

Spyware : l'espion sans visage

Reprécisons, d'abord, ce qu'est un spyware. Cette famille de logiciels espionneurs, très particuliers, mérite bien son nom, puisqu'ils espionnent effectivement l'ordinateur qu'ils infectent en collectant à l'insu de son propriétaire certains des flux utilisés notamment lors des connexions à Internet. Si cette surveillance cachée est souvent utilisée à des fins commerciales (alors que le procédé est pour le moins douteux), elle peut aussi être employée à des fins nettement moins louables, puisque ce genre de programme permet également l'enregistrement des frappes clavier effectuées par l'utilisateur et donc la détection de ses mots de passe, numéros de cartes de crédit, etc. L'étude « Laptop Liabilities » a ainsi permis de démontrer qu'à peine 7% des répondants étaient à même de définir précisément ce que faisait un 'spyware'. Honte à nous Français: ce chiffre tombe à 2% chez les utilisateurs de l'Hexagone. Tout le problème vient de ce que les gens téléchargent des 'plug-ins', programmes, 'applets', 'cookies', etc. sans se donner la peine de jeter un coup d'œil sur les conditions d'utilisation ou d'intrusion de ces produits proposés ou mis à leur disposition. Ils sont en effet près des deux tiers à n'avoir aucune idée des risques qu'ils encourent, en cas de téléchargement de logiciels espions. Or, 86% des utilisateurs avouent télécharger « occasionnellement » (le mot est coquet) des programmes sur leur ordinateur portable. A contrario, ceci démontre que les politiques restrictives de téléchargement dans le cadre de l'entreprise ne sont respectées que dans 14 % des cas. Mais il ne faudrait surtout pas croire que le spyware résulte uniquement d'un acte « volontaire ». La visite de sites pas propres (piratage, pornographie, peer-to-peer) est aussi un facteur infectieux indéniable que négligent pourtant 42% des personnes interrogées qui avouent sans vergogne s'y promener (occasionnellement, bien entendu). Quant au degré d'inconscience sur les conséquences de telles actions vis-à-vis de l'entreprise, il frise tout simplement les 90%. Pourtant 26% des personnes interrogées se sont retrouvées recevoir des pages Web ou des mails non sollicités, ce qui les a amené à découvrir sur leurs machines des softs qui n'avaient rien à y faire. Face à un des comportements aussi dangereux, il serait grand temps de prendre les choses en main et notamment de procéder, comme le suggère Geoff Haggart, vice-président EMOA de Websense à un net effort d'éducation. Car, comme il le fait remarquer :

« Les employés infectant leur ordinateur portable avec des logiciels espions ne le font pas de manière intentionnelle; s'ils savaient que leurs données personnelles et les informations de leur entreprise étaient en danger, je pense qu'ils prendraient les mesures nécessaires pour garantir leur protection ». Et de poursuivre: « Il appartient aux entreprises européennes de protéger et d'éduquer leurs employés et de faire respecter par des contraintes physiques leur politique d'usage d'Internet, afin de soustraire aux logiciels espions toutes les communications leur permettant de dérober par inadvertance des données confidentielles ». Bref, mille fois sur le réseau reprenez votre message pour du spyware effacer l'irréparable outrage !