# La cybercriminalité en forte hausse : tous aux abris !

De 10 à 1000 dollars les coordonnées Internet de comptes bancaires, avec remises sur volume, de 40 centimes à 20 dollars pour des cartes bancaires, de 1 à 15 dollars pour des identités complètes… le marché des informations volées se porte bien sur le Web. Certains sites –forcément provisoire- proposent même des échanges en cas de non-satisfaction sur la marchandise. Cela dit, comment poursuivre de tels vendeurs en cas d'insatisfaction ?

Ces quelques chiffres issus de la dernière édition du rapport sur les menaces à la sécurité Internet de Symantec (Internet Security Threat Report – Volume XIII-) portant sur la période juillet-décembre 2007, ne sont que partie la partie émergée de l'iceberg, véritable délice des paranoïaques en manque de pessimisme.

Pour un peu, ces constatations nous pousseraient à ne plus sortir de son PC, même avec une armure blindée à l'antivirus-antimalware-antirootkit-antitout… mais pas antirouille.

**Symantec traque les cybermalfrats sur toute la planète**

Comme le précise Paul Dominjon, responsable des solutions Banques et Assurances chez Symantec : «*Ce rapport permet de prendre le pouls de la menace sur Internet, et devient un support de référence chez Symantec.*»En effet, l'éditeur couvre quatre continents avec ses centres de sécurité, au sein desquels il analyse les informations collectées. Par exemple, Symantec revendique l'analyse de 20 % du trafic e-mail mondial, et a référencé 25.000 vulnérabilités. Les résultats de ce rapport reposent sur la mesure de l'activité d'après 40.000 senseurs dispatchés dans 180 pays. *« Notre objectif initial consiste à détecter au plus vite les attaques ou les menaces pour alerter, créer un remède, et l'intégrer au plus vite à nos solutions. Parfois ces attaques sont communiquées par nos clients, »*explique Paul Dominjon.

**Underground Economy Outsourcing, Pricing Flexibility**

Source : Symantec

| Current Rank | Previous Rank | Goods and Services | Current Percentage | Previous Percentage | Range of Prices |
|---|---|---|---|---|---|
| 1 | 2 | Bank accounts | 22% | 21% | $10–$1000 |
| 2 | 1 | Credit cards | 13% | 22% | $0.40–$20 |
| 3 | 7 | Full identities | 9% | 6% | $1–$15 |
| 4 | N/A | eBay accounts | 7% | N/A | $1–$8 |
| 5 | 8 | Scams | 7% | 6% | $2.50/week–$50/week for hosting, $25 for design |
| 6 | 4 | Mailers | 6% | 8% | $1–$10 |
| 7 | 5 | Email addresses | 5% | 6% | $0.83/MB–$10/MB |
| 8 | 3 | Email passwords | 5% | 8% | $4–$30 |
| 9 | N/A | Drop (request or offer) | 5% | N/A | 10%–50% of total drop amount |
| 10 | 6 | Proxies | 5% | 6% | $1.50–$30 |

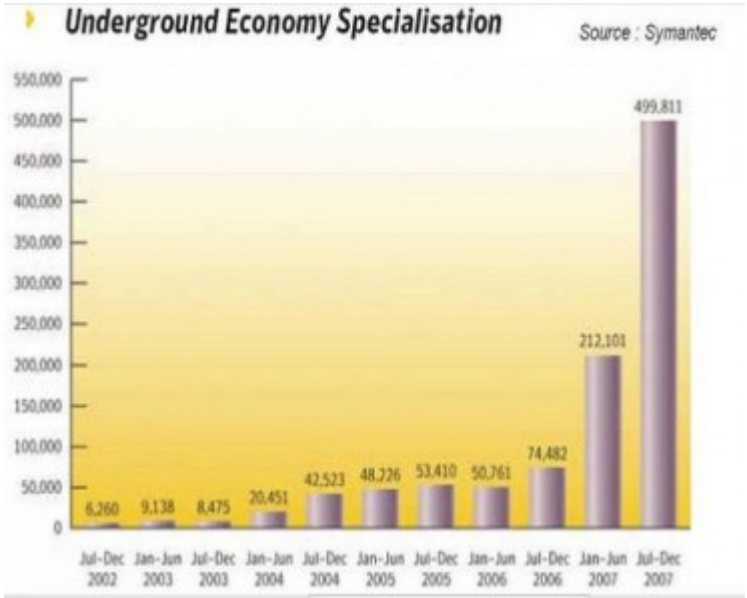
Les quatre tendances majeures : les serveurs Web sont redevenus le point central des attaques, les

