DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Analiza aplicației malițioase 'Voicemail.apk', propagată prin mesaje-capcană trimise de atacatori utilizatorilor din România în perioada sărbătorilor de Paște

Nume aplicație: Voicemail

Nume fișier: Voicemail.apk

SHA256: 74ae3f16ef4bbe436f9c092c13d038eaf3d3f5acf7f102b446ce0af394d95e06

SDK minim: 24

Nume pachet: com.iqiyi.i18n

C2: 108.171.202.195:443

1. Context

În perioada 22.04.2022 - 02.05.2022, utilizatori de terminale mobile din România au fost vizați de o campanie de infectare cu malware care se propaga prin intermediul unor mesaje-capcană venite pe telefon. Aceste mesaje erau special concepute de atacatori pentru a determina potențiala victimă să acceseze link-ul prezent în mesaj. Textul corespondent era unul într-o limbă română cu greșeli evidente și anunța utilizatorul că are un mesaj vocal, iar pentru a-l asculta trebuie să facă click pe acel URL.

Odată ce acel link era accesat de pe smartphone, dacă nu avea suspiciuni, utilizatorul descărca și instala în terminalul mobil o aplicație de tip APK, pentru a putea asculta mesajul. În realitate, mesajul nu exista, acesta fiind doar un pretext afișat de atacatori pentru a convinge potențiala victimă să execute acțiunea, mizându-se pe curiozitatea acestuia.

2. Analiza tehnică

Link-urile furnizate prin astfel de mesaje aveau un mecanism de User-Agent fencing, fiind accesibile doar utilizatorilor de terminale mobile de tip Android, cu o versiune Android minim 7.0, mecanism implementat pentru a îngreuna analiza.

Odată ce aplicația era descarcată și accesată de pe un smartphone cu sistemul de operare Android, aceasta solicita dreptul de a se instala ca Serviciu. Aplicațiile de tip Serviciu sunt considerate aplicații de sistem și primesc permisiuni aproape totale asupra tuturor celorlalte aplicații instalate: https://developer.android.com/guide/components/services.

După acordarea privilegiilor și drepturilor de serviciu, aplicația se șterge din lista aplicațiilor și rămâne activă în background, fiind practic imposibil de dezinstalat prin metodele clasice. Aceasta poate fi dezinstalată doar prin accesarea dispozitivului în modul **debugging**, prin utilitarul **adb**.

Din analiza aplicației, reiese faptul că aceasta este construită pe o aplicație legitimă (**IQIYI**), fiind inclusiv semnată cu semnatura digitală a acesteia.

3. Capabilități

- *Starea rețelelor* - aplicația interoghează starea tuturor rețelelor active
- *Lista de contacte* - aplicația are capacitatea de a accesa lista de contacte din telefon
- *Acces în aplicații instalate* - aplicația are acces nemijlocit în aplicațiile instalate pe terminalul mobil afectat și poate modifica, accesa, efectua capturi de ecran, etc.
- *Acces internet* - aplicația poate crea canale de comunicare prin TCP/UDP
- *Citire sms/mms* - aplicația poate citi toate mesajele de tip SMS stocate în dispozitiv

- *Starea telefonului* - aplicația poate afla numărul de telefon al dispozitivului, seria terminalului mobil, dacă un apel este în desfășurare, numărul de telefon al interlocutorului, etc.
- *Mesaje sms/mms* - aplicația poate trimite/recepționa/edita/șterge mesaje sms/mms care vor fi invizibile pentru utilizatorul legitim
- *Apeluri de voce* - aplicația poate efectua apeluri de tip voce fără știrea utilizatorilor. Această capabilitate poate fi folosită pentru interceptări ambientale
- *DGA (Domain Generation Algorithm)* - aplicația are un algoritm de generare de domenii pe următoarele TLD: .ua, .ru, .kz, .biz, .top, .pw, .shop, .net,.info, .br, .xyz si .cn
- *Conexiuni HTTP/S* - aplicația are cod care permite conexiuni bidirecționale prin HTTP/S
- *Rețea* - aplicația poate crea canale de comunicație bidirecționale, inclusiv prin deschiderea de porturi pe dispozitiv, atât TCP cât și UDP
- *Certificat root* - aplicația are capabilitatea de a-și instala propriul certificat root în telefon, permițând astfel interceptarea comunicației criptate
- *Obtinerea de informații GSM* - aplicația poate obține informații despre celula la care este conectat dispozitivul
- *Execuție de comenzi de sistem* - aplicația permite execuția de comenzi de sistem de la distanță
- *Detalii wifi* - aplicația poate afla detalii despre rețeaua wifi la care este conectat dispozitivul
- *Detalii GPS* - aplicația poate afla locația exactă folosind GPS-ul dispozitivului
- *Detalii despre SIM* - aplicația poate citi cartela SIM
- *Încărcare de cod* - aplicația are abilitatea de a încărca și executa cod extern, probabil module suplimentare sau versiuni viitoare.

4. Mod de replicare

Din analiza aplicației am identificat capabilitatea de replicare autonomă, de tip viral, fără necesitatea unei campanii de tip spear-phishing clasică. Acest lucru este realizat prin capabilitățile de a afla numărul de telefon al interlocutorului unui apel voce, accesarea agendei telefonice, accesarea listei de mesaje de tip SMS/MMS, coroborate cu capabilitatea de a trimite/recepționa/modifica/șterge mesaje de tip SMS/MMS.

În plus, în urma analizei codului aplicației, am putut estima faptul că aceasta are capabilitatea de a trimite/șterge mesaje prin intermediul platformei de socializare Facebook, ceea ce face această platformă un posibil vector de răspândire, pe langă propagarea prin SMS/MMS.

5. Recomandări

Dacă ați instalat aplicația **Voicemail.apk** din greșeală, nu este obligatoriu să reveniți la setările din fabrică ale terminalului mobil (*factory reset*), deși ar fi indicat! Dacă nu doriți să efectuați această resetare, puteți urma tutorialul următor pentru a vă conecta la dispozitiv, folosind un sistem **Linux**: https://developer.android.com/studio/command-line/adb

Odată conectat la dispozitiv, executați următoarele comenzi:

1) **Listarea dispozitivelor conectate**

dnz@info:~# adb devices -l

List of devices attached

192.168.57.113:5555 device product:vbox86p model:Samsung_Galaxy_S10 device:vbox86p transport_id:1

2) **Dezinstalarea aplicatiei com.iqiyi.i18n**

dnz@info:~# adb uninstall com.iqiyi.i18n