Hesperbot

Analysts at IKARUS Security Software GmbH
successfully removed a self-locking Android Malware
from an infected smartphone

Android malware is evolving at an alarming rate and becoming more aggressive and resilient in nature. This shift shows attempts to target bank accounts, messages and other personal information. It seems that cyber criminals are no longer satisfied with what they steal from their victims. Now, they try to inflict damage by other means; the latest case shows sophisticated banking malware that tries to deny all access to the victim’s smartphone using crafty software means.

Back in April of 2014, our malware analysts came across a particularly dangerous variant of the Trojan.AndroidOS.Hesperbot (see Figure 1 to view the launcher icon) that, besides stealing personal banking data and personal messages, managed to lock the user completely out of his/her smartphone. The creators of this type of malware used various methods of social engineering, like fear tactics and phishing to trick the user into installing their "very secure certificate".

Before the smartphone is infected, the victim's PC has to also be infected with an online banking Trojan. This is where the desktop version of Hesperbot (Trojan.Win32.Hesperbot) comes into play. This malware is sent through a phishing mail or downloaded while surfing suspicious websites. If the victim connects to their online bank account, a message gets injected into the website's data stream and it tricks the user to install the android app. After the installation, an activation code is generated (see Figure 2) and also verified on the modified website. At this point, the attacker is aware that someone has fallen for the trick and can start to collect money from the victim's bank account.

Shockingly, it does not end here. The mobile app asks the user now for "Device Administrator" rights, a tool mostly used by MDM Systems and corporate applications. If this permission is granted, the malicious app can prevent itself from being uninstalled. The attacker specifically designed the approval dialog in a way that makes it impossible for the user not to activate the app. The dialog will pop-up again and again and will make the device completely unusable, unless the user selects "Activate" (see Figure 3).

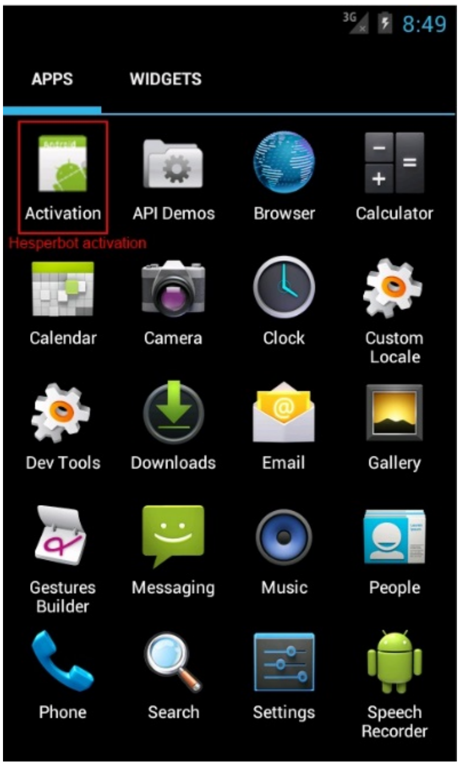
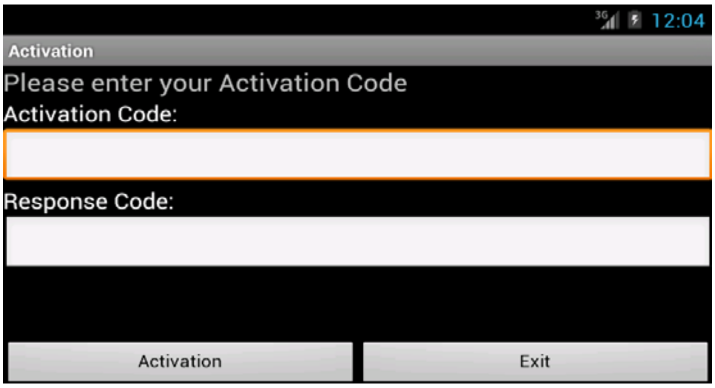


Figure 1: Android launcher menu, presenting the installed Hesperbot under the name „Activation".



Activation

Please enter your Activation Code

Activation Code:

Response Code:

Figure 2: Hesperbot requesting activation code from the user.

