



BOTNETS ET MALWARE

Il existerait selon Nicolas Woïrhaye, directeur du département CERT-LEXSI, 6 grands réseaux mondiaux de cybercriminalité agissant sur l'Internet. D'après lui, «*Le phénomène de la cybercriminalité s'internationalise et se structure en réseaux fonctionnels interdépendants*». Alors qu'il y a à peine 3 ans la cybercriminalité était peu professionnelle, relativement atomisée et concentrée sur quelques activités de type intrusion, virus ou pédophilie, «*Le phénomène s'est développé de manière exponentielle*». D'après lui, «*Les fraudeurs agissent en réseaux et en organisations hiérarchisées*» en s'attaquant en masse aux victimes internautes. Leurs 2 principales armes sont les **botnets** (réseaux puissants d'ordinateurs domestiques transformés en «zombie» et contrôlés à distance grâce à un virus) et les **malware** (programmes nuisibles tels que les trojans, backdoors, Vers..).

D'après les experts, il y aurait dans le monde des millions d'ordinateurs zombies dont la mise en réseaux (botnets) par groupe de 10 000 à 30 000 se loue à partir de 100 dollars l'heure. Leur utilisation favoriserait le développement du spamming et du phishing (fausse identité bancaire) mais aussi les attaques ciblées pour paralyser des sites web professionnels (casinos, banques...). D'après les experts de LEXSI, la réalisation des botnets serait surtout le fait de jeunes peu payés et travaillant sans le savoir vraiment pour des organisations quasi mafieuses, même s'il n'existe pas ou peu de liens apparents entre les organisations criminelles traditionnelles et ces nouveaux réseaux de cybercriminalité.

• **Les 6 grands réseaux de cybercriminalité :**

- Anglophones
- Asiatiques
- Brésiliens
- Djihadistes
- Russophones
- Sub-saharien

• **Principales activités de cybercriminalité par ordre décroissant :**

- Collecte d'identifiants bancaires
- Monétisation d'identifiants et blanchiment de fonds
- Vente de produits contrefaits (luxe, médicaments)
- Développement de malware
- Location, vente de botnets
- Arnaque de type Nigériane ou sur actions boursières
- Vente de faux papiers d'identité
- Intrusion ou «défacement» de sites commerçants
- Vente de bases de données d'email spécialisées
- Gestion de sites de jeux en ligne
- Monétisation de contenus photographiques

Source : Groupe LEXSI