

**G-Data : Armageddon numérique pour l'année 2010**

**Sécurité**

Posté par : JerryG

Publié le : 4/1/2010 0:00:00

L'Apocalypse est le dernier livre de la Bible chrétienne. On attribue traditionnellement sa composition à l'évangéliste Jean, en cette année de l'an de grâce 2010, G-Data joue son tour le prophète d'un apocalypse numérique. **Sécurité, quelle perspective pour 2010 ? De Windows 7 à la Cyberguerre.**

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 bénéfices 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 activité des acteurs de la sécurité informatique restent donc les meilleurs 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 cœur 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 ˆtre recrã©es aprã©s chaque clic parce qu'un flux de donnã©es constant fournit l'information nã©cessaire. Malheureusement, ce mã©canisme offre ˆgalement une sã©rie de points d'attaque. Comme les programmes de bureau, les applications Web ne sont ˆgalement pas exemptes d'erreurs de programmation qui peuvent ˆtre employã©es pour dã©ployer des malware. Depuis le dã©but de l'annã©e, le ver Internet Koobface a fait une utilisation intensive de Facebook, MySpace et de beaucoup d'autres rã©seaux sociaux pour se propager ˆ des contacts sains. Le potentiel de propagation de ce type de malware augmentera encore dans l'annã©e ˆ venir.

### Les serveurs Web de plus en plus ciblã©s

Jamais autant d'infections n'ont eu lieu par l'intermã©diaire de sites Web compromis. Les sites avec des mots de passe faibles ou des failles de sã©curitã© dans leurs applications Web sont automatiquement tracã©s et compromis. Une fois que les attaquants ont crã©ã© l'accã©s au serveur web, ils peuvent l'employer pour y mettre ˆ disposition des malware en tã©lã©chargement. Mais bien plus inquiã©tantes sont les attaques dites en drive-by-download. Elles exploitent des failles de sã©curitã© dans les navigateurs de sorte que l'ordinateur puisse ˆtre infectã© ˆ l'insu de l'utilisateur. Beaucoup de sites Web faiblement dã©fendus seront ˆ l'avenir visã©s par ce type d'attaque.

### Vol de donnã©es et hameã©sonnage

Le nombre d'incidents de vol de donnã©es augmente sans interruption. Pendant l'annã©e, des banques ont dã© remplacer des cartes de crã©dit de clients qui avaient subi des vols de donnã©es bancaires. L'hameã©sonnage classique n'en est pas la seule cause. Des donnã©es sont aussi rassemblã©es en utilisant des spywares ou des Troyens enregistreurs de frappes. De nouvelles techniques qui tendent ˆ dã©passer l'hameã©sonnage classique. Les destinataires d'un message d'hameã©sonnage sont de plus en plus rares ˆ accepter de saisir leurs donnã©es d'accã©s. Les banques ont aussi multipliã© 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'accã©s aux comptes. L'utilisation de mesures de protection ˆtendues est dã©une maniã©re gã©nã©rale trop peu utilisã©e. Beaucoup de services Internet se contentent d'une protection d'accã©s par nom et mot de passe. Les comptes de courrier ˆlectronique (Hotmail, Yahoo, Google), les rã©seaux sociaux (Facebook, Twitter, MySpace), les enchã©res en ligne (eBay) et les jeux sur Internet (WoW) sont devenus des cibles frã©quentes.

### Des attaques qui portent la marque de la cyberdã©linquance et du marchã© parallã©le :

ˆ Les comptes de courrier ˆlectronique publics volã©s permettent de passer ˆ travers les filtres antispam.

ˆ Les comptes et les donnã©es issus de rã©seaux sociaux sont utilisã©s pour la rã©alisation d'attaques ciblã©es.

ˆ Les comptes et les objets extraits de jeux sur Internet sont vendus avec de faux comptes ebay.

