NOUVEL HAY MAGAZINE
SANS FRONTIÈRES

Le logiciel malveillant (malware) DroidBot utilise un « enregistreur de frappes » quand on tape sur son smartphone

DroidBot permet ainsi aux pirates de **récupérer vos mots de passe** dès que vous les entrez sur le téléphone **infecté.**

Il peut aussi intercepter les SMS, souvent utilisés par les banques pour authentifier leurs clients.

DroidBot permet aux pirates de **prendre le contrôle à distance de l'appareil** infecté .

les banques touchées :

BNP Paribas ,'**Axa Banque**, **Boursorama,** la Caisse d'Epargne, **la Banque populaire**, la Banque Postale, le Crédit **Agricole,** la **Société générale** et ING.

Des clients de banques dans d'autres pays européens, le Royaume-Uni, l'Italie, l'Espagne et le Portugal, ont également été la cible de cette attaque.

Les banques elles-mêmes n'ont pas été directement touchées, mais plutôt les téléphones de leurs clients qui ont été infectés par le malware. "***Il y a beaucoup d'autres malwares dans la nature****, et nous faisons preuve d'une lutte continue contre ce type de logiciels*".

Comment se prémunir ?

Le logiciel, qui échappe facilement à la détection des antivirus, se déclenche lorsque vous **ouvrez un fichier compromis ou après l'installation d'une application infectée** , ***certaines extensions de jeux****, d'applications piratées ou encore de* ***fausses mises à jour d'applications***", ...

sources : Le Figaro, Cleafy

"*Notre meilleur conseil*", pour éviter de faire partie des victimes de cette cyberattaque, "*reste de* ***télécharger et mettre à jour ses applications mobiles via les stores officiels***", explique BNP Paribas. En effet, il est essentiel de procéder à des téléchargements de contenu (images, vidéos, thèmes, jeux, etc.) uniquement à partir de sources de confiance, et de maintenir son appareil à jour en effectuant régulièrement les actualisations de système.