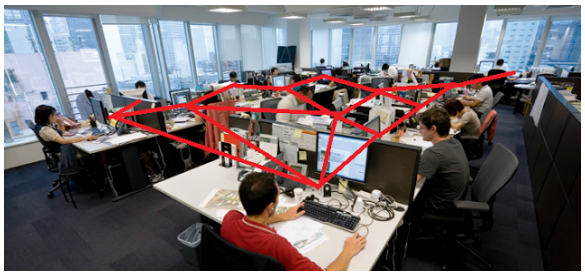
A quand le premier virus informatique acoustique ? ~ Sweet Random Science

	A quand le premier virus informatique acoustique ?

Je sais qu'ils sont payés pour cela, mais quand même : où diable vont-ils pêcher toutes ces idées ? Après la démonstration du Stanford Security Laboratory sur la façon dont les capteurs peuvent servir à espionner, voire détourner nos téléphones portables, des experts en informatique de l'institut Fraunhofer FKIE ont mis au point un protocole de transmission acoustique : des ordinateurs, pourvus qu'ils soient assez proches les uns des autres, peuvent communiquer via leurs haut-parleurs et microphones, à des fréquences inaudibles pour l'Homme, sans que cette activité ne soit détectée par les moyens de protection classiques.

Une idée qui semble relever de la science-fiction, même si la possibilité de la transmission acoustique avait déjà été proposée pour expliquer la mystérieuse persistance du malware polémique BadBIOS.

Dans leur article, publié le mois dernier dans Journal of Communications, Michael Hanspach et Michael Goetz exposent la méthode qui leur a permis de réaliser cette prouesse : en adaptant un système qui avait été imaginé pour établir des communications sous l'eau, ils sont parvenus à transmettre des informations sur des distances d'une vingtaine de mètres. Les signaux sont modulés en ondes sonores à une fréquence proche de celles des ultrasons, et sont donc inaudibles pour l'oreille humaine. Les chercheurs démontrent que cette méthode peut être utilisée pour établir un véritable réseau par lequel peuvent transiter des informations comme des mots de passe ou des identifiants de connexions, notamment lorsqu'ils sont saisis sur le clavier.

La vitesse de transmission, de l'ordre de 20 bits par seconde, ne permet évidemment pas de transmettre directement un document mais elle pourrait être suffisante pour placer une commande simple : désactiver une protection et envoyer un document par mail par exemple. De quoi rendre complètement inutiles les mesures de précaution d'isolement physique de certains site sensibles, comme les bases miliaires, les centres de services secrets ou les centrales nucléaires.

Dans une des expériences, Hanspach et Goetz établissent un réseau dans les propres locaux du Fraunhofer Institute for Communication, Information Processing and Ergonomics. Un espace de travail ouvert peut donc devenir un réseau d'échange à l'insu des utilisateurs et des logiciels anti-virus. Ce réseau serait accessible via n'importe quel terminal en mesure d'émettre et de capter des sons : un téléphone portable par exemple.

Utilisé de façon malveillante, ce système permettrait d'infiltrer un réseau, récupérer des mots de passe et les transmettre à des tiers, sans provoquer la moindre réaction des dispositifs de protection. Les anti-virus se concentrent en effet sur les modes de communication plus classiques et seraient totalement impuissants face à une attaque de ce genre.

Une faille qui sera sans doute corrigée rapidement, avec l'ajout d'un système anti-intrusion basé sur l'analyse des signaux audio émis et reçus. En attendant, on peut tout simplement désactiver les composants audio ou brider les haut-parleurs en supprimant la transmission des hautes fréquences.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://sweetrandomscience.blogspot.fr/2013/12/a-quand-le-premier-virus-informatique.html