Nasty Escobar Banking Trojan Is Targeting Google Authenticator Codes For Android

hothardware.com/news/escobar-banking-trojan-targets-mfa-codes

Lane Babuder March 14, 2022

home News

by **Lane Babuder** — Monday, March 14, 2022, 01:58 PM EDT

Did you ever think you would have a digital drug lord in the palm of your hand? No, we're not talking about a game. We're talking about malware that aims to steal your banking information. A new variant of the Abrebot malware has been nicknamed "Escobar" after its package name.

With the package name of *com.escobar.pablo*, the malware includes a number of the same features and code as another one named Aberebot. Researchers at Cyble, a security research organization, found the malware by scouring a cybercrime-oriented forum. The feature set includes remote view, phishing overlays, screen captures, text-message captures, and even multi-factor authentication capture.

All of those features are used in tandem with an attempt to steal a user's banking information. This malware even goes so far as to disguise itself as McAfee antivirus software, and even uses the McAfee logo as its icon. Masquerading as security software is nothing new—in fact, we recently reported on malware that was packaged directly inside of a fully functioning 2-factor authentication app.

Permissions	Description
READ_SMS	Access SMSes from the victim's device.
RECEIVE_SMS	Intercept SMSes received on the victim's device
READ_CALL_LOG	Access Call Logs
READ_CONTACTS	Access phone contacts
READ_PHONE_STATE	Allows 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	Allows the app to record audio with the microphone, which has the potential to be misused by attackers
ACCESS_COARSE_LOCATION	Allows the app to get the approximate location of the device network sources such as cell towers and Wi-Fi.
ACCESS_FINE_LOCATION	Allows the device's precise location to be detected by using the Global Positioning System (GPS).
SEND_SMS	Allows an application to send SMS messages.
CALL_PHONE	Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call.
WRITE_EXTERNAL_STORAGE	Allows the app to write or delete files in the device's external storage
READ_EXTERNAL_STORAGE	Allows the app to read the contents of the device's external storage
WRITE_SMS	Allows the app to modify or delete SMSes
GET_ACCOUNTS	Allows the app to get the list of accounts used by the phone
DISABLE_KEYGUARD	Allows the app to disable the keylock and any associated password security

List Of Permissions That Escobar Malware Can Abuse

The full list of dangers of this particular malware is extensive. Not only can it do what was outlined above. It can also bypass your screen lock and even send text messages to your entire contact list. It also can record audio from the microphone, get your location, and initiate phone calls. The malware even has the capability of checking the phone's access to data, such as if you turned off mobile data and turn it back on again.

The absolute biggest threat though is that it can even read from the official Google Authenticator app, without user interaction, by directly interfacing with it to capture any codes that might be used during a login process.

How can you protect yourself from such a nasty piece of work? Well, so far the malware does not look to have been included in any official distribution via the Play Store. So don't do any side-loading of APKs that you don't trust, or don't side-load at all. Watch your mobile and Wi-Fi data on your device and if there are any apps you don't recognize using extra data, look into them.

If you have any legitimate malware detecting apps, pay attention to their notices. If you believe you've been infected, unfortunately, the best way to eradicate is a factory reset. So, run a backup of anything you deem important on your device (be careful not to include the

malware of course) and run your factory reset. The researchers even recommend removing your SIM card because of the data interaction and capabilities of this app to re-activate your mobile data connection without user interaction.

Technical Analysis

APK Metadata Information

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

Figure 2 shows the metadata information of an application.

Figure 2 – App Metadata Information

If you find fraudulent behavior on your banking or financial accounts you should immediately contact the associated institution. You should also change your passwords on anything associated. Additionally, while it is a best practice to not share passwords across accounts, we know full well that people will do this anyway. If any passwords are shared with the associated account it is best to change passwords on all of them.

Tags: Android, Malware, security, trojan