***Les cyberespions utilisent la porte de service (Â« backdoor Â»)***
**SÃ©curitÃ©**
PostÃ© par : JPilo
PubliÃ©e le : 18/11/2009 0:00:00

Un espion se repose de ses aventures en buvant un cocktail aprÃ¨s avoir ingÃ©nieusement dÃ©jouÃ© la sÃ©curitÃ© du quartier gÃ©nÃ©ral de ses ennemis et dÃ©robÃ© des documents confidentiels. Câ□□est ce que font les espions dans les films. **Dans le monde rÃ©el, ils utiliseraient plutÃ´t un clavier.**

Lâ□□espionnage consiste Ã  collecter des informations. Lorsque les informations Ã©taient toujours Ã©crites sur du papier, un espion devait physiquement se dÃ©placer pour les voler. Aujourdâ□□hui, les informations sont des donnÃ©es qui rÃ©sident sur des ordinateurs et des rÃ©seaux. Lâ□□espionnage moderne utilise donc souvent des logiciels malveillants. Les cyberespions utilisent des chevaux de Troie (Â« trojans Â» et des portes de service Â« backdoors Â») pour infecter les ordinateurs de leurs cibles, et accÃ©der aux donnÃ©es depuis lâ□□autre bout du monde.

**Qui investit dans lâ□□espionnage ?** Les entreprises et les nations. Lorsque les entreprises y ont recours, cela sâ□□appelle de lâ□□espionnage industriel. Lorsque les nations y ont recours, câ□□est tout simplement de lâ□□espionnage.

Dans la plupart des cas, les attaques sont effectuÃ©es par courrier Ã©lectronique vers des individus soigneusement sÃ©lectionnÃ©s, un seul individu ou des entreprises. Les cibles reÃ§oivent ce qui ressemble Ã  du courrier Ã©lectronique ordinaire avec un document en piÃ¨ce jointe, provenant souvent dâ□□une personne qui leur est familiÃ¨re. En rÃ©alitÃ©, la totalitÃ© du message est une contrefaÃ§on. Les coordonnÃ©es de lâ□□expÃ©diteur du message sont contrefaites, et le document joint, apparemment sans danger, contient le code de lâ□□attaque. Si le destinataire ne rÃ©alise pas que le message est une contrefaÃ§on, lâ□□attaque passera inaperÃ§ue.

Des fichiers programmes tels que les fichiers EXE de Windows ne passant pas au travers des pare-feux et des filtres, les cybercriminels utilisent donc couramment des fichiers PDF, DOC, XLS et PPT comme piÃ¨ce jointe. Ils ont Ã©galement plus de chances dâ□□Ãªtre reconnus comme Ã©tant des documents sans danger par les destinataires. Dans leur forme habituelle, ces types de fichiers ne contiennent pas de code exÃ©cutable binaire ; les cybercriminels exploitent donc les vulnÃ©rabilitÃ©s dâ□□applications telles que Adobe Reader et Microsoft Word pour infecter lâ□□ordinateur.

La structure de ces fichiers dâ□□attaque a Ã©tÃ© dÃ©libÃ©rÃ©ment modifiÃ©e pour entraÃ®ner le disfonctionnement de lâ□□application de bureautique utilisÃ©e pour les ouvrir, et exÃ©cuter simultanÃ©ment le code binaire situÃ© Ã  lâ□□intÃ©rieur du document. Ce code crÃ©e habituellement deux nouveaux fichiers sur le disque dur et les exÃ©cute. Le premier est un document sain qui sâ□□ouvre Ã  lâ□□Ã©cran de lâ□□utilisateur et dÃ©tourne son attention du disfonctionnement.

Le second est une porte de service (Â« backdoor Â») qui se lance immÃ©diatement et se cache dans le systÃ¨me, souvent Ã  lâ□□aide de techniques de rootkits. Il Ã©tablit une connexion depuis lâ□□ordinateur infectÃ© vers une adresse rÃ©seau spÃ©cifique situÃ©e quelque part dans le monde. Avec lâ□□aide de cette porte de service, le cybercriminel accÃ¨de aux informations situÃ©es sur lâ□□ordinateur cible, ainsi quâ□□aux informations situÃ©es dans le rÃ©seau local auquel la cible accÃ¨de.

Les attaques utilisent souvent des programmes de porte de services tels que Gh0st RAT ou Poison Ivy pour surveiller leurs cibles Ã  distance. De tels outils leurs permettent dâ□□effectuer toutes les opÃ©rations quâ□□ils souhaitent sur la machine cible, y compris enregistrer les frappes au clavier pour collecter des mots de passe, et un gestionnaire de fichiers distant pour rechercher des documents au contenu intÃ©ressant. Les cybercriminels espionnent parfois leur cible en contrÃ´lant le microphone de lâ□□ordinateur infectÃ© Ã  distance.

Je surveille les attaques ciblÃ©es depuis qu'elles ont Ã©tÃ© observÃ©es pour la premiÃ¨re fois en 2005. Les cibles sont de grandes entreprises, des gouvernements, des ministÃ¨res, des ambassades et des associations Ã  but non lucratif, telles que celles qui font campagne pour la libertÃ© du Tibet, soutiennent les minoritÃ©s en Chine ou reprÃ©sentent la religion Falun Gong. Il serait facile de pointer du doigt le gouvernement chinois. Mais nous nâ□□avons pas de preuve. Personne ne peut prouver avec certitude lâ□□origine de ces attaques. En fait, nous devons considÃ©rer que plusieurs gouvernements sâ□□adonnent aux mÃªmes attaques.

Il est Ã©galement clair que ce que nous avons vu jusquâ□□Ã  prÃ©sent nâ□□est que le dÃ©but. Lâ□□espionnage en ligne ne peut que devenir un outil important de collecte d'informations dans le futur. La protection contre de telles attaques peut sâ□□avÃ©rer trÃ¨s difficile.

La mÃ©thode la plus efficace pour protÃ©ger des donnÃ©es contre le cyberespionnage consiste Ã traiter les informations confidentielles sur des ordinateurs dÃ©diÃ©s non connectÃ©s Ã  Internet. Les infrastructures vitales devraient Ãªtre isolÃ©es des rÃ©seaux publics. Mais isolation ne signifie pas pare-feu : cela signifie dÃ©connexion. La dÃ©connexion est pÃ©nible, compliquÃ©e et onÃ©reuse, Mais elle est Ã©galement la solution.

[ **Mikko HyppÃ¶nen**, Directeur des Laboratoires de recherche chez F-Secure ]