Root Detection Bypass with frida-push + Objection for iOS and Android

AHMET RECEP SAGLAM

Root Detection Bypass with frida-push + Objection for iOS and Android

What is Frida and Objection?

To better understand how Frida works, we first need to know about **DBI** (Dynamic Binary Instrumentation). Instrumentation means measuring the performance of an application or detecting errors in computer programming. DBI is one of these instrumentation approaches. With DBI, processes in running applications can be analyzed and modified. Frida is a DBI tool and is a tool that allows you to dynamically modify the processes of an application.

Objection is an application written in frida and is a tool for dynamic analysis in the same way as frida. The difference from frida is that it includes frequently used scripts.

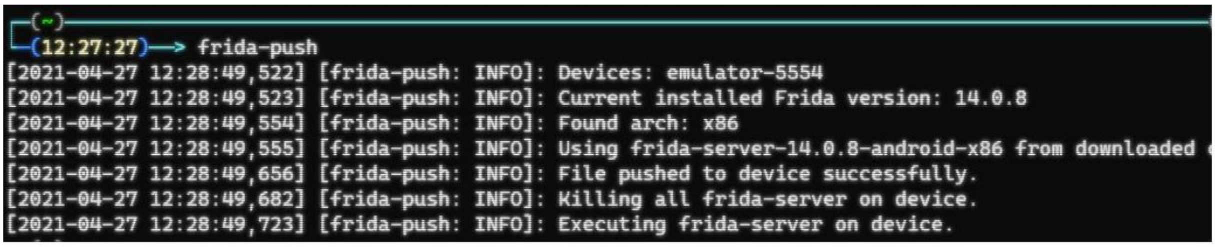
There is a file called frida-server that needs to be installed for Frida or objection to communicate with the device. This file varies depending on the Android version and architecture. The name of the tool developed to simplify its installation is frida-push.

Setup

```
pip3 install frida-push
pip3 install objection
```

Root Detection Bypass

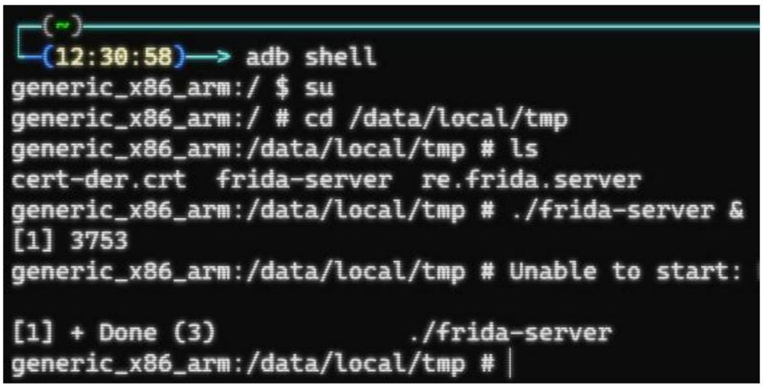
We install frida-server on our device with our frida-push tool.



```
┌─(~)
└─(12:27:27)──> frida-push
[2021-04-27 12:28:49,522] [frida-push: INFO]: Devices: emulator-5554
[2021-04-27 12:28:49,523] [frida-push: INFO]: Current installed Frida version: 14.0.8
[2021-04-27 12:28:49,554] [frida-push: INFO]: Found arch: x86
[2021-04-27 12:28:49,555] [frida-push: INFO]: Using frida-server-14.0.8-android-x86 from downloaded
[2021-04-27 12:28:49,656] [frida-push: INFO]: File pushed to device successfully.
[2021-04-27 12:28:49,682] [frida-push: INFO]: Killing all frida-server on device.
[2021-04-27 12:28:49,723] [frida-push: INFO]: Executing frida-server on device.
```

Then we connect to our device with adb Shell and run frida-server from the /data/local/tmp directory.

