Using Mobile Malware tactics for red teaming

November 2019
— Mobile solution lead at NVISO
— Primary author of SEC575 (NVISO)
— Co-author of
  — OWASP Mobile Security Testing Guide (MSTG)
  — OWASP Mobile Application Security Verification Standard (MASVS)
Mobile devices
Malware tactics for red teeming
Mobile Malware in a tiny nutshell

Malware tactics for red teaming

Ransomware

In-app Products
€13.99 - €104.99 per item

Subscription scams

Ad fraud

Premium text fraud
Mobile Banking Trojans
Malware tactics for red teaming

Malicious mobile banking trojans grew by 58% in Q1 2019

BY ALEX ROLFE  MAY 28, 2019  DAILY NEWS

Anubis Android banking malware returns with extensive financial app hit list

Thousands of new samples are targeting 188 banking and finance-related apps.

By Charlie Osborne for Zero Day | July 9, 2019 -- 09:29 GMT (10:29 BST) | Topic: Security
Android vs iOS
Malware tactics for red teaming
Necessary steps

Malware tactics for red teaming

Create application

Install application

Get the data
Creating an application
Different options

Creating an application
How does malware do it?

Creating an application
Can we do it?

Creating an application

Lime - Your Ride Anytime

Neuron Holdings, Inc.  Travel & Local

Add to Wishlist

Install
Obtaining a valid APK

Creating an application

STEP 1  Get APK from device

```
adb pull /data/app/com.limebike-1/base.apk
/data/app/com.limebike-1/base.apk: 1 file pulled. 23.6 MB/s (26939075 bytes in 1.090s)
```
Modifying the application

Creating an application

STEP 2

Decompile the application

```
$ apktool d base.apk
I: Using Apktool 2.4.0 on base.apk
I: Loading resource table...
...
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Baksmaling classes3.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

Malware For Red Teaming
SMALI code

Creating an application
Adding SMALI code

Creating an application

STEP 3

Modify

```smali
// MessagesPagerDialogFragment
// n.smalii
// n0.smalii
// NavigationOption.smalii
// o.smalii
// o0.smalii
// OnboardActivity$s.a.smalii
// OnboardActivity.smalii
// OnboardActivity_ViewBinding.smalii
// p0$s.a.smalii
// p0$b.smalii
// p0$c.smalii
// p0$d.smalii
// p0$e.smalii
// p0.smalii
// PromoCodeFragment$a.smalii
// PromoCodeFragment$b.smalii
// PromoCodeFragment.smalii
// PromoCodeFragment_ViewBinding.smalii

.method protected onCreate(Landroid/os/Bundle;)V
    .locals 2
    const/4 v0, 0x1
    const-string v1, "Welcome to this special BETA"
    invoke-static {p0, v1, v0}, Landroid/widget/Toast;->makeText(Landroid/content/Context;Ljava/lang/CharSequence;)Landroid/widget/Toast;
    move-result-object v0
    invoke-virtual {v0}, Landroid/widget/Toast;->show()V

    .line 1
    invoke-static {}, Lcom/limebike/u0/a;->a(Lcom/limebike/u0/a$);
    move-result-object v0

    .line 2
    invoke-virtual {p0}, Landroid/app/Activity;->getApplication()Landroid/app/Application;
```
Recompiling & signing
Creating an application

STEP 4
Recompile & sign

```
» apktool b base
I: Using Apktool 2.4.0
...
I: Building apk file...
I: Built apk...
» jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore keystore.keystore base/dist/base.apk  mykeystore
...
  adding: META-INF/MYKEYSTORE.RSA
  signing: resources.arsc
  ...
jar signed.
```
Testing the application

Creating an application

Possible hurdles:

- Original application already installed
- Application contains Runtime Application Self Protection (RASP)
A toast message is nice, but ...

Creating an application

DexClassLoader

