

Android malware Escobar steals your Google Authenticator MFA codes

By Bill Toulas

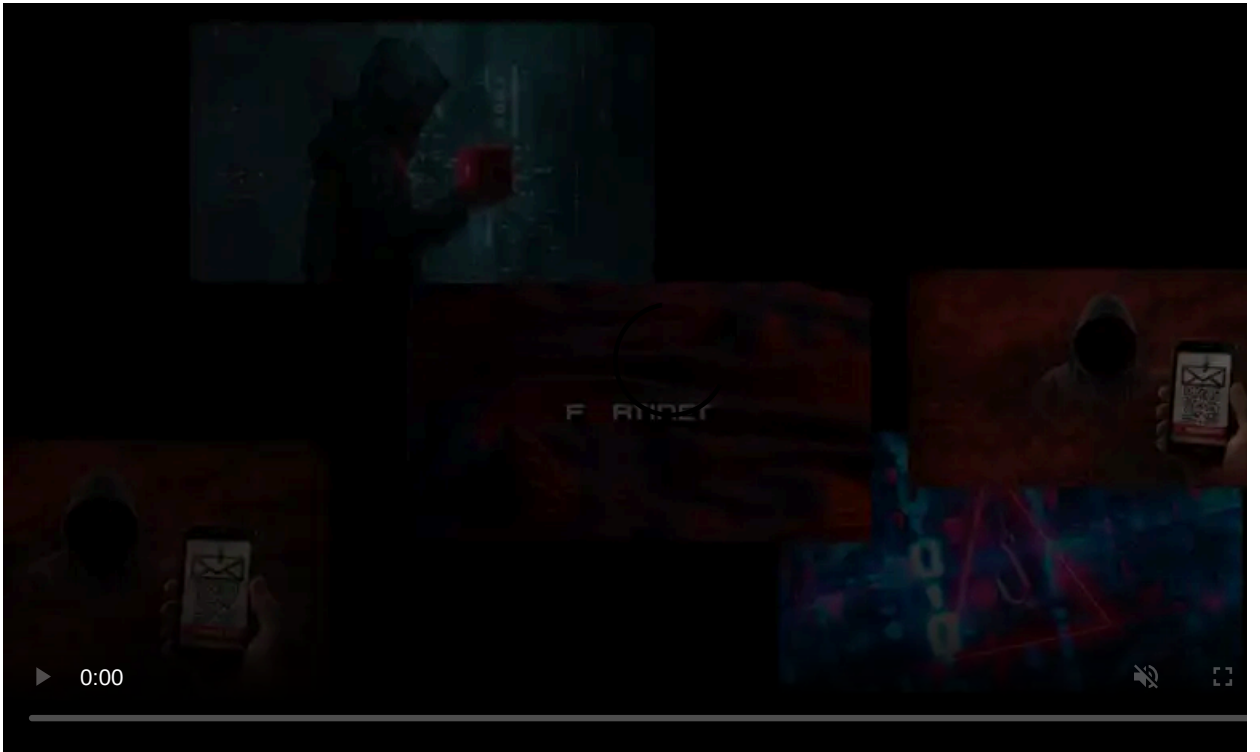
Published: 2022-03-12 · Archived: 2026-04-05 21:32:20 UTC



The Aberebot Android banking trojan has returned under the name 'Escobar' with new features, including stealing Google Authenticator multi-factor authentication codes.

The new features in the latest Aberebot version also include taking control of the infected Android devices using VNC, recording audio, and taking photos, while also expanding the set of targeted apps for credential theft.

