

Hackers et iPhone : une nouvelle passion délinquante?

Les garnements de l'informatique progressent dans le hack de l'iPhone. L'objectif, débloquent le nouveau terminal de la pomme, mais l'ego surdimensionné de certains freinent le « *travail collaboratif* », déplore un site pro-hacker...

Depuis le lancement en grandes pompes du combiné hybride téléphone-baladeur de la firme de Cupertino, les efforts de la communauté des hackers, sont intenses.

Le but du jeu est donc de débloquent l'iPhone qui pour l'instant ne fonctionne que sur le réseau EDGE d'AT&T et ne peut pas être utilisé sur le réseau cellulaire des autres opérateurs.

Les terminaux bloqués sont utilisés par les opérateurs pour récupérer la somme dépensée lors de la substitution d'un terminal, mais dans le cas de l'opérateur américain, l'iPhone ne peut pas être substitué, il est vendu au prix fort entre 499 et 599 dollars. Au lieu de cela, le téléphone est bien bloqué, mais uniquement parce qu'AT&T a signé un accord exclusif de distribution aux USA avec Apple.

Imaginons que l'iPhone soit débloquent. Cela poserait de lourds problèmes pour Apple et AT&T, car les utilisateurs américains pourraient alors changer d'opérateur, pire, le terminal pourrait alors être utilisé hors des Etats-Unis.

Avant d'affirmer que cela est possible, les hackers vont devoir relever de nombreux défis. Le principal frein pour l'instant, étant le processus d'authentification du terminal -qui permet d'initialiser le téléphone, sa caméra, et la lecture de musique- devant impérativement se faire sur la plate-forme de téléchargement iTunes. Mais à l'instar du [hack du WGA](#) (Windows Genuine Advantage) de l'OS de Redmond, Vista, cela est techniquement possible.

Selon les informations qui circulent sur des forums, des channels IRC et la presse, les travaux des hackers avancent bien, mais pour l'instant l'iPhone n'est pas officiellement « hackable ». Mais la nouvelle devrait tomber prochainement...

« Le processus d'activation d'iTunes peut être contourné assez facilement en utilisant la technique du spoofing. La prochaine étape est donc de comprendre comment nous pouvons débloquent la bête. Il est aussi important de ne pas provoquer le blocage de la carte SIM ce qui semble plus difficile, mais réalisable », peut-on lire.

Ces avancées permettent aux hackers de configurer et de lire les données embarquées dans l'iPhone, notamment, de déterminer si le téléphone est activé ou non. D'après la note laissée sur le forum de Dev Wiki, « *le reste c'est du Lego, nous devons comprendre les mécanismes de l'iPhone et comment certaines fonctions agissent avec l'ensemble. La prochaine étape cruciale va donc être de se balader dans les fichiers système du terminal, ce qui est d'ores et déjà possible.* »

Une fois l'écueil de l'activation réglé, les hackers vont devoir s'attaquer à d'autres problématiques. Par exemple, savoir si iTunes a la capacité de reconnaître un téléphone qui n'a pas été activé pour être utilisé sur le réseau AT&T. Et si c'est le cas, qu'elle sera la réaction de Apple?

Après ces questions, les hackers peuvent se focaliser sur le déblocage de la fonction téléphonique, une tâche qui est déjà simplifiée par le fait que l'iPhone utilise une carte SIM (Subscriber Identity Module) démontable.