 404 responses. They happen when the bot fails to contact a URL it needs. In the console, you’ll see the missing URL, add those in your code.

From my previous analysis of BianLian, I know the C&C sends back JSON data, and I know how some commands should be formatted. A fake server is great to test those commands safely, and see what they do + Flask dynamically reloads its code when it changes, so we can actually send different commands if we want.

Download my fake server template.

Redirecting to our fake server

Normally, the bot communicates to a C&C on `hxxp://rheacollier31532.website`. This name resolves (currently) to IP address `159.223.187.91`. So, what we'll do is redirect all traffic from the emulator and going to `159.223.187.91` on port `80` to the fake server (`127.0.0.1`) on the desired port (I used `9999`).

On Linux, use iptables: `sudo iptables -t nat -A OUTPUT -d 159.223.187.91 -p tcp -j DNAT — to-destination 127.0.0.1:9999`.

Test it on the emulator and open a browser, and request for example `hxxp://rheacollier31532.website`, you should see the request in your fake Flask server.

Videos

The resulting videos below.

Enjoy!

— the Crypto Girl