

## Votre ordinateur, un zombie ?

Pour plus de sécurité, adoptez les réflexes CASES !

### Des ordinateurs sont piratés à des fins criminelles

Les criminels profitent de l'anonymat d'Internet pour mettre le grappin sur les ordinateurs d'utilisateurs inconscients. Ils peuvent ainsi se servir des ordinateurs pour leurs méfaits. L'ampleur des activités douteuses est énorme. Des estimations font état de plusieurs milliards d'euros par an. Le but des criminels est de contrôler à distance un ordinateur privé sans se faire prendre. Les ordinateurs infectés sont reliés par les pirates en « réseaux de machines zombies » ou botnets pour commander des attaques de grande ampleur ou diffuser des spams.

Internet n'est pas utilisé que par des personnes dotées de bonnes intentions. Des criminels piratent le réseau informatique international, s'armant ainsi en secret d'un droit souverain sur les ordinateurs d'utilisateurs privés. Ils infectent des ordinateurs pour les contrôler à distance. Mieux encore, ils rassemblent les machines infectées en un réseau de machines zombies, ou botnet. Ces réseaux permettent aux pirates d'avoir des puissances de calcul élevées et leur offrent donc de toutes nouvelles possibilités d'attaque.

Le propriétaire de l'ordinateur ne sait pas que sa machine est entre de mauvaises mains, ce qui s'explique aisément : de plus en plus d'utilisateurs disposent d'une connexion Internet haut débit. Par conséquent, il n'est pas rare que les ordinateurs restent connectés 24 heures sur 24 à Internet. Ceci est facilité par des tarifs forfaitaires de plus en plus abordables. De plus, grâce à la rapidité des lignes DSL, les ordinateurs actuels ralentissent à peine lorsqu'ils exécutent les



MINISTÈRE DE L'ÉCONOMIE  
ET DU COMMERCE EXTÉRIEUR  
Direction du Commerce électronique  
et de la Sécurité informatique

commandes des pirates à l'insu de leur propriétaire.

### Comment apparaît un réseau de machines zombies ?

Ce réseau s'appelle botnet en anglais. Le nom bot vient de « robot ». Dans le monde numérique, bot désigne un programme qui peut être contrôlé à distance. Les criminels se servent de tels programmes pour prendre le contrôle d'ordinateurs privés.

Il existe plusieurs manières d'infecter un ordinateur privé par un programme malveillant qui permettra aux criminels de prendre le contrôle de la machine. Lors de la consultation de sites Internet, des programmes malveillants peuvent être téléchargés par des scripts ou des contenus multimédias sur un ordinateur non protégé. Des failles de sécurité sont alors exploitées. L'installation d'un bot sur un ordinateur personnel peut aussi se faire par l'ouverture d'e-mails d'origine inconnue et de leurs pièces jointes contenant des virus ou chevaux de Troie. Si les ordinateurs infectés sont reliés entre eux, un botnet ou réseau de machines zombies est créé. Ces réseaux comptent généralement au

moins quelques milliers d'ordinateurs, commandés à distance.

### 2/3 des infections se font par le navigateur :

Selon des études de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), la majorité des infections se font par les points faibles des navigateurs web comme Internet Explorer, Firefox ou Opera. Cette voie d'entrée représente 65 % des infections par bot. La deuxième cause (13 %) est l'installation de programmes malveillants par des pièces jointes d'e-mails. Les autres sources d'infection sont les failles de sécurité des systèmes d'exploitation (11 %) et le téléchargement de fichiers infectés d'Internet (9 %).

Un botnet créé est souvent revendu à des tiers. Le 14 mars 2009, la chaîne de télévision britannique BBC a montré comment des rédacteurs avaient pu acheter un botnet de 22 000 ordinateurs infectés. Le

logiciel de contrôle fourni et simple d'utilisation leur a permis de prendre les commandes des ordinateurs infectés du botnet.

Des pirates peuvent ainsi activer un botnet par simple pression d'une touche. Le propriétaire de la machine n'a plus qu'un « ordinateur zombie ». L'ordinateur devient le maillon involontaire d'une association virtuelle contrôlée par des pirates. Un seul pirate suffit pour diriger tous les programmes d'un botnet.

Les propriétaires de ces ordinateurs doivent être conscients que leur machine n'est pas seulement victime d'une telle attaque mais qu'elle en devient aussi l'auteur. Cela signifie pour le propriétaire qu'il se rend complice d'actes criminels s'il ne peut pas prouver que son ordinateur était équipé des mesures de protection nécessaires.