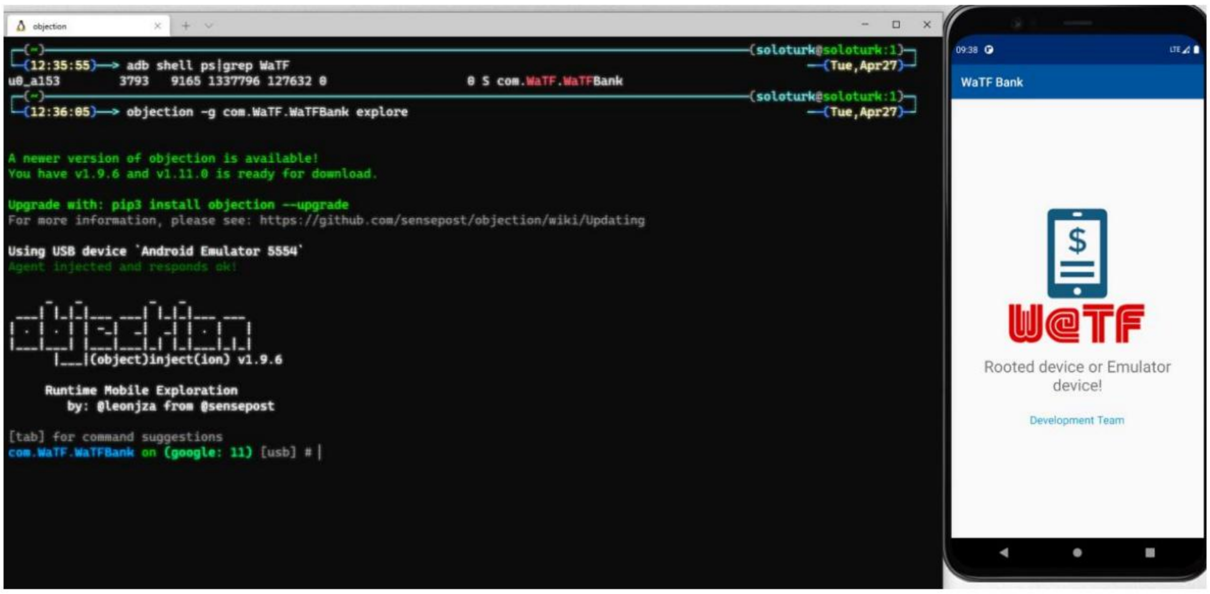
Adb Shell
Cd /data/local/tmp
./frida-server &



```
┌─(~)
└─(12:30:58)──> adb shell
generic_x86_arm:/ $ su
generic_x86_arm:/ # cd /data/local/tmp
generic_x86_arm:/data/local/tmp # ls
cert-der.crt  frida-server  re.frida.server
generic_x86_arm:/data/local/tmp # ./frida-server &
[1] 3753
generic_x86_arm:/data/local/tmp # Unable to start:

[1] + Done (3)              ./frida-server
generic_x86_arm:/data/local/tmp # |
```

Later, when you start the application and list the processes with adb, the name and pid number of the application are determined. Objection is run with the Objection -g [applicationname] explore command.