The locking of the smartphone only occurs when the user tries to uninstall the “certificate” App and the malware detects this. Once the malware has administrator rights, Android’s built in password protected lock screen activates and locks the smartphone using a password generated by the malware. The generated code is of course unknown to the user. This way all the data that is present on the smartphone will be locked away from the user, rendering the smartphone useless. (See Figure 4.)

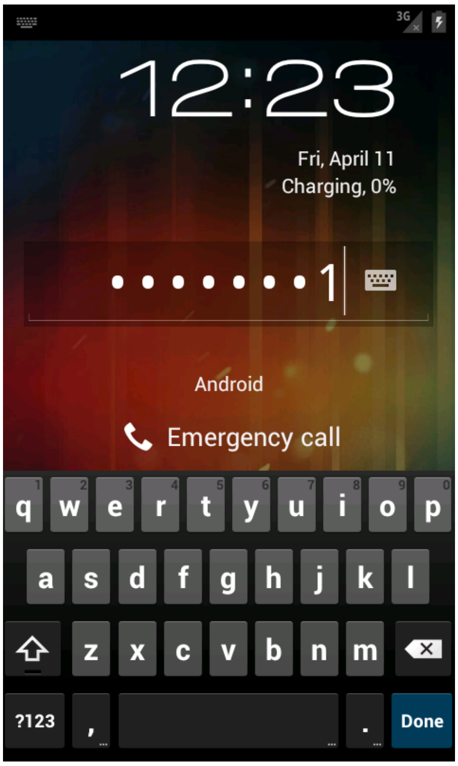
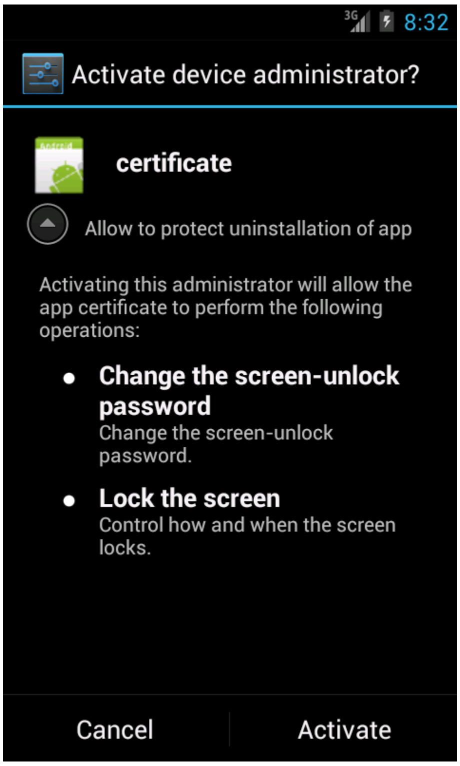


Figure 3: Attempt to unlock the infected smartphone



Activate device administrator?

certificate

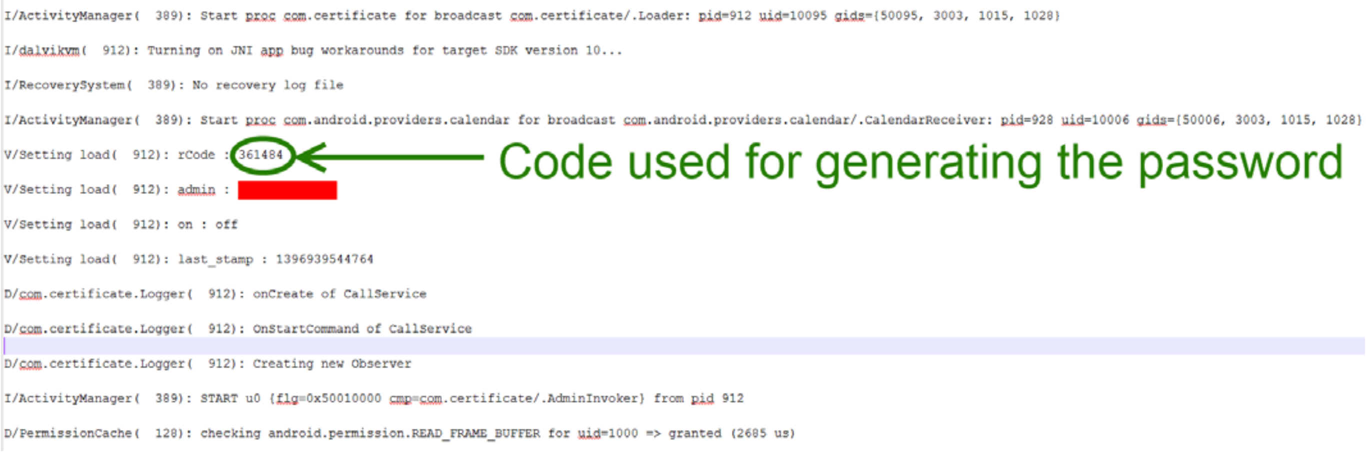
Allow to protect uninstallation of app

Activating this administrator will allow the app certificate to perform the following operations:

