LOGIQUE & CALCUL

Big Brother à nos portes (dérobées)

Parfois totalement indétectables, les portes dérobées informatiques nuisent gravement à la sécurité. Introduites à des fins d'espionnage ou de malveillance, ces « backdoors » exposent aussi chacun de nous au risque d'intrusion dans sa vie privée.

Jean-Paul DELAHAYE

Je ne veux pas vivre dans un monde où tout ce que je dis, tout ce que je fais, chaque personne à qui je parle, chaque expression de créativité, d'amour ou d'amitié, est enregistré.
Edward Snowden

En informatique et particulièrement dans tout ce qui est lié à la sécurité des systèmes, le terme de *backdoor* (signifiant « porte dérobée » ou « entrée cachée ») désigne un point d'accès secret. Celui-ci, ménagé dans un dispositif informatique, un programme, une machine, un réseau, permet d'en prendre le contrôle, d'en fausser l'usage ou au moins d'être informé de ce qui s'y passe, à l'insu de ceux qui s'en servent.

En cryptographie, ces portes dérobées donnent le pouvoir à celui qui en connaît l'existence de lire les messages chiffrés par un algorithme dont les utilisateurs pensent, de manière illusoire, qu'ils sont impossibles à percer. On a parfois envisagé d'installer des portes dérobées dont la présence serait connue de tous, mais dont l'accès serait réservé aux autorités.

Dans le cas d'un serveur reliant des machines ou constituant les nœuds principaux dans un réseau informatique, il s'agira de procédures permettant de contrôler les machines. Il s'agira aussi de dispositifs matériels mis en place dès la conception des machines, ou à l'insu de leurs fabricants après la sortie d'usine, et qui dupliquent toutes les informations qui y passent et en envoient la copie à un destinataire complice, sans que le vendeur du matériel ou ses acheteurs ne le sachent.

Parfois, une porte dérobée est une fonction utilisée normalement lors de la mise au point des dispositifs logiciels ou matériels qui permet de les observer afin de comprendre ce qui s'y passe et corriger des erreurs éventuelles ; mais il arrive qu'on oublie de la supprimer ou de la désactiver avant la commercialisation, donnant ainsi la possibilité aux concepteurs des programmes d'y accéder subrepticement. La plus fameuse histoire de ce type concerne le poker en ligne.

Poker en ligne frauduleux

Cette porte dérobée fit gagner des millions de dollars à une équipe de tricheurs qui ne fut jamais parfaitement identifiée. Le principe de la tricherie était élémentaire : les développeurs d'un logiciel de jeu de poker en ligne avaient prévu une combinaison de touches qui leur donnait accès aux cartes cachées des adversaires, y compris quand ils n'étaient liés au système que comme simples joueurs et non comme administrateurs. Une fois le logiciel vendu et installé sur une plateforme qui n'était pas informée du trucage, ils s'inscrivaient comme simples clients et, lorsque les enjeux leur semblaient en valoir la peine, ils activaient la fonction qui leur montrait toutes les cartes, ce qui augmentait considérablement leurs chances de gagner !

L'escroquerie a duré des années, aux dépens d'une multitude de clients américains des sites *Ultimate bet* et *Absolute Poker* qui utilisaient, sans le savoir, le programme truqué. Russ Hamilton et plusieurs de ses complices ont ainsi gagné des sommes considérables entre 2003 et 2007. Ils se présentaient sous des identités différentes pour jouer, mais des experts attentifs qui étudiaient les taux de réussite des joueurs ont observé que certains comptes réussissaient souvent des coups qu'ils n'auraient dû gagner que rarement. Nionio, le premier joueur repéré, obtenait un taux de réussite 20 fois supérieur, pour certaines positions de jeu, à celui des meilleurs joueurs de poker.

Les sites de jeux, obligés de reconnaître les anomalies et donc la tricherie, ont dû rembourser partiellement les joueurs roulés. Ce qui a d'ailleurs mis en péril leur équilibre financier. Dans cette histoire, les escrocs et leurs complices ont gardé l'essentiel des sommes acquises. Des études détaillées des parties jouées au cours de la période concernée indiquent que plus de 110 noms de joueurs fictifs avaient tiré des gains anormaux du jeu. Le montant des sommes volées grâce à la porte dérobée a été évalué à plus de 22 millions de dollars.

Lors du développement d'un logiciel, il est nécessaire de disposer de fonctions d'observation qui donnent des droits supérieurs à ceux des utilisateurs normaux. Cela facilite la maintenance, le repérage des