

F-Secure répond à la menace des rootkits

F-Secure annoncera et démontrera lors du Cebit d'Hannovre la première version de BlackLight Rootkit Elimination, une nouvelle technologie de lutte contre les virus Stealth, les spywares et les rootkits.

Les rootkits représentent une nouvelle forme de code malicieux, au noyau invisible, qui s'attaque aux systèmes d'exploitation incapables de les détecter (*lire notre article*), tout comme les utilisateurs et les administrateurs. « *De puissants rootkits Windows ont le potentiel pour devenir des problèmes majeurs à l'avenir* », a indiqué Mikko Hypponen, Chief Research Officer de F-Secure. « *Les programmes de rootkits ont accès à tout ce qui se trouve sur le système et peuvent silencieusement faire absolument tout ce qu'ils souhaitent sur l'ordinateur. Ces programmes d'attaque pénètrent les ordinateurs personnels et les réseaux via des virus ou des vulnérabilités* ». L'un des plus grands dangers des rootkits, après installation, provient de l'incapacité des produits de sécurité conventionnels, y compris les anti-virus et les antispywares, à les détecter et donc à les éliminer. Les éditeurs de solutions de sécurité devraient rapidement suivre l'exemple de F-Secure, qui est le premier à annoncer de nouvelles techniques de détection et d'élimination des rootkits noyau (ou *kernel rootkits*). Il sera donc intéressant de découvrir la technologie F-Secure BlackLight Rootkit Elimination, prochainement disponible en version bêta. « *Etant donné que les antivirus et produits antispyware ne sont pas capables de détecter et de stopper la nouvelle vague de virus Stealth et de spywares, nous sommes persuadés que les administrateurs et les spécialistes IT apprécieront ce nouveau niveau de sécurité* ».