### Dangers représentés par les botnets

Les ordinateurs infectés par un bot sont utilisés pour exécuter les actes criminels les plus divers. La réunion des ordinateurs zombies en botnet assure aux criminels une puissance de calcul supérieure. En outre, ceux-ci peuvent se cacher derrière des ordinateurs de tiers. Un botnet permet par exemple de voler des noms d'utilisateur et des mots de passe ou d'envoyer des spams. Il peut ainsi propager plusieurs millions de spams par minute sur Internet. D'autres malveillances peuvent aussi être pratiquées comme la lecture d'informations bancaires et des données de cartes de crédit. Selon les estimations, plus de six millions d'ordinateurs dans le monde sont regroupés en botnets les plus divers. Les cinq pays comptant le plus d'ordinateurs infectés sont la Chine, l'Allemagne, la France, l'Espagne et les États-Unis.

Mais les botnets ne sont plus depuis longtemps de simples usines à diffuser les spams. Ils sont la plus grosse activité des cybercriminels bien organisés. Entretemps, les organisations professionnelles se cachent derrière les réseaux. Il y a quelques années, elles ont reconnu à quel point il est facile d'utiliser Internet pour des escroqueries en ligne.

Ces organisations criminelles n'ont pas lésiné sur les moyens. Elles ont appris à tirer parti des faiblesses

d'Internet, des ordinateurs privés, de l'ignorance des propriétaires et de l'absence de réflexes de protection des utilisateurs. Les pirates engagent des développeurs de logiciels et achètent l'infrastructure nécessaire pour optimiser leurs activités criminelles. Ensuite, l'argent dérobé est blanchi via des hommes de paille et leur propre identité est dissimulée.

### Conseil de sécurité : règles d'or de la sécurité informatique

La première mesure de protection consiste à créer un compte utilisateur avec des droits limités. Si l'utilisateur surfe sur Internet comme administrateur, l'attaquant a tous les droits sur le système informatique pour faire encore plus de dégâts.

Sans l'installation et la mise à jour régulière d'un antivirus et d'un programme anti-spyware, deux programmes indispensables, surfer sur Internet représente un grand risque pour la sécurité. Un pare-feu installé et bien configuré est incontournable pour se protéger des bots. En cas d'infection, il bloque l'envoi incontrôlé de données par l'ordinateur.

La mise à jour du système d'exploitation et d'autres programmes courants comme le navigateur Internet est aussi très importante pour combler les failles de sécurité connues.

Ne jamais ouvrir les e-mails avec pièce jointe d'origine inconnue mais les effacer immédiatement ! La prudence est aussi de rigueur lors du téléchargement de fichiers d'Internet. Il faut aussi éviter de consulter des sites douteux.

De plus en plus souvent, les bots entrent dans un système informatique via des contenus multimédias et actifs en exploitant les failles de sécurité des versions logicielles plus anciennes. Il est donc capital de mettre régulièrement à jour les applications comme Flash Player et PDF Reader. Le risque d'infection peut en outre être réduit en désactivant « Contenus actifs » dans le navigateur.

Le portail [www.cases.lu](http://www.cases.lu) décrit en détail l'application des différentes mesures de protection.

Des études indiquent que les escroqueries en ligne sont trois fois plus importantes que les escroqueries non virtuelles. Par exemple, en 2007, Google a analysé 4,5 millions de sites Internet dont 10 % étaient pourvus de codes nuisibles.

Les botnets représentent un danger non seulement pour les utilisateurs privés mais aussi de plus en plus pour les gouvernements, l'industrie et beaucoup d'entreprises. Les grosses structures sont de plus en plus ciblées par les attaques criminelles. Celles-ci peuvent aboutir à ce que des États ou entreprises soient contraints de retirer des branches de services complètes du réseau.

### Se protéger par des réflexes de sécurité

Depuis un certain temps, de nombreux prestataires de services Internet s'attellent à modifier leur infrastructure pour être moins la cible de botnets. C'est à cet instant que chaque internaute entre en scène. Il est souvent un maillon faible de la chaîne de mesures de protection et donc la victime privilégiée de cybercriminels. C'est surtout grâce à son manque de connaissances et à ses négligences que les botnets sont possibles.

Tout le monde devrait protéger son système informatique pour que des tiers n'aient pas la possibilité de mettre la main sur l'ordinateur et de l'utiliser à mauvais escient. Les utilisateurs non informés et imprudents sont les maillons les plus faibles et la cible préférée des attaques. Tout d'abord, les criminels dénichent des utilisateurs et des systèmes informatiques non protégés. Ils profitent ensuite surtout des faiblesses des systèmes d'exploitation et programmes obsolètes pour infecter l'ordinateur et en prendre le contrôle. Un ordinateur dont les programmes ne sont pas mis à jour régulièrement est la cible d'attaques après à peine quelques minutes de surf sur Internet.

Certes, il est impossible d'exclure totalement l'infection d'un ordinateur par un bot mais la simple application de réflexes de protection permet de réduire nettement le risque d'infection. Tout comme boucler sa ceinture de sécurité en voiture, les réflexes de protection sont faciles à mettre en œuvre pour chaque utilisateur et indispensables à l'heure actuelle.