G DATA

Whitepaper 2008

Les variantes d'usurpation de données

Ralf Benzmüller, G DATA Security Labs

Go safe. **Go safer. G DATA.**

Les attaques virtuelles présentent depuis longtemps un problème de plus en plus préoccupant, impliquant la police et les services secrets du monde entier. Les différentes menaces actuelles, qui se répandent sur Internet, sont principalement d'origine criminelle et proviennent d'organismes agissant à l'échelle internationale. La délinquance virtuelle est source de milliards de dommages chaque année. L'hameçonnage par e-mail, causé par de faux sites, n'en est qu'une variante. Les vols de données par chevaux de Troie sont de plus en plus fréquents. Il s'agit maintenant de bien plus que des codes confidentiels ou numéros de transaction. C'est même leur propre identité en ligne que perdent les utilisateurs !

Hameçonnage

L'hameçonnage est une tentative d'usurpation de données confidentielles des utilisateurs par l'intermédiaire de techniques trompeuses. Depuis la première tentative de la sorte, au milieu des années 90, le nombre de menaces d'hameçonnage a considérablement augmenté. D'après une estimation du laboratoire de G DATA, cette période de croissance semble être arrivée à sa fin. En effet, depuis environ un an, le nombre de nouveaux messages et sites hameçonneurs semble rester constant. Ils sont devancés par les problèmes de langues et de jeux de caractères. Les outils souples et faciles d'utilisation tels que RockPhish permettent aux malfaisants d'héberger plusieurs pages d'hameçonnage sur un site.

Les personnes les plus ciblées sont toujours les clients de banques en ligne, particulièrement dans certains états comme le Royaume-Uni et les Etats-Unis, où seuls un code secret et un numéro de transaction bloquent l'accès des voleurs aux comptes en banque.

Nouveaux « marchés »

Les sites eBay falsifiés et leur service de paiement PayPal sont également bien placés. La recherche de nouvelles victimes est désormais en plein essor, c'est ainsi que les sites de commerce en ligne sont de plus en plus représentés dans les sites malintentionnés. Les pages d'identification de certaines plates-formes de réseaux sociaux, de recherche d'emploi et de jeux par Internet ont également fait l'objet de falsifications qui ont été détectées. Les comptes d'utilisateurs ont de plus en plus de valeur aux yeux des cyber-délinquants. Un compte eBay usurpé peut maintenant être utilisé pour blanchir l'argent gagné par le biais de l'hameçonnage. Les voleurs de données trouvent également dans les plates-formes de réseaux sociaux des informations qu'ils accumulent avant de pouvoir les revendre. Les comptes d'utilisateurs saisis peuvent également servir à diffuser du courrier indésirable.

Le filtrage anti-spam permet de protéger contre l'hameçonnage. Il reconnaît les courriers hameçonneurs et, idéalement, les empêche de s'afficher. Toutefois, pour une protection optimale, il doit détecter et bloquer toute forme de spam quel que soit le contenu. La technologie OutbreakShield de G DATA est le système de filtrage le plus efficace, qui bloque absolument toute forme de spam et de courrier d'hameçonnage en temps réel, quel que soit le contenu.

Tactique modifiée

Les systèmes de filtrage anti-spam de plus en plus efficaces ont cependant contraint les criminels à modifier leur stratégie. Désormais, l'accès aux pages hameçonneuses ne se limite plus à l'ouverture de spams : le danger existe également lors de discussion, dans les forums et avec les jeux en ligne.

Blocage

Les barres d'outils anti-hameçonnage des navigateurs Web avertissent les utilisateurs des pages dangereuses ou bloquent leur accès. IE7, FF2 et de nombreuses autres solutions de sécurité sur Internet comportent ces fonctionnalités de façon innée. Toutes les autres sont disponibles pour le téléchargement et l'installation (Phishtank, Google, Netcraft &Co, etc.). Ces outils reposent sur des processus heuristiques de détection des mauvaises adresses URL. Le danger de faux-positif perdurant, les règles sont plutôt strictes.

De nombreux fournisseurs appellent de surcroît à la force de la communauté. Quiconque trouve un site falsifié doit le reporter à l'équipe d'assistance, qui le vérifiera et l'ajoutera à la liste noire si nécessaire.

Toutefois, cette méthode présente un inconvénient majeur : la vérification du site est une procédure de très longue durée. Phishtank nécessite en moyenne annuelle deux jours, alors que les fournisseurs commerciaux ne prennent que quelques heures. Toutefois, les usurpateurs peuvent agir librement durant cette période.

