Prendre le contrôle des feux de signalisation en ville : un jeu d'enfant pour les hackers

Des chercheurs américains de l'Université du Michigan ont réussi à pirater sans problème le système des feux de signalisation des grandes villes de leur État, dévoilant des failles de sécurité informatiques inquiétantes et potentiellement dangereuses.

Avec Hervé Schauer

Atlantico : Des chercheurs américains de l'Université du Michigan ont réussi facilement à pirater le système des feux de signalisation des grandes villes de leur Etat, dévoilant des failles de sécurité informatiques inquiétantes et potentiellement dangereuses. Comment l'expliquez-vous ?

Hervé Schauer : Dans le cas présent, il ne s'agit pas à proprement parler d'un piratage mais d'un test de sécurité qui a révélé un système ouvert et non sécurisé. La responsabilité en revient d'abord au concepteur et à l'opérateur, qui pour des raisons d'économies, ont mis en place et géré un système sans protection des réseaux et des serveurs. I**l n'est pas normal qu'ils aient conçu des feux qui dialoguent sans authentification mutuelle et sans chiffrement.** Or, dans tout système normalement sécurisé, il n'y a pas de failles. Sauf que les pouvoirs publics partent du principe naïf que les gens sont honnêtes et que personne n'ira s'amuser à le falsifier ou à l'utiliser de façon malveillante, au lieu d'exiger des clauses de sécurité dans tous leurs appels d'offre. Les techniques utilisées sont d'ailleurs assez simples. Même un adolescent un peu curieux peut les pirater avec un simple ordinateur portable. D'autant que de nombreux systèmes industriels sont extraordinairement vulnérables, parce qu'ils ont été élaborés à partir de technologies anciennes et n'étaient pas conçus pour être interconnectés.

Le piratage des systèmes routiers de signalisation est-il un phénomène nouveau et courant ?

Ces attaques, qui ne sont pas nouvelles, n'en sont pas moins peu fréquentes. La raison en est simple : il n'y a pas d'argent à gagner. L'intérêt financier d'une attaque contre les systèmes de gestion des routes, des autoroutes, des feux de signalisation et des panneaux est trop faible pour motiver des piratages, souvent risqués. Or, le principal moteur de tout malfaiteur est d'abord pécunier. On peut toujours penser que des criminels qui voudraient protéger leur fuite, perturbent les feux de circulation afin de créer des embouteillages et une voie de feux verts pour s'échapper de la banque qu'ils viennent d'attaquer. Mais à ma connaissance, ce genre de piratage n'a pas encore eu lieu, au moins en France. **Les délinquants préfèrent pirater les guichets automatiques bancaires**. Même les terroristes n'y ont aucun intérêt. On ne créé pas de la terreur avec des attaques informatiques. Un piratage des feux, s'il peut s'envisager dans le cadre d'une attaque terroriste globale, ne se justifie pas à lui seul.

Peut-on alors imaginer une paralysie des feux de circulation d'une grande ville occidentale par des pirates russes ou chinois dans le cadre d'une cyberguerre politique ou idéologique ?

Pour être franc, il est surprenant que cela ne soit pas déjà arrivé. Je prends d'ailleurs les paris que dans un an, les autorités du Michigan installeront de nouveaux systèmes, qui ne seront toujours pas mis à jour et sécurisés. En tout cas, il est certain que le piratage informatique possède un usage guerrier. Quand les Russes ont envahi une partie de la Géorgie, en 2008, ils ont ainsi lancé de manière concomitante des attaques informatiques sérieuses. **Lors de la Guerre du Golfe, en 1991, les Français, qui avaient construit les systèmes téléphoniques en Irak, les avaient aussi manipulés pour aider leurs alliés américains**. Mais pour pouvoir utiliser des feux de signalisation dans un contexte guerrier, encore faudrait-il que les pirates soient sur place, car les attaques à distance sont beaucoup plus difficiles et compliquées.

Les autorités françaises ont-elles pris la mesure du danger de ces attaques ?

Des cadres de l'Agence nationale de la sécurité des systèmes d'informations (ANSSI), qui dépend du gouvernement, sont en effet conscients de la menace. Mais sont-ils majoritaires ? Les hauts responsables au niveau gouvernemental ont-ils, eux-mêmes, compris les enjeux ? Difficile de savoir. En tout cas, l'ANSSI agit. D'ailleurs, la France fait partie de ces quelques pays, qui possèdent une agence dédiée. Pour les hommes politiques, ce type de piratage est très complexe à apprécier, car il ne se voit pas, ne se sent pas et n'est pas très vendeur.

Quelles sont les solutions pour y remédier et s'en protéger ?

On se protège d'abord en amont avec une bonne organisation,**puis en intégrant systématiquement la sécurité dans l'ensemble des projets**. Il faut désormais considérer que dans nos sociétés modernes hyperconnectées, la sécurité n'est plus un luxe. Et c'est ce que la législation actuelle essaie de faire. Aujourd'hui, il est impossible de détenir des données nominatives accessibles sans aucune sécurité. La CNIL a d'ailleurs prononcé des amendes en l'absence de protection des données personnelles. En ce moment, les décrets d'application de la loi de programmation militaire, qui sont en préparation, vont proposer la même chose sur tous les systèmes industriels, y compris ceux qui pilotent les feux de signalisation.