

Rôle de l'Internet dans la Propagation des Malwares

Introduction

L'Internet joue un rôle essentiel au coeur de l'activité quotidienne d'une entreprise, quelle que soit sa taille. Son site Web constitue son principal vecteur de communication avec les clients actuels et futurs, mais également avec d'autres acteurs essentiels de son activité. Les salariés de l'entreprise réalisant la plus grande partie de leur travail via le Web, l'impact du courrier électronique sur la rapidité et l'efficacité des communications internes et externes a été considérable. Globalement, e-mail et accès à Internet représentent 90 % des applications critiques à l'activité des PME.

Les outils Internet ont métamorphosé le monde économique, générant des gains extraordinaires en efficacité et en productivité. Malheureusement, les créateurs de malware (programme malveillant) ont eux aussi su tirer avantage de cette évolution. Il fallait auparavant des mois pour qu'une menace infecte quelques milliers d'ordinateurs. L'Internet a donné aux pirates les moyens d'atteindre des centaines de milliers d'ordinateurs, en quelques minutes seulement.

Evolution des menaces de sécurité

Les menaces de sécurité font partie du paysage quotidien de l'utilisateur d'outils informatiques depuis 1986 et la découverte de Brain, un virus s'attaquant au secteur d'amorçage. Les virus de secteur d'amorçage se propageaient en s'inscrivant sur une disquette, puis en se transférant sur le PC de l'utilisateur au démarrage. En 1995, les virus de secteur d'amorçage ont laissé la place aux macro virus. Ces virus étaient programmés en langage script et visaient plus particulièrement les documents Microsoft Word et Excel. La technique de propagation de ces deux types de virus était lente et inefficace : elle nécessitait l'intervention de l'utilisateur pour passer d'un ordinateur à l'autre sur disquette. Un simple logiciel antivirus suffisait pour éradiquer ce type de menace.

Tout a changé en 1999, avec l'apparition du virus Melissa. Première menace véhiculée par e-mail, Melissa n'avait pas besoin d'être transportée physiquement d'un ordinateur à l'autre. Bien au contraire, elle a pu se répandre rapidement et facilement en exploitant la rapidité et l'efficacité inhérentes aux communications réseaux. C'est ce concept qui serait dorénavant utilisé par les créateurs des menaces. Des virus e-mail aux menaces hébergées sur le Web en passant par les vers de réseau, l'Internet était devenu le nouveau vecteur de diffusion.

En plus de ces incroyables avantages pour la propagation des menaces, l'Internet offrait aux créateurs de malware la possibilité d'afficher et de partager leur code avec d'autres programmeurs. Cette mise en réseau a permis de développer de nouvelles versions d'une menace simplement en apportant quelques modifications à un code existant. Même pour les programmeurs novices et les " script kiddies ", pirates néophytes, créer et diffuser massivement de nouvelles menaces était devenu rapide et facile. De même, les détenteurs de réseaux de zombies et de listes e-mail de spamming ont commencé à louer ou même à vendre leur code malveillant, fournissant aux programmeurs un réseau de diffusion naturel pour leurs créations.

Face à cette rapidité et à cette efficacité inédites, les applications bureautiques antivirus se sont avérées incapables d'offrir une protection suffisante, dépassées par la fréquence et le nombre de nouvelles menaces apparaissant constamment.

Une méthode de propagation efficace

Ainsi qu'il a été dit plus haut, l'Internet a créé un environnement particulièrement propice à la création et la diffusion des menaces informatiques. Le concept sous-jacent de l'Internet consiste à relier tous les ordinateurs en un réseau afin qu'ils puissent communiquer. Rapidement, les auteurs de malwares ont compris qu'ils pouvaient tirer profit du formidable potentiel de ce réseau pour propager leurs menaces. Ces pirates n'avaient plus besoin d'infecter un ordinateur à la fois, mais pouvaient désormais diffuser massivement leur code auprès du grand public.

L'apparition de l'Internet a donné naissance à un mécanisme de diffusion des menaces faisant appel à plusieurs techniques différentes, parmi lesquelles l'e-mail, le spam, les bots (robots), les vers de réseau et les drive-by downloads (téléchargements intempestifs).

Les Virus

La première menace sérieuse qui se soit propagée par Internet a utilisé le courrier électronique. Des virus, comme Loveletter par exemple, ont été diffusés sous la forme d'une pièce jointe à un e-mail. Si l'on ouvrait la pièce jointe, le virus était activé et infectait l'ordinateur. Ensuite, le virus se multipliait en envoyant un clone à chaque destinataire figurant dans le carnet d'adresses du client e-mail de la victime, en utilisant le nom de la victime comme expéditeur. De cette façon, les destinataires du message pensaient que l'e-mail avait été envoyé par une personne qu'ils connaissaient. Loveletter a ainsi contaminé des centaines de milliers d'ordinateurs en une seule journée, causant des dommages pour un montant estimé entre 5 et 7 milliards de dollars.

