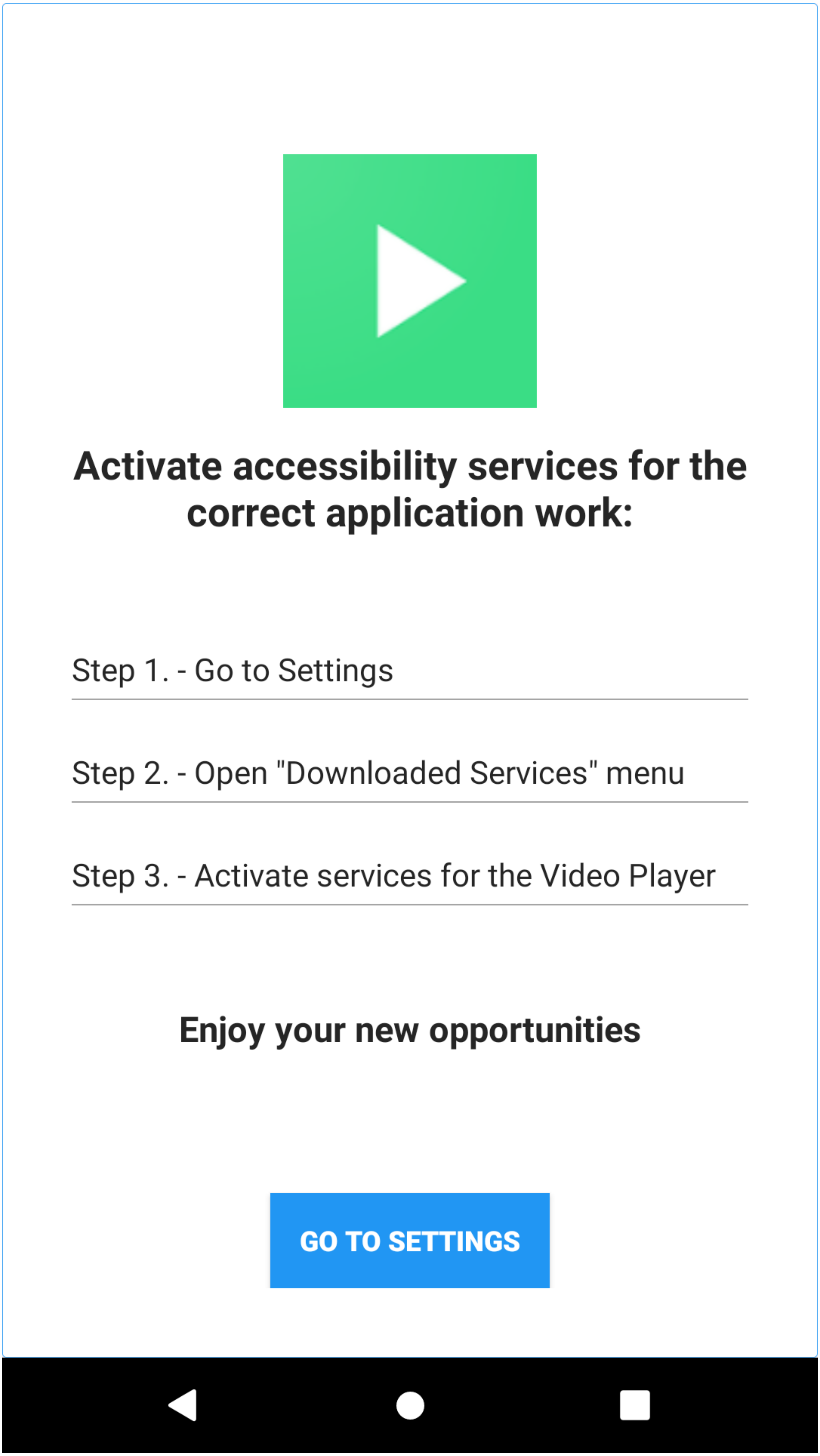
Affected Platforms: Android Impacted Users: Android End-Users Impact: Banking Credential Leak + Remote Control Severity Level: Medium

We have been closely investigating the Android BianLian botnet (also known as Hydra). This botnet emerged in 2018. It is still very alive in 2022, particularly active since the beginning of 2022, where we are closely monitoring at least three independent campaigns.