- **Change the screen-unlock password**
  Change the screen-unlock password.
- **Lock the screen**
  Control how and when the screen locks.

Figure 4: Hesperbot requesting administrator rights.

Here at IKARUS Security Software GmbH our talented analysis team found a way to unlock smartphones that were infected by Hesperbot and remove the malware, without causing data loss. Since sensitive data on the smartphone cannot be accessed by normal means and the data that we needed was only available to the malware that was sitting on the smartphone, our team had to hack the smartphone and override the installed malware to make it reveal its code for us.

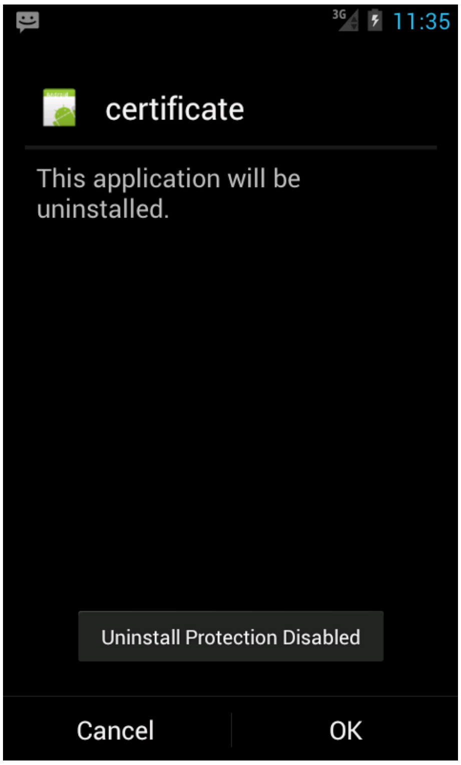


```
I/ActivityManager(  389): Start proc com.certificate for broadcast com.certificate/.Loader: pid=912 uid=10095 gids={50095, 3003, 1015, 1028}

I/dalvikvm(  912): Turning on JNI app bug workarounds for target SDK version 10...

I/RecoverySystem(  389): No recovery log file

I/ActivityManager(  389): Start proc com.android.providers.calendar for broadcast com.android.providers.calendar/.CalendarReceiver: pid=928 uid=10006 gids={50006, 3003, 1015, 1028}

V/Setting load(  912): rCode : 361484

V/Setting load(  912): admin : [redacted]

V/Setting load(  912): on : off

V/Setting load(  912): last_stamp : 1396939544764

D/com.certificate.Logger(  912): onCreate of CallService

D/com.certificate.Logger(  912): OnStartCommand of CallService

D/com.certificate.Logger(  912): Creating new Observer

I/ActivityManager(  389): START u0 {flg=0x50010000 cmp=com.certificate/.AdminInvoker} from pid 912

D/PermissionCache(  128): checking android.permission.READ_FRAME_BUFFER for uid=1000 => granted (2685 us)
```

Code used for generating the password

Figure 5: Tricking the malware into giving away ist code.

After the code was found (see Figure 5), our team used the malware's own malicious code to generate the password that finally unlocked the infected smartphone. At this point removing the malware (that now became harmless) was a routine task (see Figure 6).



certificate

This application will be uninstalled.

Figure 6: Successful uninstallation of Trojan.AndroidOS.Hesperbot

We at IKARUS suggest the use of mobile anti-virus to protect your handheld device from viruses like Hesperbot. Our very own **IKARUS mobile.security** App is capable of doing just that and even more. Check out **IKARUS mobile.security** in Google Play and make a step towards a more secure Android smartphone.

Authors:

Sebastian Bachmann, BSc

Tibor Éliás, BSc