Le BIOS peut cacher des ‘rootkits’

John Heasman, consultant de la firme britannique

Next-Generation Security Software (NGS), a révélé lors des conférences Black Hat que la menace des rotkits ? des programmes intrusifs non détectés par les systèmes de sécurité et d’antivirus – pourrait bien se cacher dans la mémoire flash du BIOS. Pour cela, les attaquants utiliseraient une collection d’outils de contrôle et de gestion de l’alimentation, la *Advanced Configuration and Power Interface* (ACPI), et son langage de programmation pour glisser des modules d’un rootkit dans la mémoire flash du BIOS. Les hackers pourraient remplacer des fonctions légitimes du langage ACPI par leurs propres fonctions, malicieuses comme il se doit ! La menace est très sérieuse, même si la programmation du BIOS n’est pas à la portée de tout le monde. Le BIOS s’exécute à chaque fois que la machine est démarrée. Si des fonctions y sont cachées, elles peuvent s’exécuter avant même que les protections ne soient engagées sur le poste. Et comme elles ne figurent pas sur le disque, elles ne sont pas détectables ! Et même si elles l’étaient, ultérieurement et avec des produits adaptés, elles échapperaient aux opérations classiques destinées à remettre un système à zéro, à savoir le formatage d’un disque et la réinstallation du système d’exploitation. Le seul moyen actuellement de se protéger contre cette menace serait d’interdire de reflasher la mémoire du BIOS. Ou d’utiliser des ordinateurs qui n’utilisent que des BIOS signés, comme c’est le cas chez Intel avec SecureFlash ou chez Phoenix Technologies avec TrustedCore.