menaces ciblent plutôt l'utilisateur et ses informations que sa machine, l'économie du cybercrime se consolide, et les différents modèles et techniques d'attaques des codes malicieux évoluent compliquant la tâche des solutions de protection. *« On remarque une spécialisation des cyberdélinquants, via une segmentation des offres : vente de numéros de carte de crédit, vente de coordonnées bancaires, de profils d'utilisateurs plus ou moins détaillés. Le tout proposé à divers tarifs sous forme de catalogues,»*ajoute Paul Dominjon.

**Tout augmente : vulnérabilités, malwares, phishing et spam**

*« Sur les six mois étudiés, 11.253 vulnérabilités propres à des sites ou à du cross-site scripting ont été documentées par Symantec. Bien au-delà des 2.134 vulnérabilités traditionnelles recensées pendant la même période, »* explique le rapport. Les attaques massives basées sur une diffusion globale ont cédé la place aux techniques furtives ciblées visant chaque PC via le Web. Les réseaux d'entreprise fortifiés nécessitent plus d'effort et savent mieux réagir. Le Web devient donc à nouveau le canal de prédilection cybercriminels.

Victime de choix : les sites communautaires ou réseaux sociaux auxquels, pour des raisons qui dépassent l'entendement, les internautes et employés accordent leur confiance. Ah émotion quand tu nous tiens ! Parler de soi et de sa cour virtuelle peut rendre… peu raisonnable. *« Bien entendu, le nombre et la qualité des informations sur un membre de ces sites permettent aux pirates de se constituer des fichiers très qualifiés, »*souligne Paul Dominjon. *« Par la suite, il leur est facile de lancer des attaques massives qui se propagent aux réseaux sociaux des victimes. »*




Toujours sur le second semestre 2007, Symantec a détecté 499.811 nouveaux programmes malveillants, soit une augmentation de 571 % par rapport à 2006. L'éditeur a recensé 711.912 nouvelles menaces au cours de l'année 2007 (en hausse de 468 % en un an) pour un total de 1.122.311 à la fin de l'année 2007.

Autre tendance forte soulignée par le rapport : *« Le réseau Symantec Probe Network a détecté au total 207 547 messages uniques de phishing, soit une augmentation de 5 % par rapport au premier semestre 2007. Ramené à la journée, ce chiffre correspond à une moyenne de 1.134 messages uniques de phishing par*

*jour. »*

Enfin, les spams sont aussi de la fête, et représentent 71 % des e-mails contrôlés, soit une hausse de 16 % à 2006 (61 %).

**Les banques dans l'œil du cyclone**

Symantec relève que les données d'identité, les cartes de crédit et autres coordonnées bancaires représentent 44 % des marchandises disponibles sur les serveurs des cybercriminels. Bien sûr, les comptes bancaires mènent la danse "en tête de gondole" pour 22 % des marchandises disponibles, un chiffre en légère augmentation par rapport au premier semestre 2007 où ils atteignaient 21 %. De plus, le nombre d'infections potentielles des systèmes bancaires par des chevaux de Troie est en augmentation de 86 % générant une logique recrudescence des vols de coordonnées bancaires et de leur vente sur les serveurs susmentionnés.

Réseaux sociaux, comptes bancaires, profils e-bay… Sortez couverts et mettez au moins à jour vos anti-quelque-chose. Sinon, à quoi bon que votre éditeur se décarcasse. Dans ces situations, les pirates limitent toujours leurs efforts aux cibles plus faciles.