



G Data Communiqué de presse 2009

Sécurité, quelle perspective pour 2010 ?



Paris, le 23 décembre 2009 – Ces dernières années le cybercrime s’est organisé en un marché parallèle établi. Une professionnalisation qui explique en partie le nombre croissant de nouveaux malware apparus en 2009 : une partie des bénéficiaires est investie afin d’améliorer l’infrastructure et les nouvelles techniques d’attaque. Dans cette perspective, il y a peu d’espoir d’une amélioration en 2010. Prudence des utilisateurs et réactivité des acteurs de la sécurité informatique restent donc les maîtres mots.

G Data profite de cette fin d’année pour livrer son analyse des futures tendances possibles en terme de sécurité :

- Les applications du Web 2.0 seront la cible d’attaques variées
- Le nombre de sites Web intégrant des logiciels malveillants progressera
- Bien que moins axé sur les banques, l’hameçonnage restera une source de collecte de données et d’argent de premier ordre.
- Windows 7 sera la nouvelle cible des attaques
- Des rootkits plus complexes feront leur apparition
- L’expansion des services de Cloud Computing attirera de plus en plus de cybercriminels

Réseaux sociaux au coeur des attaques

Le Web 2.0 offre à l’internaute beaucoup de nouvelles possibilités. En utilisant la technologie AJAX (javascript asynchrone et XML), les pages Web ne doivent plus être recrées après chaque clic parce qu’un flux de données constant fournit l’information nécessaire. Malheureusement, ce mécanisme offre également une série de points d’attaque. Comme les programmes de bureau, les applications Web ne sont également pas exemptes d’erreurs de programmation qui peuvent être employées pour déployer des malware. Depuis le début de l’année, le ver Internet Koobface a fait une utilisation intensive de Facebook, MySpace et de beaucoup d’autres réseaux sociaux pour se propager à des contacts sains. Le potentiel de propagation de ce type de malware augmentera encore dans l’année à venir.

Les serveurs Web de plus en plus ciblés

Jamais autant d’infections n’ont eu lieu par l’intermédiaire de sites Web compromis. Les sites avec des mots de passe faibles ou des failles de sécurité dans leurs applications Web sont automatiquement tracés et compromis. Une fois que les attaquants ont créé l’accès au serveur web, ils peuvent l’employer pour y mettre à disposition des malware en téléchargement. Mais bien plus inquiétantes sont les attaques dites en drive-by-download. Elles exploitent des failles de sécurité dans les navigateurs de sorte que l’ordinateur puisse être infecté à l’insu de l’utilisateur. Beaucoup de sites Web faiblement défendus seront à l’avenir visés par ce type d’attaque.



Vol de données et hameçonnage

Le nombre d'incidents de vol de données augmente sans interruption. Pendant l'année, des banques ont dû remplacer des cartes de crédit de clients qui avaient subi des vols de données bancaires. L'hameçonnage classique n'en est pas la seule cause. Des données sont aussi rassemblées en utilisant des spywares ou des Troyens enregistreurs de frappes. De nouvelles techniques qui tendent à dépasser l'hameçonnage classique. Les destinataires d'un message d'hameçonnage sont de plus en plus rares à accepter de saisir leurs données d'accès. Les banques ont aussi multiplié les protections pour limiter les risques. Certains services comme PayPal restent encore des exceptions : ils exigent seulement un nom et un mot de passe pour l'accès aux comptes. L'utilisation de mesures de protection étendues est d'une manière générale trop peu utilisée. Beaucoup de services Internet se contentent d'une protection d'accès par nom et mot de passe. Les comptes de courrier électronique (Hotmail, Yahoo, Google), les réseaux sociaux (Facebook, Twitter, MySpace), les enchères en ligne (eBay) et les jeux sur Internet (WoW) sont devenus des cibles fréquentes. Des attaques qui portent la marque de la cyberdélinquance et du marché parallèle :

- Les comptes de courrier électronique publics volés permettent de passer à travers les filtres anti-spam.
- Les comptes et les données issus de réseaux sociaux sont utilisés pour la réalisation d'attaque ciblée.
- Les comptes et les objets extraits de jeux sur Internet sont vendus avec de faux comptes ebay.

L'hameçonnage n'est pas la seule source de collecte de données. L'information offerte sur des sites Internet publics et sur les réseaux sociaux au sujet des entreprises et de leurs employés peut aussi être utilisée pour des attaques ciblées. Appelées "spear-phishing", ces méthodes d'attaque se multiplient. Par exemple, un directeur d'entreprise peut recevoir un email prenant la forme d'une proposition commerciale dont la pièce jointe est un PDF modifié nommé "Offre.pdf". Un fichier compromis qui infecte le PC une fois ouvert.

