AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre d'Alerte et de Réponse et
Aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

Le malware ANUBIS

Contenu

I. Contexte

Une menace n'attend pas l'autre sur internet et surtout sur les téléphones intelligents, puisque pratiquement tout le monde en a un de nos jours. Il n'est donc pas surprenant d'apprendre que les pirates visent de plus en plus ces appareils et surtout les appareils Android et son système ouvert. Le logiciel malveillant **Anubis** fait trembler Google et les utilisateurs de téléphones intelligents Android. Ce malware cherche de façon sournoise à vider les comptes bancaires de ses victimes et soutirer plusieurs autres informations. Google a beau faire des efforts pour endiguer ces menaces, le problème c'est que les pirates aussi sont ingénieux et trouvent des moyens de contourner les défenses du Play Store.

II. Fonctionnement

Détecté et supprimé par Google il y a quelques mois, le logiciel malveillant Anubis semble s'être frayé de nouveau un chemin sur le Play Store et les appareils Android. Ce sont les experts en cybersécurité de chez Sophos qui ont détecté le retour d'Anubis sur le Play Store, alors que ce malware adopte la stratégie de la furtivité pour mieux frapper.

On parle donc ici de la bonne vieille stratégie du cheval de Troie qui consiste à s'incruster inaperçue sur l'appareil, d'y rester "endormi", puis de se réveiller après un certain délai pour attaquer quand notre garde est basse, Caché dans des applications en apparence inoffensive (services financiers, boutiques en ligne, ou applications automobiles), un code caché va télécharger le logiciel malveillant Anubis à notre insu. Ne contenant aucun lien malveillant, ce code caché permet ainsi de contourner les défenses de Google qui n'y voit que du feu.

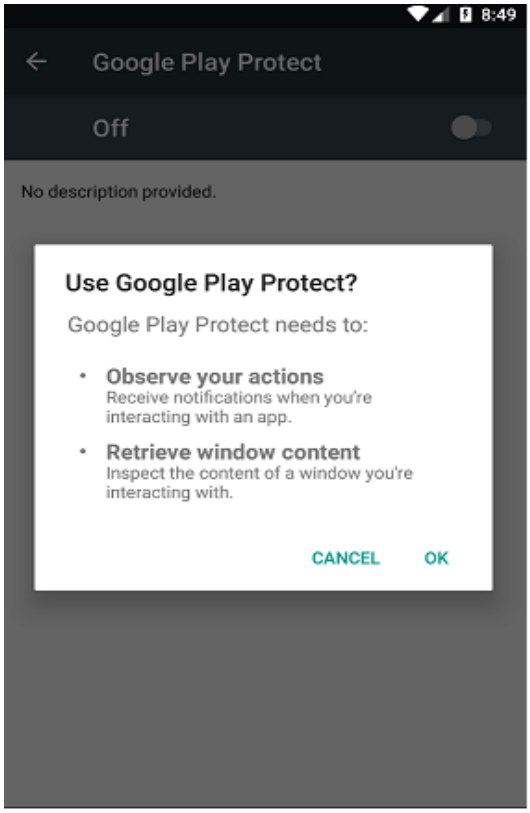
Vicieux à souhait, le logiciel malveillant Anubis cherche particulièrement à collecter nos informations bancaires et vider nos comptes, mais aussi toutes données sur notre téléphone intelligent. Une fois qu'Anubis se réveille, ce dernier nous demande d'accéder à notre caméra, notre microphone, nos messages textes, notre agenda et notre espace de stockage. En fait, il se déguise en Google alors que la notification de ses demandes est faite sous le nom de Google Play Protect. Si on fait l'erreur de lui accorder tous ces accès, Anubis se retrouve alors dans la caverne d'Alibaba. Non seulement peut-il à nous espionner, enregistrer nos mots de passe et installer des rançongiciels, mais surtout avoir accès à notre compte bancaire. Selon Sophos, Anubis cible plus de 70 applications bancaires différentes et est ainsi capable de récupérer nos données bancaires. De plus, Anubis peut également voler nos informations lorsqu'on effectue un achat sur eBay, Amazon ou avec PayPal

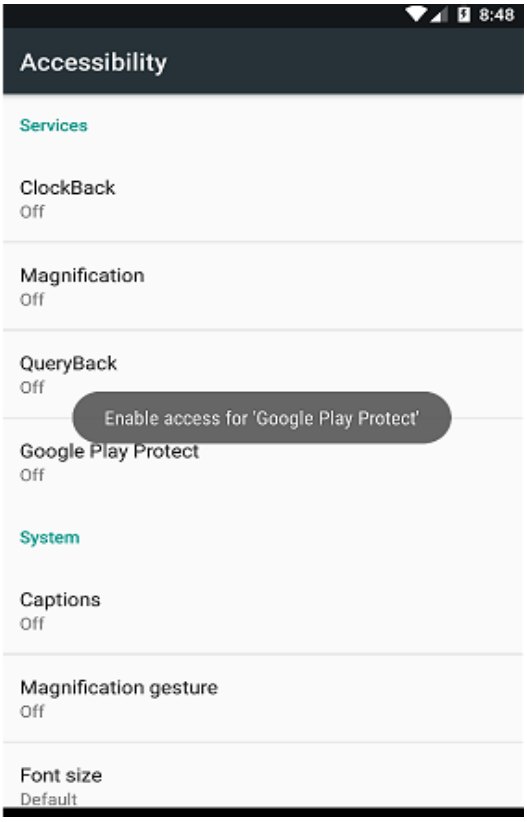
III. Comment se protéger ?

