APPLICATION REMOTE ACCESS TROJAN FOR ANDROID HACKING

ABHRANEEL DEY
(20BPS1031)

CSE3502 - INFORMATION SECURITY MANAGEMENT

SUBMITTED TO: DR. NACHIYAPPAN S WINTER SEMESTER 2022-23 SLOT: G2

INTRODUCTION

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.

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.

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.

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.

METHODOLOGY

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

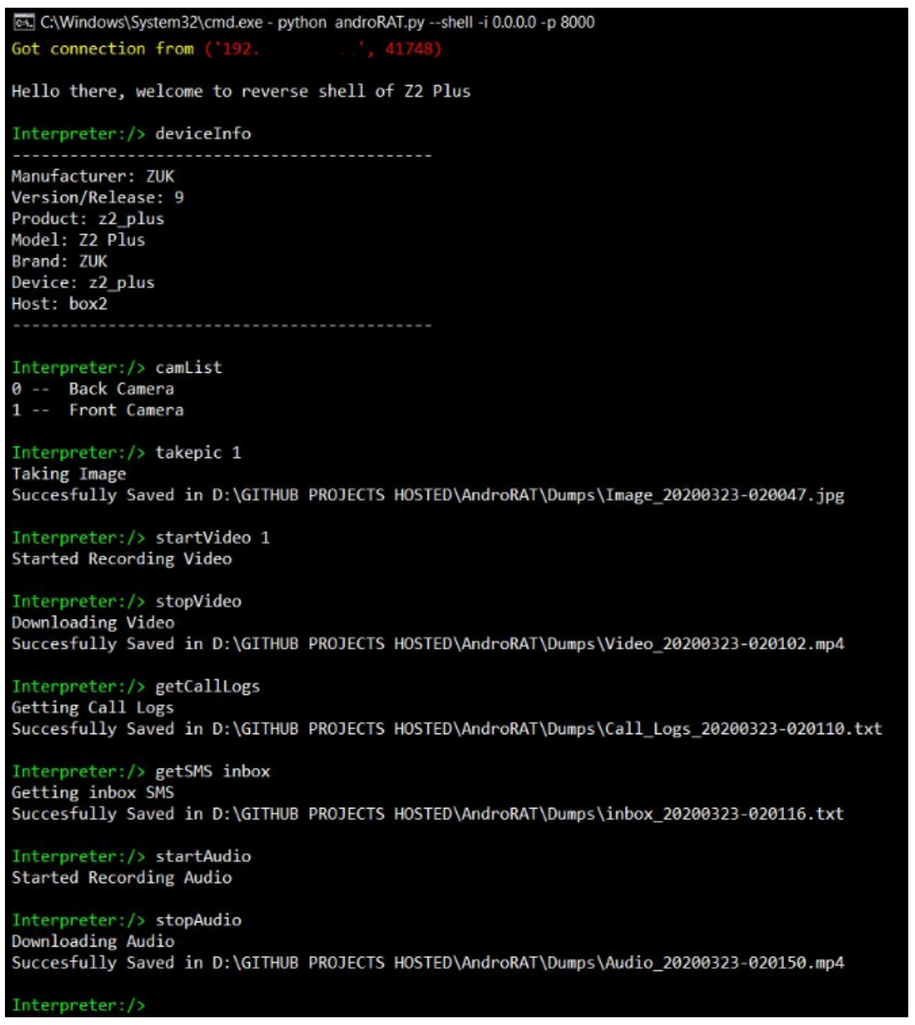
OUTCOME

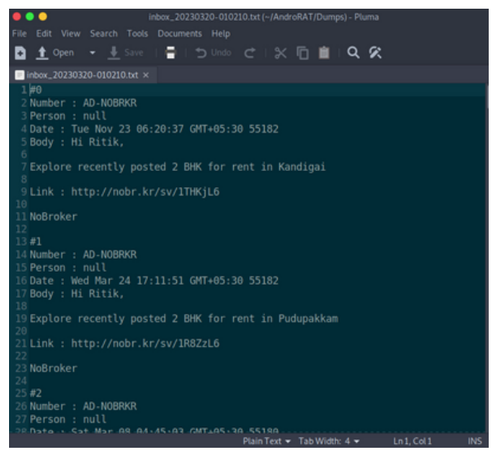
Once the user downloads our application in their mobile phone and uses it, we get remote access through the meterpeter session from our attacking machine. Now we can exploit the complete device like: Find out the location of files Take pictures or videos Enable geolocation and get the live location, get access to the OS kernel etc.

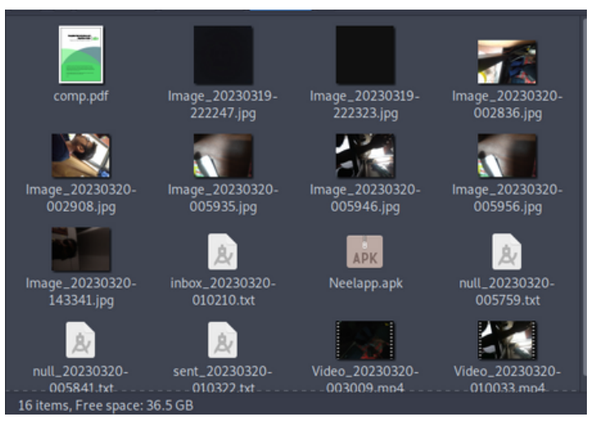
SCOPE

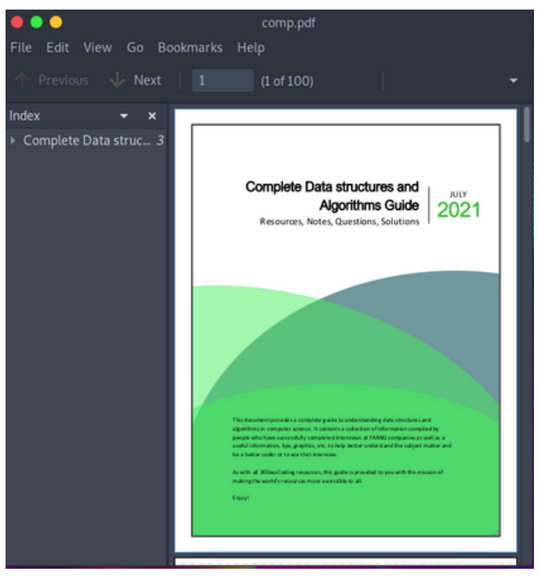
This project can be used in defense system to spy on mobile phones of enemies. Moreover this can be used in multiple ethical ways to hack into hazardous mobile phones to retrieve useful information or even track the complete cellphone.

RESULTS









CONTACT INFORMATION

abhraneel.dey2020@vitstudent.ac.in