adb shell ps| grep WaTF
objection –g com.WaTF.WaTFBank explore

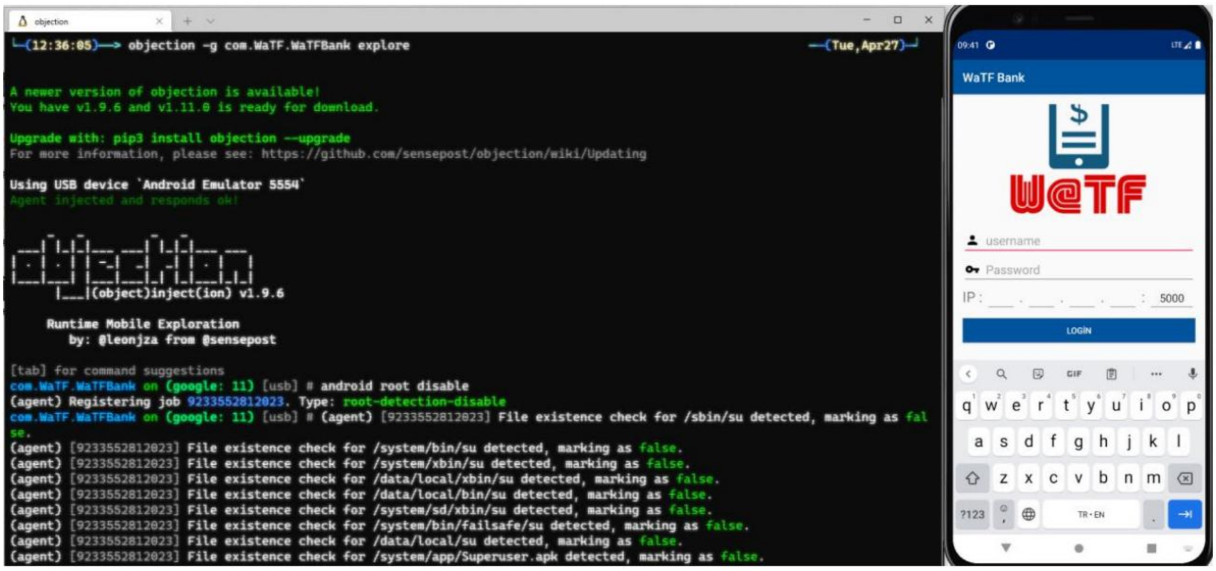


```
┌─(~)────────────────────────────────────────────────(soloturk@soloturk:1)─┐
└─(12:35:55)──> adb shell ps|grep WaTF                          ─(Tue,Apr27)─┘
u0_a153      3793   9165 1337796 127632 0              0 S com.WaTF.WaTFBank
┌─(~)────────────────────────────────────────────────(soloturk@soloturk:1)─┐
└─(12:36:05)──> objection -g com.WaTF.WaTFBank explore          ─(Tue,Apr27)─┘

A newer version of objection is available!
You have v1.9.6 and v1.11.0 is ready for download.

Upgrade with: pip3 install objection --upgrade
For more information, please see: https://github.com/sensepost/objection/wiki/Updating

Using USB device `Android Emulator 5554`
Agent injected and responds ok!

     |___|(object)inject(ion) v1.9.6

     Runtime Mobile Exploration
        by: @leonjza from @sensepost

[tab] for command suggestions
com.WaTF.WaTFBank on (google: 11) [usb] # |
```

Rooted device or Emulator device!

Development Team

The root bypass operation is performed by running the android root disale command from within the Objection tool. When the application is put into the background and called again, the bypass operation of the root check will be completed successfully.



```
└─(12:36:05)──> objection -g com.WaTF.WaTFBank explore                                        ──(Tue,Apr27)─┘

A newer version of objection is available!
You have v1.9.6 and v1.11.0 is ready for download.

Upgrade with: pip3 install objection --upgrade
For more information, please see: https://github.com/sensepost/objection/wiki/Updating

Using USB device `Android Emulator 5554`
Agent injected and responds ok!

     _   _         _   _
 ___| |_|_|___ ___| |_|_|___ ___
| . | . | | -_|  _|  _| | . |   |
|___|___| |___|___|_| |_|___|_|_|
      |___|(object)inject(ion) v1.9.6

     Runtime Mobile Exploration
        by: @leonjza from @sensepost

[tab] for command suggestions
com.WaTF.WaTFBank on (google: 11) [usb] # android root disable
(agent) Registering job 9233552812023. Type: root-detection-disable
com.WaTF.WaTFBank on (google: 11) [usb] # (agent) [9233552812023] File existence check for /sbin/su detected, marking as fal
se.
(agent) [9233552812023] File existence check for /system/bin/su detected, marking as false.
(agent) [9233552812023] File existence check for /system/xbin/su detected, marking as false.
(agent) [9233552812023] File existence check for /data/local/xbin/su detected, marking as false.
(agent) [9233552812023] File existence check for /data/local/bin/su detected, marking as false.
(agent) [9233552812023] File existence check for /system/sd/xbin/su detected, marking as false.
(agent) [9233552812023] File existence check for /system/bin/failsafe/su detected, marking as false.
(agent) [9233552812023] File existence check for /data/local/su detected, marking as false.
(agent) [9233552812023] File existence check for /system/app/Superuser.apk detected, marking as false.
```