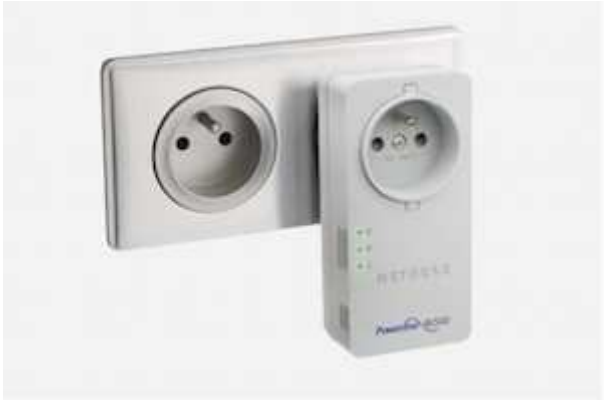
http://www.01net.com/actualites/pirater-le-cpl-de-son-voisin-c-est-simple-comme-un-coup-de-jus-633462.html

- **01net**
- Actualités
- Sécurité

Pirater le CPL de son voisin, c’est simple comme un coup de jus

22/11/2014 à 08h30 Mis à jour le 22/11/2014 à 19h52



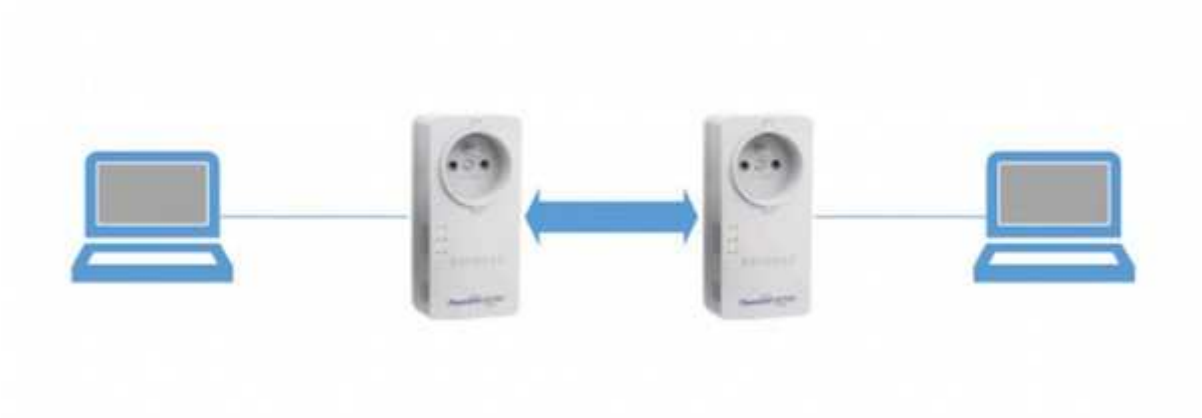
Exemple de prise CPL. - Exemple de prise CPL.

Un chercheur en sécurité a trouvé une faille pour s'introduire à distance dans un grand nombre de prises courant porteur en ligne. Permettant, par exemple, de se greffer sur l'accès Internet d'un parfait inconnu.

Si vous disposez d’une box Internet avec décodeur TV, il y a des chances que vous utilisez des prises courant porteur en ligne pour interconnecter les deux. C’est en effet la solution la plus simple et qui offre la meilleure qualité de débit. Mais saviez vous qu’en faisant cela, vous augmentez considérablement le risque de vous faire pirater votre accès Internet? Voire même de vous faire espionner? C’est en effet ce que vient de démontrer le chercheur en sécurité Sébastien Dudek, à l’occasion de la conférence NoSuchCon, qui s’est déroulée du 19 au 21 novembre au siège du parti communiste. *« J’ai récemment emménagé dans une colocation,* explique le jeune ingénieur diplômé en 2012. *Mais le wifi était de mauvaise qualité, j’ai donc acheté des prises CPL. C’est comme ça que tout a commencé. »*