The Android malware typically poses as a video player, Google Play app, or a mobile banking application. Once installed, it asks the victim to activate Accessibility Services for the app to "work correctly." In reality, this is needed by the malware to overlay images and validate forms without user interaction. Asking for Accessibility Services activation should raise an alarm in the victim's mind. Unfortunately, many won't understand this is not legitimate.



Activate accessibility services for the correct application work:

Step 1. - Go to Settings

Step 2. - Open "Downloaded Services" menu

Step 3. - Activate services for the Video Player

Enjoy your new opportunities

Figure 1: Malware asking to activate Accessibility Services. Unfortunately, many users will accept and won't understand this helps the malware capture gestures, click on forms

without user’s consent, etc.

Once this is done. It is game over. The installed application apparently disappears from the smartphone, leaving the victim under the impression that it did not work or crashed. In reality, the malware is running in the background and contacting a C2 for apps to monitor.

Whenever the victim launches an app monitored by the threat actors, the malware downloads up-to-date HTML and images to inject on the smartphone. The injected web page is displayed as an overlay of the real app, but the victim has no way to see the trick. This is how threat actors get the mobile banking credentials of their victims. It is important to note that this malware does not affect the targeted applications or exploit them in any way. Instead, it inserts itself between the user and the application to intercept the user's credentials, much like a man-in-the-middle attack.

Video Overview: Example of infection with Android Bian Lian malware. In this video, we mimic an existing C2 taken from another campaign (left hand side). On the right, a smartphone is infected with Bian Lian. Our fake C2 shows communication with the infected smartphone. The end-user activates Accessibility Services.

Note the infected Video Player disappears from the list of applications: the end-user can’t see it any longer. Then, the end-user launches an application. See how the malware injects a fake login page. This login page actually “sits” on top of the existing bank’s app. The Bian Lian malware, running in the background, takes regular screenshots of the victim’s smartphone. This is a way the malware can steal banking credentials.

Note the mobile banking apps are genuine and have no security flaw. The attack is conducted by the Bian Lian malware. (This research video has no sound.)

During our investigations, we noticed the C2 is targeting European banks. It is also currently developing support for the Photo TAN some banks use. Photo TAN is a popular two-factor authentication method where the user scans a matrix shown on their PC, laptop, or tablet with the smartphone. This generates a TAN to verify online orders.

We have downloaded the corresponding injected pages:

Figure 2: Corresponding injected pages.

Fortunately, the web pages are not ready yet:

```
inj/com.db.pbc.phototan.db$ cat index.html This is the message! inj/com.commerzbank.photoTAN$ cat
index.html This is the message!
```

Copy

Fortinet customers are protected:

- The malware is detected as Android/BianLian.10484!tr or Android/Agent.FRJ!tr
- The malicious URLs of the C2 are blocked by our Web Filtering services
- The threat is being actively monitored by Fortinet’s Central Threat System and our FortiRecon team.
- As much as possible, we are reaching out to concerned banks and trying to bring the botnet down.

## IOC

- a3b826de0c445f0924c50939494a26b0d99ef3ccac80faacca98673625656278
- hxxp://loa5ta2rso7xahp7lubajje6txt366hr3ovjgthzmdy7gav23xdqwnid[.]onion/api/mirrors
- hxxp://zhgggga[.]in

## Targeted applications

The following applications are currently targeted by the C2. Note the list may change at any moment.

- At.aerztebank.aerztebankmobile
- At.bank99.meine.meine
- At.ing.diba.client.onlinebanking
- At.volksbank.volksbankmobile
- Com.bankaustria.android.olb
- Com.bawagpsk.bawagpsk
- Com.commerzbank.photoTAN

- Com.db.pbc.phototan.db
- Com.db.pwcc.dbmobile
- Com.easybank.easybank
- De.comdirect.app
- Mobile.santander.de.smartsign

In addition to those banking apps, the C2 also monitors a few vendor PIN applications like samsung.settings.pas or huawei.settings.pin. Those appear in all Android Bian Lian malware to help malware authors grab the PIN or unlock the screen.

Many thanks to several colleagues who are helping for this investigation, in particular: David Malcher, Aamir Lakhani, Bhumit Mali, and Anil Aphale.

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.