Engagement des utilisateurs

Les solutions techniques contre l'hameçonnage ne sont donc pas infaillibles. La sensibilisation des utilisateurs est le meilleur moyen de lutter contre la perte de données, comme dans de nombreux autres cas de vol. Les internautes doivent généralement agir avec prudence lors de la saisie de données personnelles sur Internet. La vérification de l'adresse URL (https:// nom de domaine à lire de droite à gauche) devrait faire partie des obligations de l'utilisateur.

Pharming

Le pharming est une approche de substitution à l'hameçonnage classique. Elle consiste à diriger l'utilisateur, à son insu, vers des sites falsifiés, même si le nom de domaine est correct.

Technique de pharming

Ce type de menace est basé sur la détermination de l'adresse IP du nom de domaine. Pour cela, le système DNS même peut être ciblé. Dans les domaines de diffusion comme les WLAN, il est très facile de falsifier les tâches DNS.

Les serveurs DNS mal entretenus ou configurés permettent des actions malveillantes allant du remplissage du cache avec des fausses informations ou de l'empoisonnement du cache DNS au craquage du serveur DNS.

Le démantèlement des systèmes DNS démarre au niveau des clients, principalement par des chevaux de Troie. Comment se protéger facilement ? Il existe des méthodes simples de protection contre les attaques sur serveur DNS. Par exemple, les utilisateurs peuvent enregistrer le lien vers le site de leur banque comme adresse IP dans la rubrique des favoris. Cela paraît autrement lors des attaques sur l'infrastructure DNS. Dans ce cas, l'utilisateur d'Internet doit se fier aux opérateurs des serveurs DNS.

Crime-Ware

Chevaux de Troie, exploits et codes nuisibles

Voici un autre phénomène d'usurpation d'identité : les chevaux de Troie. Ils sont désormais les concurrents de la majorité écrasante des attaques d'hameçonnage.

Les divers mécanismes de protection contre l'hameçonnage et l'information grandissante des utilisateurs commencent à porter leurs fruits. Mêmes les contre-mesures des instituts financiers comme iTAN, mTAN, Token pour les transactions limitées et l'interface de banque en ligne à domicile contribuent à empêcher l'exploitation d'informations hameçonnées.

Les cyber-délinquants ont besoin de trouver de nouveaux moyens pour saisir les données et les monnayer le plus vite possible, du moins dans la plupart des états.

Les cyber-délinquants ont ainsi développé diverses sortes de logiciels criminels dans cet objectif :

- **Les enregistreurs de frappe** enregistrent les actions du clavier. Ils peuvent agir comme pilotes ou renvoyer des informations aux interfaces des systèmes d'exploitation prévues à cet effet (WinAPI Set-WindowsHook oder WinAPI GetKeyboardState). Ils s'intègrent dans les processus systèmes en cours comme winlogon.exe, services.exe ou utilisent des rootkits. Leur activation est souvent soumise à certaines conditions. Cela peut être le cas si un site déjà ouvert fait partie d'une liste de noms de domaines souvent très longue ou si plusieurs fenêtres de certains titres sont ouvertes.{}
- **Enregistreurs de frappe à l'écran :** les claviers visuels ont été développés pour contrecarrer les enregistreurs de frappe sur clavier. Les auteurs de logiciels malveillants ont réagi en inventant les enregistreurs de frappe à l'écran ou screenloggers. Ils font des captures d'écran de tout le contenu affiché à intervalles réguliers (par exemple, Rbot) ou un graphique de l'environnement de la souris à chaque clic. Parfois, des séquences d'images sont même instantanément transformées en film AVI.
- **Manipulation des navigateurs :** certains parasites comme Torpig modifient l'apparence du navigateur. Ils sont en mesure de représenter la ligne supérieure contenant la bonne adresse bien que le contenu vienne d'un autre domaine trafiqué. Même le cadenas signalant une liaison sécurisée peut être affiché de façon tout à fait injustifiée.
- **Falsification des contenus :** certains processus malveillants, comme certaines variantes de Bancos ou Nurech, manipulent le contenu de certains sites en y ajoutant des champs de formulaire supplémentaires, voire des pages entières. Ce faisant, les certificats SSL existants restent actifs. Sans outils spéciaux, il est impossible de savoir si ces données sont falsifiées ou non. Les données ainsi obtenues sont alors transmises à l'agresseur comme aux serveurs Web authentiques. La ses-

sion continuant normalement après le vol des données, la victime ne peut pas avoir le moindre soupçon. L'attaque ne sera constatée qu'après réception de la facture.

