

Sécurité totale, un idéal impossible à atteindre !

Par Pierre Marc Bureau,
Chercheur en malware
chez ESET





Si vous avez sursauté en lisant ce titre, c'est probablement parce que vous ne passez pas assez de temps en compagnie de vos administrateurs réseaux ou autres professionnels de la sécurité.

Loin de moi l'idée d'être alarmiste, j'appelle au réalisme. La sécurité de nos systèmes et de nos réseaux n'est pas un état qu'on atteint une fois pour toutes. La sécurisation de nos systèmes sera le résultat d'un effort qui devra être soutenu et constant. Il y aura toujours place à l'amélioration, pour tout le monde.

Les menaces contre les systèmes informatiques évoluent constamment. Pour bien évaluer une menace et les risques qui y sont associés, on doit tenir compte de sa probabilité. La probabilité d'occurrence d'une menace est déterminée en fonction de la capacité d'un attaquant de pénétrer un système, de sa motivation et des opportunités qui s'offrent à lui. Avec l'évolution rapide des systèmes informatiques, ces trois facteurs sont en constante augmentation.

«La capacité d'un attaquant est fondée sur sa connaissance de l'informatique offensive et des réseaux qu'ils ciblent.»

Premièrement, la capacité d'un attaquant est fondée sur sa connaissance de l'informatique offensive et des réseaux qu'ils ciblent. L'Internet est un terrain fertile pour échanger toutes sortes d'informations et les forums spécialisés y apparaissent par centaine chaque année. Sur ces forums, on peut trouver des informations sur les dernières failles de sécurité autant que des astuces pour cloner une carte RFID permettant d'accéder à un bâtiment sécurisé.

Un autre exemple a été donné lors du dernier concours pwn2own organisé à la conférence CanSecWest. Des experts en sécurité ont réussi à s'introduire dans trois ordinateurs sécurisés (un utilisant Microsoft Windows, l'autre Mac OS X et le dernier Linux). Ces prouesses montrent que plusieurs individus ont la capacité de pirater des ordinateurs même si ceux-ci sont tenus à jour avec les derniers correctifs.

Puisque les entreprises et les individus stockent maintenant toutes leurs informations sur des ordinateurs et que la plupart de ces informations peuvent être facilement revendues, il devient alléchant d'attaquer les systèmes pour les dérober.

Au cours des dernières années, nous avons noté une forte augmentation du nombre d'attaques dont le but final était d'installer un agent conçu pour dérober des informations. Les informations volées ne s'arrêtent pas aux numéros de carte de crédit; plusieurs groupes s'intéressent maintenant aux comptes relatifs aux jeux en ligne, réseaux sociaux et serveurs FTP ou SSH sauvegardés dans vos applications favorites, etc. Les pirates utilisent rarement cette information pour eux-mêmes mais la vendent à d'autres groupes spécialisés dans l'utilisation de ces renseignements. Puisque les éditeurs de logiciels préfèrent souvent ajouter de nouvelles fonctionnalités à leurs logiciels plutôt que de les sécuriser, les zones et opportunités d'attaques augmentent. Les administrateurs réseaux doivent régulièrement gérer la mise à jour de dizaines d'applications et chaque jour qui passe avant la mise en place d'un correctif est une opportunité de plus pour un attaquant de pénétrer le réseau et de s'y installer.

«Les pirates utilisent rarement cette information pour eux-mêmes mais la vendent à d'autres groupes spécialisés dans l'utilisation de ces renseignements.»

L'augmentation du nombre d'utilisateurs et d'ordinateurs connectés à nos réseaux est aussi responsable des opportunités grandissantes d'attaques. Plus il y a d'ordinateurs connectés à un réseau et plus il y a d'utilisateurs en ligne, plus les chances d'une erreur humaine surviennent. Nous ne devons pas seulement concentrer nos efforts contre les fameux pirates informatiques, figures mythiques tapant sur leur clavier plus vite que leur ombre et vivant dans leur caverne en se nourrissant de soda. Les menaces les plus courantes contre lesquelles nous devons nous prémunir sont les outils automatisés concoctés par des programmeurs, bons ou moins bons, qui veulent voler notre argent ou nos informations. Ces outils automatisés sont les logiciels malveillants qui polluent nos réseaux et nos boîtes de courrier électronique.

«les malware sont indépendants, ils ne prennent jamais de pause et peuvent rapidement trouver une victime mal protégée sur un réseau.»

Les malware s'attaquent souvent aux proies faciles puisqu'ils sont programmés pour exploiter certaines failles de sécurité ou deviner un mot de passe à partir d'un petit dictionnaire. Par contre, leur distribution et leur rapidité d'action nous rappellent que c'est une menace qui doit être prise au sérieux. Le plus souvent, les malware sont indépendants, ils ne prennent jamais de pause et peuvent rapidement trouver une victime mal protégée sur un réseau.

La seule méthode efficace pour sécuriser un ordinateur ou un réseau est la défense en profondeur, c'est-à-dire de ne pas se fier uniquement à un mécanisme de sécurité comme un firewall ou un antivirus mais bien d'utiliser tous les outils disponibles pour réduire au maximum le risque d'attaque. Ces outils sont de natures diverses. Ils commencent par le domaine juridique où l'on doit avoir des lois justes qui comprennent les crimes informatiques et les punissent équitablement. L'éducation des utilisateurs est aussi un outil essentiel pour prévenir les cas d'extorsion ou d'infections causés par un utilisateur. Côté technologie, plusieurs moyens doivent être déployés incluant un pare-feu, un filtre anti spam et, bien sûr, une solution antivirale. Tous les logiciels installés, incluant ceux de sécurité, et les systèmes d'exploitation doivent être rigoureusement tenus à jour.

Il est évident qu'un grand nombre de malware sont créés pour attaquer le très populaire système d'exploitation Microsoft Windows. Par contre, il est bon de rappeler que des menaces existent aussi contre Linux et Mac OS X. Peu importe le système d'exploitation, les utilisateurs seront toujours vulnérables à des attaques d'ingénierie sociale. Un logiciel antivirus qui les aide à identifier des fichiers suspects est toujours un atout. Du côté des serveurs, nous recommandons aussi l'utilisation d'un antivirus puisque même s'ils sont administrés par des utilisateurs confirmés, on doit s'assurer de l'intégrité du contenu qui y est hébergé ou qui y transite.

«Peu importe le système d'exploitation, les utilisateurs seront toujours vulnérables à des attaques d'ingénierie sociale.»

Il faut se rappeler que l'ordinateur le plus sécurisé est éteint et verrouillé dans un coffre fort.

La sécurité informatique n'est pas une simple case que l'on peut cocher sur une liste de tâches relative à la gestion du réseau. C'est un processus que l'on doit répéter régulièrement afin de bloquer le plus de brèches possibles.