L'hameã©sonnage n'est pas la seule source de collecte de donnã©es. L'information offerte sur des sites Internet publics et sur les rã©seaux sociaux au sujet des entreprises et de leurs employã©s peut aussi ˆtre utilisã©e pour des attaques ciblã©es. Appelã©es ˆ spear-phishing, ces mã©thodes d'attaque se multiplient. Par exemple, un directeur

Une entreprise peut recevoir un email prenant la forme d'une proposition commerciale dont la piÃ©ce jointe est un PDF modifiÃ© nommÃ© "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'une attaque, la collecte de donnÃ©es restera un des points importants en 2010.

### Windows 7, nouvelle cible

Avec Windows 7, Microsoft a en grande partie surmontÃ© les problÃ©mes de Vista. Depuis son introduction du marchÃ© en octobre 2009, seulement quelques voix critiques ont Ã©tÃ© entendues et il est tout Ã©vident que Windows 7 trouvera son chemin sur des ordinateurs des clients. Malheureusement en voulant faciliter l'utilisation des outils de sÃ©curitÃ© de Windows 7, Microsoft a ouvert quelques portes jusque-lÃ© fermÃ©es par Vista. Il est assez probable que les malware utilisent ces portes laissÃ©es ouvertes par les utilisateurs. Les premiÃ©res attaques de scareware reprenant le design de Windows 7 ont dÃ©jÃ© Ã©tÃ© dÃ©tectÃ©es.

### Cyberattaque : les nouveaux chemins empruntÃ©s

La plupart des malware cherchent Ã© se cacher des outils de dÃ©tection. Une des tactiques est de devenir actif dans le systÃ©me avant l'antivirus. Par consÃ©quent, le secteur de boot est une cible intÃ©ressante. Des rootkits rÃ©sident ainsi dans le secteur de boot du disque dur et sont ainsi chargÃ©s longtemps avant la protection du systÃ©me d'exploitation et de l'antivirus. En 2010, les malware pourraient aller encore plus loin. Alors que les rootkits de MBR (Master Boot Record) Ã©taient encore jusqu'Ã© peu rÃ©servÃ©s Ã© des dÃ©monstrations en laboratoire, ils font maintenant partie de quelques familles largement distribuÃ©es de virus. Les prochaines gÃ©nÃ©rations sont dÃ©jÃ© dans les starting-blocks. De nouveaux malware qui utilisent des failles de sÃ©curitÃ© dans des composants matÃ©riels pourraient ainsi voir rapidement le jour. Une autre nouveautÃ© est Ã© prÃ©voir du cÃ©tÃ© des malware afin de rÃ©pondre Ã© la nouvelle tendance de la virtualisation. Virtualiser des logiciels, des systÃ©mes d'exploitation et du matÃ©riel est maintenant rendu possible par les progrÃ©s des unitÃ©s de calcul. Utiliser des machines virtuelles devient toujours plus facile et plus efficace. Les environnements isolÃ©s donnent de nouvelles occasions de protÃ©ger l'ordinateur et ses donnÃ©es. Les attaquants vont rÃ©agir face Ã© ces nouvelles parades et nous nous attendons Ã© l'apparition de malware qui attaquent les programmes les plus populaires de virtualisation.

### Cloud Computing et sÃ©curitÃ©

TrÃ©s Ã© la mode, dÃ©porter sur des serveurs externes le stockage ou le traitement de donnÃ©es comporte toutefois des risques. Dans bien des cas, la sensibilitÃ© des donnÃ©es dÃ©portÃ©es n'est souvent pas suffisamment considÃ©rÃ©e. En contaminant ce type de prestataire, un malware peut alors accÃ©der aux donnÃ©es 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 Ã© des pertes ou des vols de donnÃ©es.

DÃ©une maniÃ©re plus gÃ©nÃ©rale, 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'annÃ©e fournisse le premier cas sÃ©rieux.

### La cyberguerre continue

Beaucoup d'internautes se sont habituÃ©s aux inconvÃ©nients d'Internet : spam, ver, hameÃ§onnage, 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.