Pour inciter le destinataire à ouvrir la pièce jointe, le pirate ajoutait un texte dans le corps du message, lui disant que la pièce jointe était une lettre d'amour à son attention. Cette technique était une ébauche rudimentaire de ce que l'on connaît maintenant sous le nom de piratage psychologique. Sans entrer dans les détails, le piratage psychologique est une méthode de tromperie utilisée par les pirates informatiques dans le but d'infecter le système de leur victime. Le piratage psychologique exploite une faille contre laquelle les logiciels de sécurité ne pourront jamais rien : la nature humaine de l'utilisateur.

Le Spam

Les menaces véhiculées par e-mail ont ensuite logiquement évolué vers le spam. Si les premières menaces e-mail s'apparentaient à une chaîne de courrier, qui dépendait d'une erreur du destinataire pour poursuivre sa diffusion de façon linéaire, le spam est envoyé directement aux destinataires ciblés.

La plupart du temps, le spam prend la forme d'une "publicité" pour des produits ou des services. Le recours au spam est généralement utilisé pour assurer la promotion d'un site Web pour adultes, d'un plan d'investissement, la vente de médicaments illégaux, entre autres offres promotionnelles. Par conséquent, le spam constitue le plus souvent avant tout une nuisance. Pourtant, il sert parfois à véhiculer certaines menaces informatiques (virus, spyware, chevaux de Troie, rootkits...).

Le cabinet d'études Gartner, spécialisé dans les technologies de pointe estime qu'entre 2 et 6 % du spam sert à propager une menace de ce type. Ce pourcentage peut sembler modeste, mais il devient beaucoup plus significatif si l'on considère par ailleurs que 80 à 95 % du trafic e-mail entrant sur le réseau d'une entreprise est du spam. Qu'il serve ou non à véhiculer une menace, le spam demeure une source d'inquiétude pour les entreprises par le volume impressionnant de messages qu'il représente : l'impact sur les performances du réseau peut être considérable.

Les Vers de Réseau

Un ver de réseau est capable de se mouvoir avec fluidité sur le réseau de l'entreprise, en toute autonomie. Comme ils sont totalement indépendants d'une intervention de l'utilisateur, les vers peuvent se propager très rapidement. Par exemple, en juillet 2001, le ver Code Rouge a infecté 359 000 systèmes en 14 heures, causant des dommages estimés à plus de 2,6 milliards de dollars. De même, en septembre 2001, le ver Nimda a infecté plus de 160 000 systèmes en sept heures, et même jusqu'à 450 000 systèmes en 24 heures.

Les vers se propagent généralement en exploitant les failles du système d'exploitation, mais ils peuvent également prendre la forme d'une pièce jointe à un e-mail. Une fois que le ver a atteint le système de sa victime, son moteur SMTP intégré lui permet de contourner complètement les programmes de messagerie existants et de se propager librement sur le réseau de l'entreprise, sans qu'aucune action de la part de l'utilisateur ne soit nécessaire. Comme le ver s'accompagne de tout ce dont il a besoin pour établir une connexion avec un serveur de messagerie, il est capable de se propager à n'importe quelle adresse e-mail qu'il aura récupérée sur l'ordinateur infecté. Puisque le ver n'utilise pas le programme de messagerie installé sur le système, l'utilisateur de l'ordinateur infecté peut parfaitement ne pas se rendre compte qu'un ver est en train de se propager.

Les vers accaparent une grande partie du débit disponible, à mesure qu'ils se dupliquent et se diffusent librement sur le réseau. Les performances du réseau peuvent donc se dégrader, parfois jusqu'au blocage complet. Les vers peuvent également être porteurs d'autres menaces - spyware, virus, chevaux de Troie - susceptibles d'entraîner des problèmes supplémentaires.

Les Bots

Lorsque les créateurs de malware souhaitent réaliser un envoi particulièrement volumineux de spam, de virus ou de spyware, ils peuvent pour cela utiliser un Bot. Un "bot", diminutif de "Web Robot", est un logiciel programmé pour exécuter des tâches simples et répétitives sur Internet. En moyenne, un botnet correspond à un réseau de 20 000 ordinateurs infectés, également appelés "zombies", utilisés pour lancer une menace coordonnée à très grande échelle. Les plus grands réseaux de zombies peuvent comporter plus d'un million d'ordinateurs infectés.

Puisque les bots ont la faculté de communiquer avec d'autres services réseau, ils sont souvent utilisés pour communiquer avec d'autres ordinateurs au moyen de différents protocoles réseau. Un bot peut être associé à un spyware pour dérober certaines informations confidentielles. Il s'agit généralement d'un numéro de carte de crédit, d'identifiants bancaires ou autres informations commerciales. L'attaque peut également et tout simplement cibler les identifiants VPN ou autres codes de connexion d'une entreprise. Ils sont parfois également utilisés pour lancer une attaque DDos (attaque par déni de service distribué), au cours de laquelle un grand nombre de zombies envoie au réseau de la victime des millions de requêtes de connexion, jusqu'à le paralyser et à en bloquer l'accès. Des attaques DDos ont ainsi été lancées contre des sites comme eBay, America Online, Amazon, CNN, E-Trade, et Yahoo.

