Information Security and Management
Review 1

Application remote access trojan for Android Hacking

ABHRANEEL DEY
20BPS1031

ABSTRACT

The main idea of this project is to create an application which would gain remote access to any Android Operating System.

The custom made application would be executed as a default app in the smartphone and all the information of the Android mobile phone will be available to the hacker.

android

Vulnerabilities of Android

01 Threat One: Data in Transit

Android is susceptible to man-in-the-middle attacks and various exploits that hack into unsecured communications over public Wi-Fi networks and other wireless communication systems.

02 Threat Two: Untrustworthy App Stores

Untrustworthy app stores can cause headaches due to lack of security protocols. Sideloading, in which you install apps without an app store, is also a process to manage carefully due to a lack of foundational security measures.

03 Threat Three: SMS Trojans

This type of app accesses a mobile device's calling or text message capabilities, allowing them to send text messages with malicious links to everyone in a user's address book.

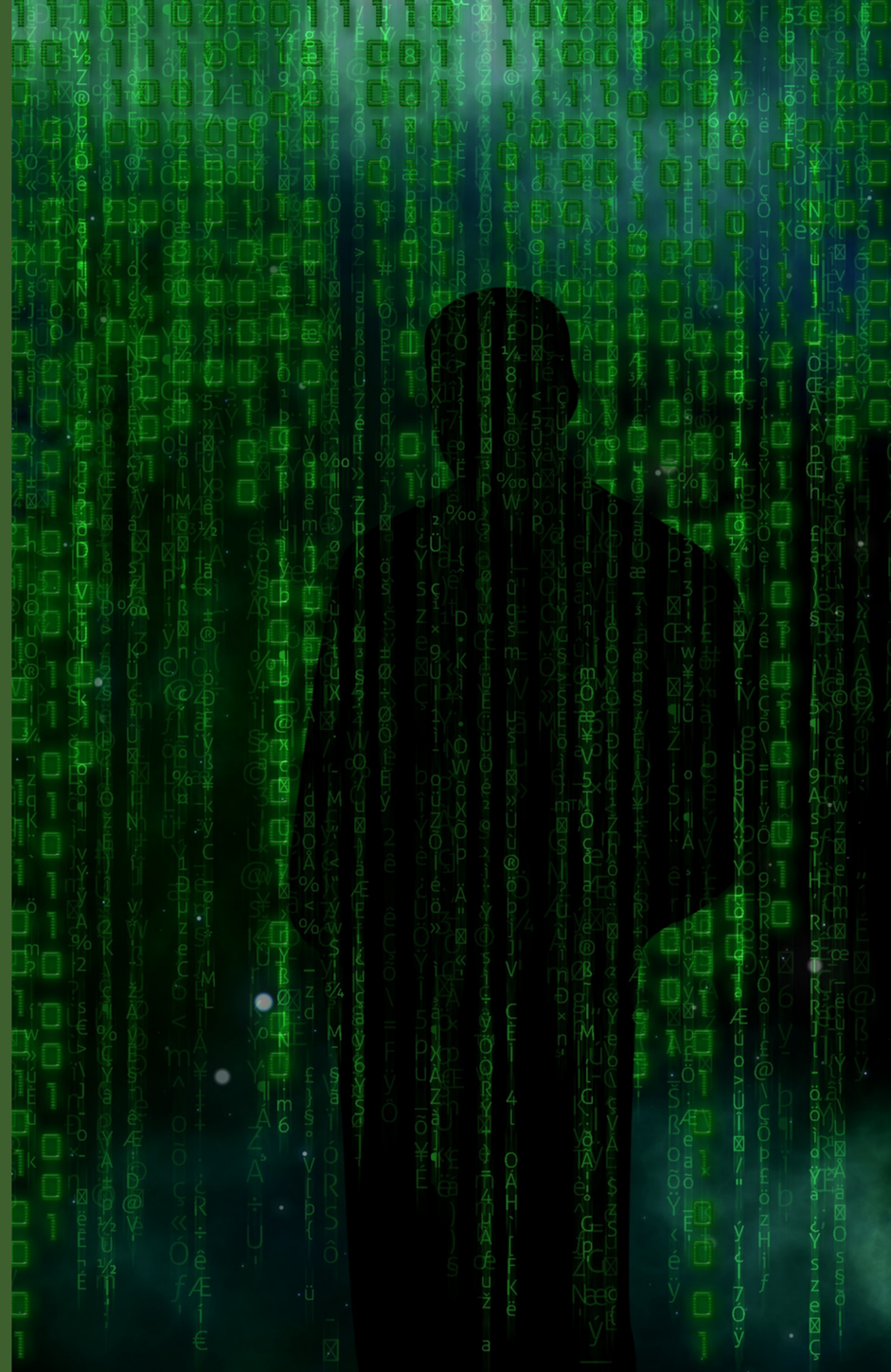
IMPLEMENTABLE IDEA

- The idea is to use a remote access trojan directory like ***FATRAT / PRORAT / ANDRORAT*** and clone it to the attacker machine
- Then changing or writing own python code to manipulate the RAT to work for Android OS
- Then using ***APKTOOL*** to reverse engineer Android Applications
- Then generating a mirror of some genuine application
- Then using the ***Msfvenom*** payload to generate an APK payload
- Finally using the remote meterpreter session of the Android phone to gain access

OUTCOME

Once the user downloads our application in their mobile phone and uses it, we get remote access through the meterpreter session from our attacking machine. Now we can exploit the complete device like:

- Find out the location of files
- Take pictures or videos
- Enable geolocation and get the live location
- Get access to the OS kernel etc.



THANK YOU