Les compteurs électriques n'isolent pas le trafic

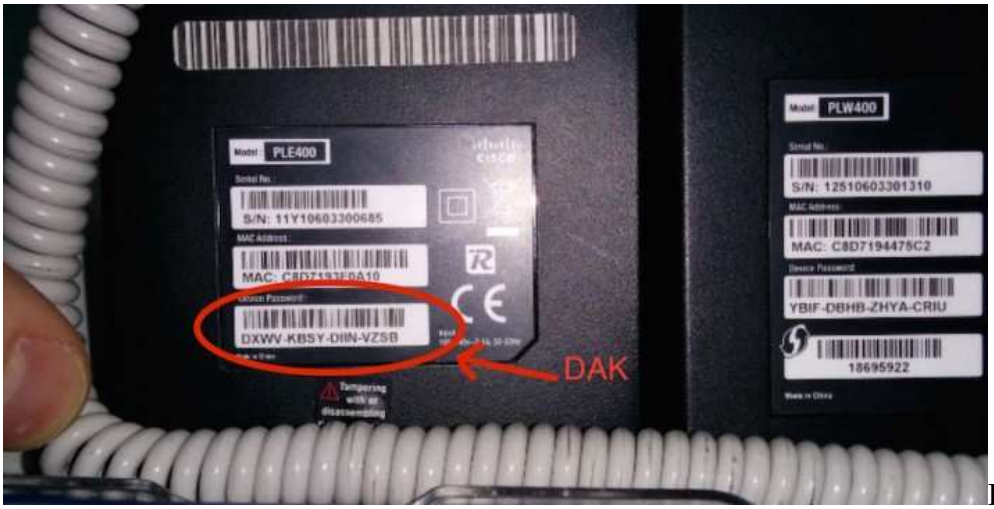
Recherche documentaire sur Internet, analyse de trafic protocolaire, reverse engineering… le hacker décortique méthodiquement ses adaptateurs et, finalement, découvre un moyen pour s'introduire à distance dans un grand nombre de réseaux CPL. Sa méthode repose tout d'abord sur une faille dans le réseau électrique lui même. *« Contrairement à ce que l'on pourrait penser, les signaux CPL ne sont pas arrêtés par les compteurs électriques. Seuls les plus récents sont capables de les filtrer. Quand les compteurs sont plus anciens, on arrive à capter les signaux d'appartements voisins, voire même au niveau de tout un immeuble »*, explique M. Dudek.



Entre deux prises CPL, le trafic circule par le courant électrique de manière chiffré. - Entre deux prises CPL, le trafic circule par le courant électrique de manière chiffré.

Mais capter les signaux ne suffit pas pour s'introduire dans un flux CPL, car ce dernier est plutôt bien chiffré (AES 128 bits pour les plus récents). Certes, certains utilisateurs négligents oublie d'activer l'appairage de sécurité qui, par une simple pression de bouton, permet de générer une nouvelle clé de chiffrement. Dans ce cas, le mot de passe du réseau est celui défini par défaut. Et souvent, il s'agit de « HomePlug » ou « HomePlugAV ». *« L'accès au réseau est alors immédiat. La prise CPL pirate s'associe automatiquement aux autres. Et l'on peut surfer gratuitement sur Internet »*, explique le chercheur.

Mais comment faire lorsque une nouvelle clé a bien été définie? En menant plus loin ses recherches, M. Dudek découvre que chaque prise CPL dispose d'un mot de passe unique baptisé « Direct Access Key », qui est d'ailleurs affiché sur le boitier (voir image ci-dessous). Et celui-ci, oh surprise, permet de changer le clé de chiffrement entre les prises CPL, à condition d'envoyer la bonne requête à travers le réseau électrique (SetEncryptionKeyRequest). La principale difficulté reste donc à trouver ces fameux DAK (autrement que de s'introduire par effraction dans un appartement, évidemment).



Des codes intéressants se trouvent sur les prises... - Des codes intéressants se trouvent sur les prises...

Mais là encore, le chercheur fait une belle découverte. Pour les prises CPL basés sur le chipset Qualcomm Atheros - qui est l'un des plus diffusés - il se trouve que le DAK est… un dérivé de l'adresse MAC de l'adaptateur. Et ce n'est pas tout: l'algorithme de dérivation est librement accessible. Voilà qui est bien pratique, car il existe par ailleurs une requête spéciale dans le standard HomePlug AV (« Sniff ») qui permet de récupérer automatiquement l'adresse MAC d'une prise CPL branchée sur un routeur-modem. Et le tour est joué.

En résumé, n'importe qui dans un immeuble peut se brancher sur l'Internet de son voisin, à condition que celui-ci dispose d'un CPL basé sur Qualcomm Atheros et que les compteurs électriques ne soient pas trop récents. *« La faute revient aux fabricants qui utilisent tous le même algorithme de dérivation, car il leur est fourni par Qualcomm. Ils devraient utiliser leur propre algorithme »*, souligne l'ingénieur. La bonne nouvelle dans cette affaire est pour les Freenautes: ils peuvent dormir tranquille, car les prises CPL fournis par Free reposent sur un autre chipset.

Source:

La présentation de Sébastien Dudek

Par Gilbert Kallenborn