dysfonctionnements et leur correction. Il est tentant de laisser actives ces fonctions en conditionnant leur accès à la connaissance d'une clé ou d'une manœuvre particulière telle que l'appui simultané sur trois touches éloignées du clavier.

Le programmeur peut aussi se garder la possibilité de désactiver complètement le système informatique si celui auquel on l'a vendu ne paye pas son abonnement, ou s'il est devenu un ennemi, ou tout simplement si on veut l'inciter à acheter une nouvelle version du logiciel ou de la machine.

On peut également installer la porte dérobée après coup, sans que les développeurs en aient connaissance : la version modifiée du logiciel pourra par exemple mémoriser les codes des cartes bancaires utilisées et les envoyer à une adresse aux mains de pirates. La porte dérobée pourrait aussi donner le contrôle complet de l'ordinateur et, par exemple, en faire un esclave pour envoyer massivement des messages publicitaires. La prise de contrôle d'un ordinateur permet aussi de l'enrôler dans ce qu'on nomme des botnets (des armées d'ordinateurs sous contrôle), puis de les faire participer, à l'insu bien sûr de leurs propriétaires, à l'attaque massive d'un site internet, attaque qui rendrait celui-ci momentanément inopérant (attaque par déni de service).

Le réseau mis en danger

Parmi les affaires récentes les plus graves de porte dérobée, il y a celle concernant les équipements réseau commercialisés par la firme américaine F5-Network, un concurrent de Cisco qui emploie plus de 4 000 salariés et dont le chiffre d'affaires avoisine 2 milliards de dollars.

Le Français Florent Daignière découvrit le 12 février 2012 une grave faille de sécurité concernant une partie importante des machines vendues par F5-Network. Après en avoir averti les responsables de la firme, la faille fut rendue publique en juin 2012 : une porte dérobée donnait accès aux niveaux de contrôle les plus élevés des machines. En langage technique, elle permettait de devenir administrateur de la machine, laquelle aurait pu mener une attaque sur tout le réseau auquel elle participait. On corrigea la faille,

Portes dérobées et tricheries au jeu

Les portes dérobées autorisent celui qui les a placées à opérer des actions dont les utilisateurs n'ont pas connaissance : lecture d'informations privées, copie et envoi de données à des tiers, prise de contrôle partiel ou complet du système informatique, voire destruction de ce dernier.

© De Pra/Shutterstock.com

La plus célèbre affaire de tricherie au poker en ligne, qui a rapporté au moins 20 millions de dollars à ses protagonistes, était fondée sur une porte dérobée présente à l'insu des sites qui proposaient innocemment des jeux de Poker en ligne. La porte dérobée avait été installée par certains des ingénieurs qui avaient développé le programme : elle leur permettait de connaître les cartes cachées des autres joueurs.

Les portes dérobées sont susceptibles de concerner tous les types de systèmes ou de machines électroniques et obligent les autorités de surveillance des jeux de casino à Las Vegas à des mesures particulières, telles que le contrôle par un second technicien de toute modification opérée par un premier technicien. Ce soin méticuleux a été mis en place à la suite d'une affaire de porte dérobée installée dans les circuits des bandits manchots de casinos du Nevada.

Ron Harris, qui était technicien dans une entreprise de machines de casino, avait échangé les circuits de plusieurs machines (des EPROM) par des circuits qu'il avait programmés lui-même, pour qu'elles fassent gagner tout joueur effectuant une certaine séquence de jeu du type : insérer 3 pièces, puis 2 pièces, puis 2, puis 1, puis 3, puis 5. Il n'allait pas jouer lui-même ces séquences, car cela aurait été suspect, mais il faisait jouer des complices. Il fut arrêté non pas à cause des 24 jackpots qu'il gagna grâce à ces bandits manchots truqués, mais à cause d'une autre manipulation qui avait permis à l'un de ses complices de gagner au *Keno* un lot de 100 000 dollars qui attira l'attention des autorités et les conduisit à lui.

Il fut condamné à sept ans de prison (voir http://www.americancasinoguide.com/slot-machines/the-worlds-greatest-slot-cheat.html).