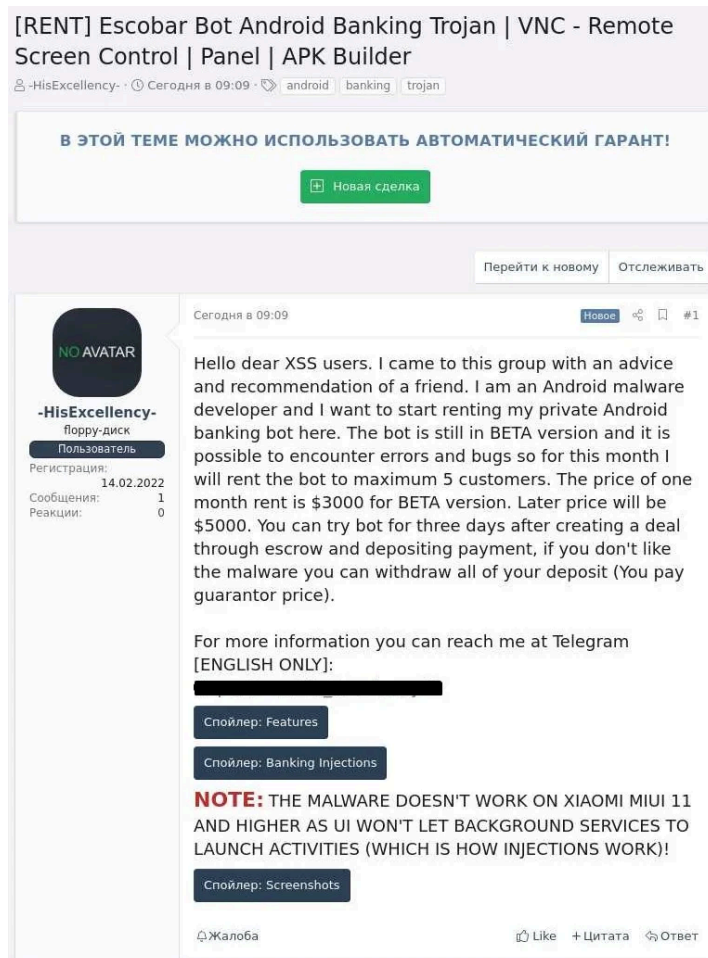
The main goal of the trojan is to steal enough information to allow the threat actors to take over victims' bank accounts, siphon available balances, and perform unauthorized transactions.



Visit Advertiser website [GO TO PAGE](#)

Rebranded as Escobar

Using [KELA](#)'s cyber-intelligence DARKBEAST platform, BleepingComputer found a forum post on a Russian-speaking hacking forum from February 2022 where the Aberebot developer promotes their new version under the name 'Escobar Bot Android Banking Trojan.'



Seller's post on a darknet forum (KELA)

The malware author is renting the beta version of the malware for \$3,000 per month to a maximum of five customers, with threat actors having the ability to test the bot for free for three days.

The threat actor plans on raising the malware's price to \$5,000 after development is finished.

MalwareHunterTeam first spotted the suspicious APK on March 3, 2022, masqueraded as a McAfee app, and warned about its stealthiness against the vast majority of anti-virus engines.

This was picked up by [researchers at Cyble](#), who performed an analysis of the new 'Escobar' variant of the Aberebot trojan.

According to the same analysts, Aberebot first appeared in the wild in [the summer of 2021](#), so the appearance of a new version indicates active development.

Old and new capabilities

Like [most banking trojans](#), Escobar displays overlay login forms to hijack user interactions with e-banking apps and websites and steal credentials from victims.

The malware also packs several other features that make it potent against any Android version, even if the overlay injections are blocked in some manner.

The authors have expanded the set of targeted banks and financial institutions to a whopping 190 entities from 18 countries in the latest version.

The malware requests 25 permissions, of which 15 are abused for malicious purposes. Examples include accessibility, audio record, read SMS, read/ write storage, get account list, disabling the keylock, making calls, and accessing precise device location.

Everything that the malware collects is uploaded to the C2 server, including SMS call logs, key logs, notifications, and Google Authenticator codes.

```
else if (this.f501000000.contains("Get Google Authenticator Codes")) {
    Intent launchIntentForPackage = getPackageManager().getLaunchIntentForPackage("com.google.android.apps.authenticator2");
    f499000000 = true;
    flags = launchIntentForPackage.setFlags(268435456);
}
```

Code to snatch Google Authenticator codes (Cyble)

The above is enough to help the crooks overcome two-factor authentication obstacles when assuming control of e-banking accounts.

2FA codes arrive via SMS or are stored and rotated in HMAC software-based tools like Google's Authenticator. The latter is considered safer due to not being susceptible to SIM swap attacks, but it's still not protected from malware infiltrating the userspace.

Moreover, the addition of VNC Viewer, a cross-platform screen sharing utility with remote control features, gives the threat actors a new powerful weapon to do whatever they want when the device is unattended.

```
} else if (this.f501000000.contains("Start VNC")) {
    AccessibilityService.Ooo000 = true;
} else if (this.f501000000.contains("Enable Notification Access")) {
    if (!getApplicationContext().getSharedPreferences("sharedPrefs", 0).getBoolean("notification", false)) {
        SharedPreferences.Editor edit = getApplicationContext().getSharedPreferences("sharedPrefs", 0).edit();
        edit.putBoolean("uninstallProtection", false);
        edit.apply();
        flags = new Intent("android.settings.ACTION_NOTIFICATION_LISTENER_SETTINGS").setFlags(268435456);
    }
} else if (this.f501000000.contains("Stop VNC")) {
    AccessibilityService.Ooo000 = false;
} else {
    try {
        if (this.f501000000.contains("VNCClick")) {
            String str11 = this.f501000000;
            float floatValue = Float.valueOf(str11.substring(str11.indexOf('*') + 1, this.f501000000.indexOf('*'))).floatValue();
            String str12 = this.f501000000;
            AccessibilityService.Ooo0000 = Float.valueOf(str12.substring(str12.indexOf('*') + 1, this.f501000000.indexOf('*'))).floatValue();
            AccessibilityService.Ooo0000 = floatValue;
            AccessibilityService.f467000000 = "click";
            str = this.f501000000;
        } else if (this.f501000000.contains("VNCHold")) {
            String str13 = this.f501000000;
            float floatValue2 = Float.valueOf(str13.substring(str13.indexOf('*') + 1, this.f501000000.indexOf('*'))).floatValue();
            String str14 = this.f501000000;
            AccessibilityService.Ooo0000 = Float.valueOf(str14.substring(str14.indexOf('*') + 1, this.f501000000.indexOf('*'))).floatValue();
            AccessibilityService.Ooo0000 = floatValue2;
            AccessibilityService.f467000000 = "hold";
            str = this.f501000000;
        } else if (this.f501000000.contains("VNCDrag")) {

