



Article de Philippe Giroux
Directeur de la pratique de sécurité
ESI Technologies

Les stratégies des codes malicieux

Que ce soit en créant des virus, des spywares, des vers informatiques, des bannières publicitaires intempestives, des pourriels ou autres formes encore, les programmeurs de code malicieux ne cessent de trouver de nouvelles idées pour déjouer ceux qui tentent de les bloquer. Ces idées vont des plus simples aux plus évoluées.

Le but d'un code malicieux est de se faire ouvrir par la victime. À force d'entendre la mise en garde disant qu'un fichier inattendu ne devait pas être ouvert, certains utilisateurs ont cessé d'ouvrir les fichiers joints à leur courriel. Les codes malicieux ont donc choisi de se présenter sous un nom qui tromperait ces utilisateurs.

Pour plusieurs, un nom se terminant par .com correspond au nom du site Web d'une entreprise ou encore à l'extension de ses adresses de courriels. Par contre, un fichier se terminant par .com est bel et bien un exécutable, au même type qu'un fichier .exe. Ainsi, des utilisateurs ont ouvert une ressource nommée microsoft.com en croyant aller voir un site web de confiance alors qu'ils démarraient plutôt un programme malicieux.

À la fin juillet 2004, le ver MyDoom-o a innové en utilisant le nom de domaine de la cible attaquée pour personnaliser encore plus le corps du message ainsi que le nom de sa pièce jointe. En allant chercher encore plus de confiance que les autres, le ver a réussi à se propager à une vitesse supérieure, réussissant même parfois à entrer dans un réseau avant que la signature antivirus associée n'y parvienne.

Sur les sites Web, plusieurs dessinent une bannière dont les contours, les couleurs et le contenu sont ceux d'une fenêtre par défaut de Windows. Les utilisateurs vont alors cliquer sur le X du coin supérieur droit en pensant fermer une fenêtre d'erreur qui ne les intéresse pas. Cependant, en cliquant n'importe où dans l'image en question, ils activent plutôt un lien qui peut autant les conduire à des sites Web non professionnels que leur ouvrir des messages publicitaires à la chaîne ou divulguer de l'information à un inconnu.

Les polluposteurs ont aussi plusieurs stratégies pour obtenir une adresse de courriel. L'une d'elle est d'envoyer à une adresse potentielle un lien qui offre de se désabonner de la liste utilisée pour envoyer le présent message. Certains, plus subtiles, mettent dans le message un lien http avec un numéro unique qui pointe vers leur serveur. À l'activation de ce lien, le serveur choisi par le polluposteur reçoit la confirmation que son message a été reçu et lu, donc que l'adresse est valide. Il pourra alors l'inonder sur-le-champ ou la revendre à d'autres en tant qu'adresse confirmée.

Une autre stratégie consiste à écrire un message qui captera l'attention du lecteur et lui demandera de le faire suivre à toutes les personnes qu'il connaît. Chaque personne qui se laisse tromper ajoute quelques dizaines d'adresses de courriels à la copie qu'il fait suivre. En quelques instants, chaque copie du message contient des centaines d'adresses de courriels valables. Quand le polluposteur revoit l'un d'eux, il a plusieurs adresses valables et récentes entre les mains.

Devant toutes ces subtilités, il devient de plus en plus difficile pour un utilisateur régulier de ne pas se laisser piéger. C'est pourquoi les entreprises d'aujourd'hui sont contraintes de déployer une infrastructure qui protégera les utilisateurs de ces pièges.

Ainsi, les passerelles de courrier électronique doivent absolument bloquer toutes les extensions de fichiers exécutables et refuser de distribuer un courriel qui serait destiné à un trop grand nombre d'adresse à la fois. Dans le même sens, un système de filtrage d'URL doit aussi être déployé pour éviter qu'un utilisateur, volontairement ou non, ne se retrouve à accéder un site Web malicieux. Puisque maintenant le frein à leurs codes malicieux est en infrastructure, les programmeurs mal intentionnés ont commencé à lutter contre ces mécanismes.

Le polluposteur s'installe aujourd'hui un laboratoire dans lequel il opère sa propre passerelle anti-pourriel et tente d'en écrire un qui contiendra le message voulu mais ne semblera pas suspect à la passerelle de filtrage.

De leur côté, les fichiers joints aux courriels se chiffrent maintenant à l'aide d'un mot de passe écrit dans le message. La passerelle ne peut donc filtrer le code malicieux en transit car il est alors chiffré. Par contre, l'utilisateur l'ouvrira facilement car en lisant le message, il apprendra le mot de passe qui déchiffrera le fichier.

En juillet 2004, un virus est allé encore plus loin que tous les autres en matière de contre-mesure. Les fabricants d'antivirus ont des techniques de travail qui permettent d'exécuter le virus dans un sous-système indépendant pour observer son comportement. C'est ainsi qu'ils identifient la signature du virus et peuvent ensuite le bloquer. Par contre, ce dernier virus ne se laisse pas faire.

À son démarrage, il regarde s'il est exécuté dans une telle prison ou s'il est libre. S'il est libre, il fera sa contamination. Par contre, s'il détecte qu'il est étudié, il s'arrêtera immédiatement pour ne pas révéler son mode d'opération.

La souris fait tout ce qu'elle peut pour déjouer le chat; le chat doit faire tout son possible pour attraper la souris. Aujourd'hui, cela exige une bonne infrastructure de sécurité qui identifiera et bloquera le maximum de pièges tendus à ses utilisateurs. Cette infrastructure doit couvrir tous les services offerts aux utilisateurs, le minimum étant le plus souvent le courriel et le Web.

Malgré cela, l'infrastructure ne pourra être parfaite et tout bloquer. Il faut donc sensibiliser les utilisateurs pour qu'ils repèrent eux-mêmes les signes d'un tel piège et n'y tombent pas. Il faut également leur offrir un environnement qui répondra à tous leurs besoins, mais sans plus. En ayant un minimum de droits, le code malicieux qui les trompera représentera un minimum de risques.