Que ce soit pour la revente ou l'utilisation dans le cadre d'attaque, la collecte de données restera un des points importants en 2010.

Windows 7, nouvelle cible

Avec Windows 7, Microsoft a en grande partie surmonté les problèmes de Vista. Depuis son introduction du marché en octobre 2009, seulement quelques voix critiques ont été entendues et il est tout à fait évident que Windows 7 trouvera son chemin sur des ordinateurs des clients. Malheureusement en voulant faciliter l'utilisation des outils de sécurité de Windows 7, Microsoft a ouvert quelques portes jusque-là fermées par Vista. Il est assez probable que les malware utilisent ces portes laissées ouvertes par les utilisateurs. Les premières attaques de scareware reprenant le design de Windows 7 ont déjà été détectées.

Cyberattaque : les nouveaux chemins empruntés

La plupart des malware cherchent à se cacher des outils de détection. Une des tactiques est de devenir actif dans le système avant l'antivirus. Par conséquent, le secteur de boot est une cible intéressante. Des rootkits résident ainsi dans le secteur de boot du disque dur et sont ainsi chargés longtemps avant la protection du système d'exploitation et de l'antivirus. En 2010, les malwares pourraient aller encore plus loin. Alors que les rootkit de MBR (Master Boot Record) étaient encore jusqu'à peu réservés à des démonstrations en laboratoire, ils font maintenant partie de quelques familles largement distribuées de virus. Les prochaines générations sont déjà dans les starting-blocks. De nouveaux malware qui utilisent des failles de sécurité dans des composants matériels pourraient ainsi voir rapidement le jour.



Une autre nouveauté est à prévoir du côté des malware afin de répondre à la nouvelle tendance de la virtualisation. Virtualiser des logiciels, des systèmes d'exploitation et du matériel est maintenant rendu possible par les progrès des unités de calcul. Utiliser des machines virtuelles devient toujours plus facile et plus efficace. Les environnements isolés donnent de nouvelles occasions de protéger l'ordinateur et ses données. Les attaquants vont réagir face à ces nouvelles parades et nous nous attendons à l'apparition de malware qui attaquent les programmes les plus populaires de virtualisation.

CloudComputing et sécurité

Très à la mode, déporter sur des serveurs externes le stockage ou le traitement de données comporte toutefois des risques. Dans bien des cas, la sensibilité des données déportées n'est souvent pas suffisamment considérée. En contaminant ce type de prestataire, un malware peut alors accéder aux données de multiples entreprises.

Les risques sont similaires pour les particuliers. En externalisant le traitement ou le stockage d'images, de texte et de feuilles de calculs sur des serveurs en ligne anonyme, l'utilisateur s'expose à des pertes ou des vols de données.

D'une manière plus générale, plus les entreprises et les individus se servent des services de Cloud, plus de telles plates-formes deviennent attrayantes pour des attaques potentielles. Il est probable que l'année fournisse le premier cas sérieux.

La cyberguerre continue

Beaucoup d'internautes se sont habitués aux inconvénients d'Internet : spam, ver, hameçonnage, etc. Il ne faut pas pour autant se contenter de cette situation. Les solutions existent pour combattre efficacement cette économie parallèle. Un des meilleurs exemples reste McColo : fin 2008, lorsque les serveurs de cette société ont été fermés, le volume mondial de Spam est tombé d'un tiers du jour au lendemain et il a fallu plusieurs mois pour qu'il atteigne à nouveau son niveau le plus haut. Les initiatives et les coopérations se multiplient afin de bloquer l'infrastructure des cybercriminels - particulièrement les Botnets. Ces réseaux d'ordinateurs zombie sont dans 80% des cas des ordinateurs de particuliers. Malheureusement, beaucoup d'utilisateurs ne comprennent pas les conséquences de l'infection de leur machine pour les autres internautes, mais aussi pour la santé de l'ensemble du réseau. Espérons que l'année à venir verra les internautes, les forces de l'ordre et les spécialistes en sécurité IT travailler main dans la main.

Pour toute question ou demande de visuels :

Jérôme Granger - G Data Software AG

Tél. : 01 41 48 51 46 – mob. 06 08 77 32 26 – e-mail : jerome.granger@gdata.fr