Les Drive-By Downloads

Les téléchargements intempestifs "drive-by download" font partie des menaces web. Il s'agit d'une menace sensiblement différente de celles évoquées précédemment, en ce sens qu'elle compte sur la victime pour venir à elle, plutôt que d'attaquer le système de la victime. Un "drive-by download" permet d'installer des menaces - bot, spyware, adware, chevaux de Troie - à l'insu de l'utilisateur et sans aucune intervention de sa part. Lorsque l'utilisateur visite un site Web infecté, la menace est automatiquement téléchargée en arrière-plan. Le site infecté peut être un site malveillant développé par un concepteur malintentionné pour offrir une apparence respectable, mais il peut également s'agir d'un site légitime victime d'un piratage puis d'une infection par cette menace. En tous cas, l'utilisateur n'a même pas conscience d'avoir été infecté.

Se protéger contre les menaces véhiculées par Internet

Pour garantir à l'organisation une protection adéquate contre les menaces qui se propagent par l'Internet, il convient d'adopter une approche globale, développant plusieurs niveaux de sécurité. Même s'il s'agit d'une première démarche incontournable, l'installation d'une solution de sécurité bureautique ne suffira pas pour gérer le volume, la rapidité et l'efficacité des menaces véhiculées par Internet. Seul, un logiciel de ce type ne permet donc plus de garantir l'intégrité des actifs du réseau de l'entreprise. Pour mettre en place une protection globale, il est impératif de compléter le logiciel de sécurité bureautique par une solution de sécurité avancée au niveau de la passerelle, qui

analysera à la fois le trafic entrant et le trafic sortant afin de détecter et de supprimer les menaces avant qu'elles n'atteignent l'ordinateur des utilisateurs.

La plupart des attaques réseau se propagent par e-mail, via le Web, ou utilisent le réseau interne de l'entreprise avant de parvenir jusqu'au système d'un utilisateur du réseau. Certaines menaces, comme les vers de réseau, s'attaquent directement au réseau de l'entreprise, sans avoir besoin de passer par le système d'un utilisateur. Par conséquent, il est essentiel de doter le réseau d'une solution de sécurité bien conçue au niveau de la passerelle pour fermer la porte aux menaces.

Conclusion

Pour garantir à l'organisation une protection adéquate contre les menaces qui se propagent par l'Internet, il convient d'adopter une approche globale, développant plusieurs niveaux de sécurité. Même s'il s'agit d'une première démarche incontournable, l'installation d'une solution de sécurité bureautique ne suffira pas pour gérer le volume, la rapidité et l'efficacité des menaces véhiculées par Internet. Seul, un logiciel de ce type ne permet donc plus de garantir l'intégrité des actifs du réseau de l'entreprise. Pour mettre en place une protection globale, il est impératif de compléter le logiciel de sécurité bureautique par une solution de sécurité avancée au niveau de la passerelle, qui analysera à la fois le trafic entrant et le trafic sortant afin de détecter et de supprimer les menaces avant qu'elles n'atteignent l'ordinateur des utilisateurs.

La plupart des attaques réseau se propagent par e-mail, via le Web, ou utilisent le réseau interne de l'entreprise avant de parvenir jusqu'au système d'un utilisateur du réseau. Certaines menaces, comme les vers de réseau, s'attaquent directement au réseau de l'entreprise, sans avoir besoin de passer par le système d'un utilisateur. Par conséquent, il est essentiel de doter le réseau d'une solution de sécurité bien conçue au niveau de la passerelle pour fermer la porte aux menaces.

NETGEAR ProSecure STM : Solution de management des menaces Web et E-mail

Le boîtier ProSecure STM fait appel à une technologie exclusive qui détecte et bloque les attaques de façon appropriée à la rapidité et à l'étendue de leur propagation. Par cette approche, il est possible de détecter le spam et les attaques de malwares dès leur apparition, et de bloquer en temps réel tous les messages associés.

Le boîtier ProSecure STM intègre la technologie Netgear de Stream Scanning (Scan à la Volée), en attente de brevet, qui permet d'analyser les flux de données au moment où ils entrent sur le réseau. Grâce à la technologie Stream Scanning, les boîtiers NETGEAR STM peuvent traiter un volume important de données en temps réel, une seule analyse suffisant pour identifier le spam, les malwares, les atteintes à la sécurité ou les applications inappropriées. Il est ainsi possible de garantir aux utilisateurs du réseau un contenu e-mail et Web sûr, sans temps d'attente.

Le boîtier ProSecure STM utilise un système de défense comportemental et proactif qui supprime l'intervalle existant jusqu'alors entre l'exploitation d'une vulnérabilité et sa correction. La solution NETGEAR intègre une analyse chirurgicale qui permet d'identifier les caractéristiques suspectes du trafic réseau entrant et sortant, et de les neutraliser jusqu'à ce qu'elles puissent être examinées de manière approfondie.