```

VNC Viewer code in Aberebot (Cyble)

Apart from the above, Aberebot can also record audio clips or take screenshots and exfiltrate both to the actor-controlled C2, with the complete list of supported commands listed below.

Command	Description
Take Photo	Capture images from the device's camera
Send SMS	Send SMS to a particular number
Send SMS to All Contacts	Send SMS to all the contact numbers saved in the device
Inject a web page	Inject a URL
Download File	Download media files from the victim device
Kill Bot	Delete itself
Uninstall an app	Uninstall an application
Record Audio	Record device audio
Get Google Authenticator Codes	Steal Google Authenticator codes
Start VNC	Control device screen

Table of commands accepted by Aberebot (Cyble)

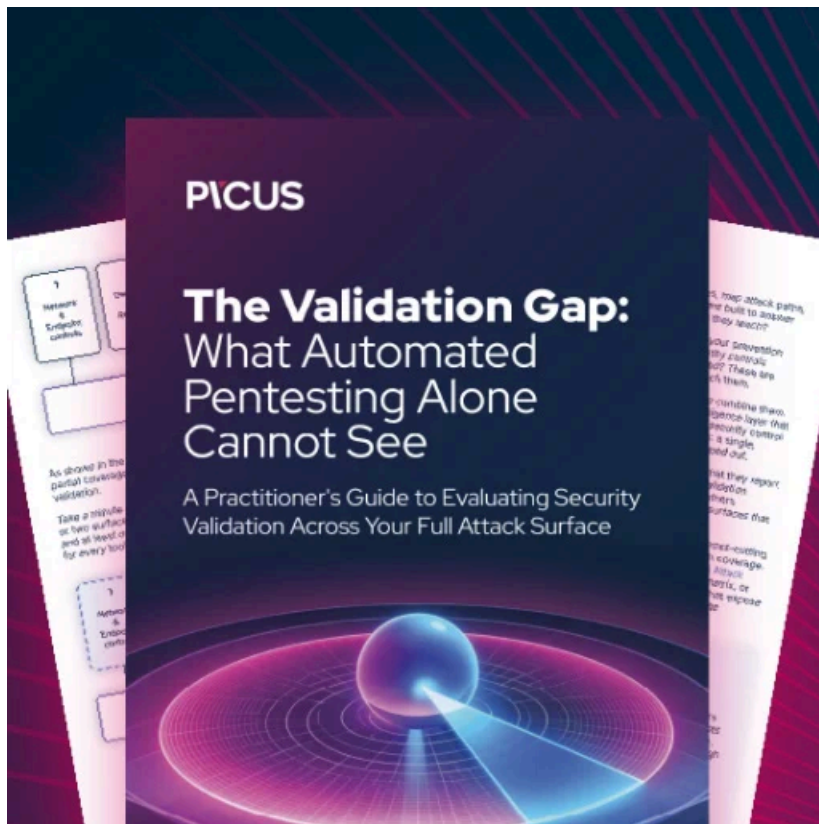
Should we be concerned?

It is still early to tell how popular the new Escobar malware will become in the cybercrime community, especially at a relatively high price. Nevertheless, it's now powerful enough to entice a wider audience.

Also, its operational model, which involves random actors that can rent it, means its distribution channels and methods may vary greatly.

In general, you can minimize the chances of being infected with Android trojans by avoiding the installation of APKs outside of Google Play, using a mobile security tool, and ensuring that Google Play Protect is enabled on your device.

Additionally, when installing a new app from any source, pay attention to unusual requests for permissions and monitor the app's battery and network consumption stats for the first few days to identify any suspicious patterns.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/android-malware-escobar-steals-your-google-authenticator-mfa-codes/>