Admin : la cible préférée des hackers

Le rapport M-Trends de FireEye, publié fin février, confirme l'intérêt que les hackers portent aux administrateurs systèmes et aux équipes de la sécurité des SI. Comme l'explique le Pdg de FireEye, David de Walt, de passage à Paris cette semaine, plus de 9 attaques sur 10 recensées par sa société démarrent par un ciblage d'individus via des méthodes de spear phishing (ou harponnage). Un cocktail mélangeant **ingénierie sociale et liens ou pièces jointes infectieuses**. Or, pour convaincre leurs cibles de tomber dans ce piège, les assaillants détournent de plus en plus les identités des responsables de la DSI. En 2014, dans 78 % des cas, les techniques de phishing exploitaient les identités des informaticiens ou celles d'éditeurs d'antivirus. Un bond spectaculaire en un an, selon l'étude de FireEye : en 2013, cette proportion n'était que de 44 %.

Par ailleurs, les informaticiens, et particulièrement les administrateurs, sont eux-mêmes la cible des techniques de ciblage des hackers. « *Le phishing est souvent associé à des keyloggers (malwares enregistrant les frappes clavier) afin de récupérer des login et mots de passe* », relève David de Walt. Logique donc de se focaliser sur les personnels de l'entreprise disposant des droits d'accès les plus étendus : les administrateurs système. « *Qui plus est, ces personnes ont l'habitude de travailler depuis leur domicile, d'où elles bénéficient d'accès aux systèmes. Dans ce contexte, repérer les comportements anormaux devient très difficile* », reprend David de Walt.

Cette focalisation des assaillants sur les employés de la production IT n'est pas réellement une surprise. Les documents Snowden avaient déjà montré que, pour ses intrusions, la NSA cible particulièrement cette population, notamment en raison des privilèges qu'elle détient sur les systèmes.

A lire aussi :

La NSA mène la chasse aux administrateurs systèmes
Administrateurs des SI : pourquoi une charte spécifique s'impose (tribune)

Crédit photo :