- Précédemment, les **hijackers de sessions** interrompaient la connexion de leurs victimes, après envoi de leurs données. Les menaces étaient alors immédiatement constatées. Mais depuis quelques temps, les sessions sont reprises de telle manière que l'auteur de l'attaque modifie les montants et les coordonnées bancaires en sa faveur (Bancos par exemple). La victime voit, elle, ses propres informations. Même le montant total du compte est falsifié en conséquence. Ici aussi, l'escroquerie ne peut être constatée que sur les relevés de compte.
- **Usurpation d'identité DNS :** comme cela a été précédemment mentionné, la possibilité d'attribuer une fausse adresse IP à un nom de domaine est de plus en plus employée. La famille logicielle malveillante QHosts utilise fréquemment le fichier hôte du répertoire comme point de départ de ses attaques C:\windows\system32\drivers\etc. Ce dossier sert à attribuer une adresse IP à un nom de domaine. Si cette opération se déroule avec succès, aucune tentative de vérification de l'adresse IP n'aura lieu. Les entrées sur le serveur DNS offrent toutefois une autre possibilité. Elles sont manipulées de telle sorte que les requêtes DNS sont redirigées sur un serveur contrôlé par l'agresseur. La plupart des sites obtiennent des résultats corrects, mais d'autres ne sont pas dans le même cas.
- **Redirecteurs :** leur redirection de données rend possible une attaque intermédiaire. Il peut s'agir d'un mandataire local ou d'un serveur mandataire contrôlé par l'auteur de l'attaque. Il est ainsi possible d'épier l'ensemble de la communication en réseau de la victime, ce qui permet de surveiller les messages électroniques, chats, pages Web visitées, données de formulaire et téléchargements de fichiers.
- **Renifleurs :** les renifleurs sont installés pour saisir le flux de données d'un réseau. La méthode d'usurpation ARP leur permet de fonctionner même sur réseau désactivé.
- **Les chevaux de Troie** espions recherchent des informations utiles dans tout le PC. Il peut s'agir d'adresses e-mail ou de fichiers au contenu particulier ou d'un certain type de fichiers. Ces données sont rassemblées et transmises à l'auteur des attaques. Les informations de connexion, clés de registre et mots de passe (ou leurs caractères de substitution) enregistrés dans le système sont une cible privilégiée de ce genre de programme. Les mots de passe pour l'accès à certaines pages Web et aux boîtes de messagerie sont enregistrés dans la zone de stockage protégée lorsque l'utilisateur accepte la possibilité d'enregistrer le mot de passe. Cette proposition souvent utilisée est affichée par le navigateur ou le fournisseur de boîte de messagerie. Il est donc judicieux de renoncer à l'enregistrement automatique des mots de passe et informations de connexion. Même les mots de passe de jeux, clés de registre de système d'exploitation et logiciels favoris, stockés à des emplacements connus du système, que ce soit des registres ou des fichiers, peuvent être usurpés.
- Un clic involontaire sur un lien peut également provoquer des pertes de données. Le **cross site scripting** permet de lire des données. C'est ainsi que le bouton « Enchérir » des enchères sur eBay a été manipulé pour que l'utilisateur accède à une page d'identification falsifiée.
- **Les cookies** sont en fait inoffensifs et indispensables pour les achats dans de nombreux sites de commerce en ligne. Ils fournissent cependant des informations importantes sur les sites que l'utilisateur consulte fréquemment. Ces informations ont une valeur élevée aux yeux des logiciels publicitaires. Les vols de cookies ne sont pas non plus inintéressants. En effet, si un utilisateur a omis de se déconnecter d'un commerce électronique ou d'un site de rencontres, le cookie accorde l'accès au profil de la victime.

Mesures de protection

Chaque menace nécessite des solutions spéciales qui doivent s'orienter en fonction de la situation concernée. Les systèmes Unified Threat Management (UTM) garantissent de solides bases de solution. Ils intègrent différentes technologies de sécurisation, comme les pare-feu, les anti-virus, les détections ou la prévention contre les intrusions dans une solution, ce qui garantit une protection intégrale. Les partisans du concept du « best of breed » achètent toujours les meilleurs composants détachés et acceptent la configuration la plus précise. Le sujet se rapproche maintenant de « l'analyse comportementale » : la technologie d'analyse comportementale représente un procédé prétendu « proactif » d'analyse anti-logiciel malveillant potentiel. Cette technologie analyse les contenus actifs (active contents) qui comportent des codes potentiellement nuisibles, en fonction du comportement de l'utilisateur dans le système de fichiers, dans le registre ou encore dans la mémoire vive de son ordinateur. Certaines solutions reposent sur des processus de sandbox, qui provoquent l'exécution de l'analyse dans un volet protégé spécifique.

