

Un risque pour les « box » des fournisseurs d'accès

Le « drive-by pharming » est un nouveau risque d'attaque qui menace les routeurs ADSL des particuliers et les boîtiers des fournisseurs d'accès.

Deux scientifiques de l'Indiana University School of Informatics et un expert de Symantec ont démontré, fin 2006, que les failles de sécurité des boîtiers d'accès à Internet pouvaient être utilisées par des pirates. Cette exploitation

permettrait de lancer des attaques du type « drive-by pharming », une version sophistiquée du phishing. Elle consiste à détourner les connexions d'un routeur personnel (ADSL ou Wi-Fi) vers des faux sites afin de récupérer des données confidentielles à l'insu de l'internaute. Pour démontrer son efficacité, les chercheurs ont créé une page Web fictive incluant un code JavaScript malveillant. Il suffit de visualiser cette page pour

que l'attaque se mette en place.

Aucun cas de « drive-by pharming » n'a encore été signalé. Mais cette nouvelle arnaque devrait se répandre prochainement. « Elle est simple à effectuer et, en plus, il existe des outils permettant de l'automatiser. Mais elle ne fonctionne que sur les routeurs dont les mots de passe par défaut n'ont pas été changés », précise Hervé Schauer, expert en sécurité informatique. Or, selon Symantec, la

moitié des utilisateurs ne les auraient pas modifiés. De quoi imaginer différents scénarios d'attaque. « *Le plus simple est la modification de la configuration de l'appareil en désactivant le firewall intégré. Autre scénario : l'installation d'un plug-in malveillant sur le boîtier pour servir ensuite de relais de spam ou pour capturer des mots de passe* », explique Nicolas Ruff.

PH. R.