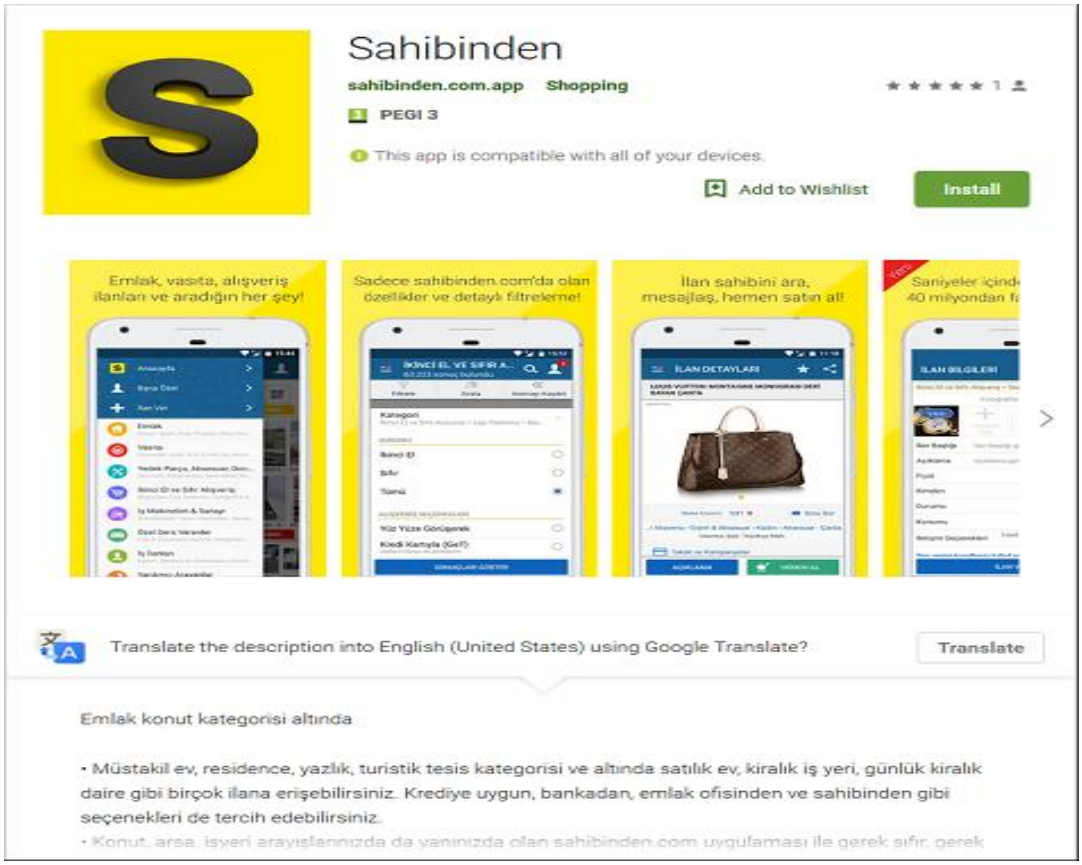
Si Google travaille activement à supprimer les applications infectées, il n'en demeure pas moins que le risque est réel.

Afin de ne pas être infecté, la solution est simple, il faut éviter de télécharger ces applications. Néanmoins, la meilleure prévention est de télécharger des applications provenant de développeurs crédibles surtout dans le domaine des applications comptables ou financières. En cas de doute, il est toujours possible d'installer un antivirus sur son téléphone ou bien utiliser une application comme Malwarebytes pour tenter de détecter et retirer le logiciel malveillant

IV. Annexe


8:49
Google Play Protect
Off
No description provided.
Use Google Play Protect?
Google Play Protect needs to:
Observe your actions
Receive notifications when you're interacting with an app.
Retrieve window content
Inspect the content of a window you're interacting with.
CANCEL
OK


8:48
Accessibility
Services
ClockBack
Off
Magnification
Off
QueryBack
Off
Enable access for 'Google Play Protect'
Google Play Protect
Off
System
Captions
Off
Magnification gesture
Off
Font size
Default


Sahibinden
sahibinden.com.app
Shopping
PEGI 3
This app is compatible with all of your devices.
Add to Wishlist
Install
Emlak, vasıta, alışveriş ilanları ve aradığın her şey!
Sadece sahibinden.com'da olan özellikler ve detaylı filtreleme!
İlan sahibini ara, mesajlaş, hemen satın al!
Translate the description into English (United States) using Google Translate?
Translate
Emlak konut kategorisi altında
• Müstakil ev, residence, yazlık, turistik tesis kategorisi ve altında satılık ev, kiralık iş yeri, günlük kiralık daire gibi birçok ilana erişebilirsiniz. Krediye uygun, bankadan, emlak ofisinden ve sahibinden gibi seçenekleri de tercih edebilirsiniz.