

Le vol du code source de Cisco à l'origine de multiples attaques

L'affaire avait à l'époque fait grand bruit. En mai 2004, 800 Mo du système d'exploitation Cisco IOS (*Internetworking operating system*), versions 12.3 et 12.3t, avaient été illégalement copiés et publiés sur un site Web où tout un chacun aurait pu le télécharger pendant quelques jours. A l'époque, l'équipementier tentait de minimiser ce vol. « *Cisco pense que la publication inadéquate de cette information n'accroît pas les risques pour les clients de ses équipements* », expliquait le groupe américain dans une lettre à ses clients et à ses partenaires. Les analystes estimaient également que les risques de dégâts pouvant être causés par des pirates sur des réseaux utilisant le système d'exploitation seraient limités car il existe des centaines de versions de ce système. Par ailleurs, une arrestation avait été confirmée par les services de police à Londres en septembre dernier. Mais cette arrestation n'a pas empêché l'exploitation de ce code. A grande échelle, semble-t-il. Selon le *New York Times*, après un an d'enquête de la part des autorités américaines, il apparaît que le vol à été à l'origine de nombreuses intrusions dans certains autres systèmes informatiques comme celui de la NASA, de plusieurs organismes militaires américains et de laboratoires de recherche. **Un seul 'hacker', âgé de 16 ans?** Toutes ces attaques auraient pour origine une seule et même personne. Il s'agirait d'un étudiant suédois de 16 ans, déjà soupçonné de s'être frauduleusement introduit sur le réseau de son université. D'ailleurs, le jeune 'hacker' ne chercherait pas à cacher ses forfaits. Dans un mail à l'une de ses victimes, une chercheuse de l'université de Berkeley, il écrit: « *Patuxent River (une base militaire US) a complètement fermé son réseau, ils ont été morts de trouille lorsque je leur ai dit que j'avais volé les plans du F-18* ».