```java
public class DexClassLoader
extends BaseDexClassLoader
```

A class loader that loads classes from .jar and .apk files containing a `classes.dex` entry. This can be used to execute code not installed as part of an application.
Installing the application
Different approaches

Installing the application

[Logos of Google Play, Apkpure, Amazon Appstore, Aptoide, NVISO]
How does malware do it?

Installing the application

Millions of Android users tricked into downloading 85 adware apps from Google Play

Zack Whittaker @zackwhittaker / 7 months ago

Half a million Android users tricked into downloading malware from Google Play

Zack Whittaker @zackwhittaker / 8 months ago
Chamois Family

Installing the application

- 5 stages of obfuscation and anti-RE
- Dynamic payload system
- Premium SMS & Ad fraud

Source: Chamois: The Most Impactful Android Botnet of 2018 - Maddie Stone
How does malware do it?

Installing the application

Source: Android Security & Privacy 2018 Year In Review (Google)
Third party app stores

Installing the application
Drive-by downloads

Installing the application
Can we do it?

Installing the application

Yes, but…

Easy installation ✓

Accepts malware ✗

Allowed by EULA ✗

Controlled environment ✗

Loading external code ✗
Can we do it?

Installing the application

Yes, but...

- Easy installation: ✔️
- Accepts malware: ✗
- Allowed by EULA: ✗
- Controlled environment: ✗
- Loading external code: ✗
Can we do it?

Installing the application

Yes, but…

- Easy installation: ✅
- Accepts malware: ❌
- Allowed by EULA: ❌
- Controlled environment: ✅
- Loading external code: ✅

Join our BETA and ride for free!
Participate in our BETA of the application and ride for free the entire week!

Step 1
Download the beta application

Step 2
Install the application* and log in
*You may have to temporarily allow external sources to...
Get the data
Application sandboxes

Get the data
How does malware do it?

Accessibility

Overlay attacks

Phishing
Accessibility (A11Y)

Get the data

![Accessibility Icon]

**Use TalkBack?**

TalkBack wants permission to:

- **Monitor your actions**
  - Allows TalkBack to know when you are using an app.

- **Retrieve window content**
  - Inspect the content of a window you’re interacting with.

- **Turn on Explore by Touch**
  - Touched items will be spoken aloud and the screen can be explored using gestures.

- **Turn on enhanced web accessibility**
  - Scripts may be installed to make app content more accessible.

- **Observe text you type**
  - Includes personal data such as credit card numbers and passwords.

[Settings] [Cancel] [OK]
Accessibility (A11Y)

Get the data

For applications to work properly, enable Google Service!

The Services are provided by Google Inc. ("Google"), located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States.

By using our Services, you are agreeing to these terms. Please read them carefully.

Our Services are very diverse, so sometimes additional terms or product requirements (including age requirements) may apply. Additional terms will be available with the relevant Services, and those additional terms become part of your agreement with us if you use those Services.

You must follow any policies made available to you within the Services.

Don’t misuse our Services. For example, don’t interfere with our Services or try to access them using a method other than the interface and the instructions that we provide. You may use our Services only as permitted by law, including applicable export and re-export control laws and regulations. We may suspend or stop providing our Services to you if you do not comply with our terms or policies or if we are investigating suspected misconduct.

Distracts you and prevents you from obeying traffic or safety laws.

Observe your actions
Receive notifications when you’re interacting with an app.

Retrieve window content
Inspect the content of a window you’re interacting with.

Turn on Explore by Touch
Touched items will be spoken aloud and the screen can be explored using gestures.

Turn on enhanced web accessibility
Scripts may be installed to make app content more accessible.
Overlay attacks

Get the data

SYSTEM_ALERT_WINDOW

public static final String SYSTEM_ALERT_WINDOW

Allows an app to create windows using the type
WindowManager.LayoutParams.TYPE_APPLICATION_OVERLAY, shown on top of all other apps. Very few apps should use this permission; these windows are intended for system-level interaction with the user.
BankBot

Get the data
Can we do it?

Get the data

- Annoy user to give access
- Pretend to be Google / Samsung / …
- Full control over all visual items

- Not granted by default
- Can be activated with Accessibility
- Probably not needed
Can we do it? – Credentials

Get the data

Intune

Enter password

Microsoft

jeroen@mobilesearch.onmicrosoft.com

Password

Forgot my password

Sign in with another account

Sign in

Gmail

Corporate WiFi

Password

Show password

Advanced options

WIFI

Full control
Can we do it? – 2FA

Get the data

G Suite

MS Authenticator
Conclusion
Can we do it?

Conclusion

Create application
- Easy to copy
- Some development required

Install application
- Social engineering
- Blocked by MDM

Get the data
- Easy social engineering
- Most applications not protected
Thank you!

Jeroen Beckers
linkedin.com/in/beckersjeroen
jbeckers@nviso.be