Infamous Aberebot android banking trojan has returned as Escobar with new features, including stealing Google Authenticator multi-factor authentication code.

The new feature in the latest Escobar version includes remote control of the infected Android devices using VNC, recording audio, and taking photos, while also expanding the set of targeted apps for credential theft. The main goal of this trojan is to steal bank account details, check available balances and perform unauthorized banking transactions.

The owner of the malware is renting its beta version for $3000 per month for a max of five customers and also they are planning to raise its price to $5000. One can use its free version for free for three days.

During the investigation by the Cyble team, security researchers came across twitter posts. In that researcher has mentioned a malware whose name and icon are similar to legitimate antivirus McAfee. The researcher also found that this malware is the latest variant of the popular banking Trojan, Aberebot. This new variant is capable of stealing 2FA Code.

Technical Analysis

APK Metadata Information

- Name: McAfee
- Package: com.escobar.pablo
- SHA256 Hash: a9d1561ed0d23a5473d68069337e2f8e7862f7b72b74251eb63ccc883ba9459f

The malware requests users for 25 different permissions, some of that permission is listed below.

Permissions Description

- READ_SMS Access and read SMS from the victim’s device.
- RECEIVE_SMS Intercept SMS received on the victim’s device
- READCALLLOG Give access Call details
- READ_CONTACTS Give access phone contact.
- READPHONESTATE Give access to phone state, including the current cellular network information, the phone number and the serial number of the phone, the status of any ongoing calls, and a list of any Phone Accounts registered on the device.
- RECORD_AUDIO Give access the app to record audio with the microphone, which has the potential to be misused by attackers
- ACCESSFINELOCATION Give access to the device’s precise location to be detected by using the Global Positioning System (GPS).
- SEND_SMS Give access to the application to send SMS messages.
- CALL_PHONE Give access to an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call.
- WRITEEXTERNALSTORAGE Give access the app to write or delete files in the device’s external storage
- READEXTERNALSTORAGE Give access the app to read the contents of the device’s external storage
- WRITE_SMS Give access to the app to modify or delete SMS.

Source code review - The researcher has observed a defined launcher activity in the malicious app’s manifest file, which loads the first screen of the app, as shown in the below figure

Below are a few commands used by the application to control the infected device.

Command Description

- Take Photo Capture images from the device’s camera
- Send SMS Send any SMS to a particular number
- Send SMS to All Contacts Automatically send SMS to all the contact numbers saved in the device
- Inject a web page Inject a malicious URL
- Download File Let download media files from the victim’s device
- Kill Bot Delete itself
- Uninstall an app Uninstall an application

Indicators Of Compromise

Indicators Indicator Type Description

22e943025f515a398b2f559c658a1a188d0d889f SHA1 Escobar APK

a9d1561ed0d23a5473d68069337e2f8e7862f7b72b74251eb63ccc883ba9459f SHA256 Escobar APK

d57e1c11f915b874ef5c86cedb25abda MD5 Escobar APK

How To Prevent Malware Infection

- Download and install software only from official app stores like Google Play Store or the iOS App Store.
- Use reputed anti-virus software.
- Use strong passwords and enforce multi-factor authentication(2FA).
- Enable biometric security features such as fingerprint or face recognition for unlocking the mobile device where possible.
- Be wary of opening any links received via SMS or emails delivered to your phone.
- Be careful while enabling any permissions.

How To Identify Whether You Are Infected

- Regularly check the Mobile/Wi-Fi data usage and battery usage of applications installed in mobile devices.

What To Do When You Are Infected

- Disable Wi-Fi/Mobile data and remove SIM card — as in some cases, the malware can re-enable the Mobile Data.
- Remove the application in case a factory reset is not possible.
- Perform a factory reset.