Bilan des dommages

L'usurpation de données ne concerne maintenant plus seulement les espions, services secrets et terroristes. Les réseaux de cyber-délinquants ont à présent reconnu la valeur des données. En octobre 2005, des clients de la banque suédoise Nordea se sont vus proposer un outil anti-spam à télécharger gratuitement. Cela a installé une version de l'enregistreur de frappe nommé Haxdoor, qui créait un message d'erreur incitant l'utilisateur à saisir de nouveau ses codes d'accès. Après avoir constaté de nombreux comptes de clients de Nordea usurpés, la banque a fermé son portail Internet.

Les dommages causés ont coûté environ 900 000 euros. L'ampleur des dommages

causés par les usurpations de comptes en banque en ligne ne sont qu'estimables. Les banques allemandes sont restées discrètes à propos de la valeur des dommages causés. Pour 2006, BITKOM estime environ 3 250 cas d'hameçonnage, d'une valeur moyenne de 4 000 euros chacun, ce qui représente au total 13 millions d'euros, la tendance étant en hausse [5]. Au Royaume-Uni, l'information est légèrement meilleure. En 2006, l'APACS a estimé à 46,5 millions d'euros le coût des dommages survenus dans le cadre de la gestion des comptes en banque en ligne,

et à 214,6 millions d'euros les dommages dus au vol de références de cartes bancaires.

Dans le monde entier, le coût des dommages dus aux pertes de données se compte en milliards d'euros.

Ces activités malveillantes ne sont toutefois plus limitées aux données de comptes bancaires depuis longtemps. Certains logiciels espions gobent toutes les données de formulaire saisies sur les ordinateurs infectés. Sont également concernés les codes d'accès sur les forums, boîtes de messagerie électronique, sites de commerce en ligne, sites de recherche d'emploi et salons de discussions. La quantité de données ainsi saisie se mesure en téraoctets et ne peut se traiter qu'à l'aide d'un ordinateur/d'une base de données d'architecture très performante.

Dans le plus simple des cas, les données, non triées, sont revendues au noir, à 60 euros les 380 Mo.

Les codes d'accès peuvent s'utiliser pour le blanchiment d'argent ou l'envoi de spam de forum.

Les logiciels espions du type chevaux de Troie assemblent tous les documents d'un ordinateur et les renvoient à l'agresseur. Dans le cas du cheval de Troie découvert à la chancellerie allemande en août dernier, l'envoi de 160 Go sur des serveurs chinois aurait pu être évité. Même les bases de données ont fait l'objet de quelques coups majeurs. Parmi les exemples les plus connus sont inclus le site de recherche d'emploi Monster.com et le portail étudiant StudiVZ.

De nombreux cas ne sont toutefois pas d'emblée connus du public, les personnes et organismes concernés craignant de compromettre leur réputation. Ces chiffres montrent que le vol d'informations est un marché florissant.

Conclusion

Le vol et recel de données est une activité répandue dans le monde entier. Les auteurs agissent à l'échelle internationale et sur des réseaux de niveau d'organisation élevé. Au cours des dernières années, la Generation eCrime a agi sur différents niveaux infrastructurels, tactiques ou économiques. Elle bénéficie maintenant de plusieurs années d'expérience dans le l'industrie de l'eCrime. En 2008, elle acquerra certainement de nouveaux marchés et le concept de crimeware continuera de se développer.

L'introduction de solutions sécurisantes performantes, qui incluent les anti-virus, filtres anti-hameçonnage, pare-feu et filtres anti-spam, devrait devenir obligatoire pour tous les utilisateurs. Toutefois, un sondage de G DATA Security datant de février 2008 montre que les utilisateurs ne prennent toujours pas tous ce problème au sérieux : 47 % des utilisateurs Windows interrogés parcourent Internet sans protection, 73 % d'entre eux gérant leur compte en banque sur Internet. Cette négligence de prendre au sérieux la protection des données et le niveau d'information pauvre sur la méthode des cyber-délinquants facilite malheureusement l'exercice en masse des activités douteuses de l'industrie de l'eCrime.