



## Économie des réseaux de PC zombies

Yuri Namestnikov



KASPERSKY Lab

Comment les propriétaires de réseaux de PC zombies gagnent-ils de l'argent ?	5
Attaques par déni de service distribué	5
Collecte d'informations confidentielles	6
Hameçonnage	8
Courrier indésirable	9
Courrier indésirable de recherche	9
Installation de logiciels publicitaires et de programmes malveillants	10
Augmentation du nombre de clics	11
Location et vente de réseaux zombies	11
Conclusion	12

Les réseaux de PC zombies ont considérablement évolué ces 10 dernières années. De quelques dizaines d'ordinateurs, gérés depuis des centres de commandes, ils sont passés à des millions de machines constituant des réseaux complexes et dotés d'une administration décentralisée. Quel est l'intérêt de créer de si grands réseaux de zombies ? Une seule réponse : l'appât du gain.

Un réseau de PC zombies, ou botnet, est un réseau d'ordinateurs infectés par un programme malveillant, qui permet à des individus mal intentionnés d'administrer ces ordinateurs à l'insu de leur propriétaire. Les réseaux de zombies représentent désormais une source de revenus stables pour un grand nombre de bandes cyber-criminelles. Le faible coût de production et la simplicité de l'administration des réseaux de PC zombies contribuent à leur popularité, et expliquent leur augmentation.

De nombreuses possibilités s'offrent aux individus qui souhaitent exploiter un réseau de zombies, du cybercriminel expérimenté au moins qualifié. Il est possible de monter de toutes pièces un réseau de zombies, les instructions nécessaires à leur création se trouvant facilement sur Internet.

Pour mettre sur pied un nouveau réseau de PC zombies, le cybercriminel peut infecter les ordinateurs des victimes à l'aide d'un programme spécial baptisé « bot ». Les bots sont des programmes malveillants qui regroupent les ordinateurs infectés au sein des réseaux de zombies.

Les moins doués pour la programmation peuvent tout simplement acquérir des réseaux de PC zombies, commercialisés sur certains forums. Les acheteurs peuvent demander l'obscurcissement (l'obscurcissement est une pratique qui consiste à brouiller le code en vue de compliquer la détection par les logiciels antivirus) et le chiffrement du code de leurs programmes, afin qu'ils ne puissent être découverts par les logiciels antivirus.

Le cybercriminel peut également choisir de détourner un réseau de PC zombies existant.

L'étape suivante pour le cybercriminel consiste à infecter les ordinateurs des victimes à l'aide de programmes malveillants. Il peut pour cela avoir recours à l'envoi de courriers non sollicités, à la diffusion de messages dans les forums ou sur les réseaux sociaux, ou encore au téléchargement à la dérobée. Le bot peut lui-même développer des fonctions de diffusion automatique, comme n'importe quel virus ou vers.

Diverses astuces d'ingénierie sociales sont exploitées lors de la diffusion de messages non sollicités ou de la publication de messages sur des forums ou des réseaux sociaux, afin de pousser la victime potentielle à installer le bot. Il peut s'agir d'une invitation à regarder une vidéo intéressante qui requiert un codec spécial. Une fois ce codec téléchargé et exécuté, l'ordinateur est infecté à l'insu de son utilisateur. Il devient un « esclave », à la merci du cybercriminel à la tête du réseau.

La deuxième technique la plus utilisée est celle du téléchargement à la dérobée, c'est à dire le téléchargement discret d'une application malveillante.

Lorsque la victime accède à une page Web infectée, le programme malveillant est téléchargé sur son ordinateur via diverses vulnérabilités présentes dans les applications et les navigateurs Internet le plus souvent utilisés. Des codes d'exploitation sont utilisés pour tirer profit des vulnérabilités. Ces codes permettent non seulement de télécharger discrètement un programme malveillant, mais également de l'installer à l'insu de l'utilisateur. Si l'attaque réussit, l'utilisateur ne se doute même pas que son ordinateur est infecté. Ce mode de diffusion des applications malveillantes est le plus dangereux : si la ressource compromise est très fréquentée, ce sont des dizaines de milliers d'utilisateurs qui seront infectés !

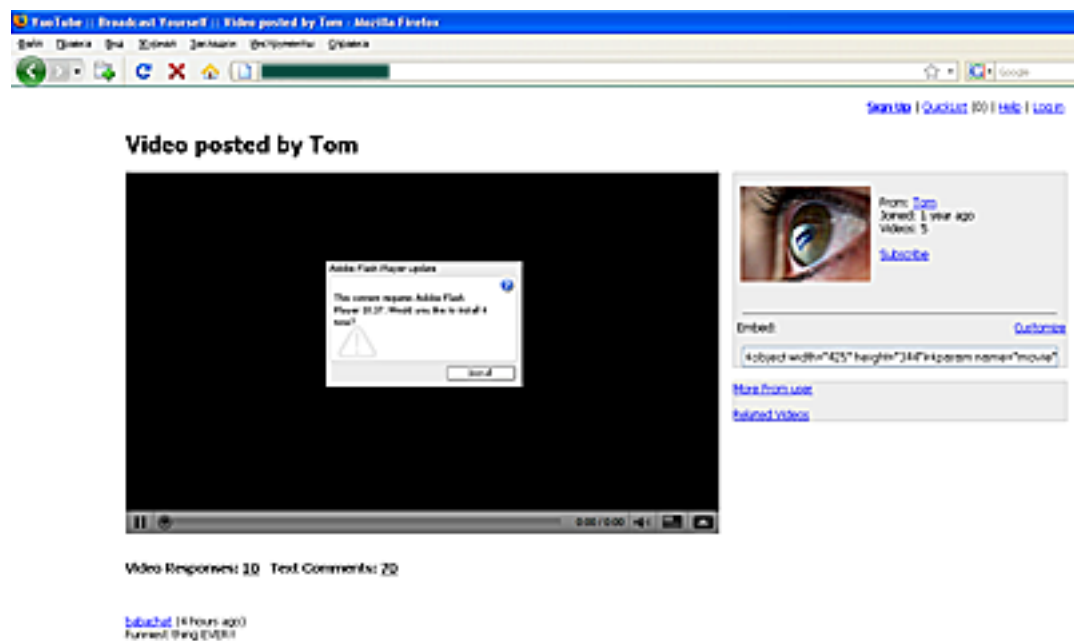


Figure1. Piège pour l'utilisateur. (Fausse page YouTube)

Le bot peut avoir des fonctions de diffusion automatique via les réseaux informatiques. Il peut par exemple se propager en infectant tous les fichiers exécutables accessibles, ou en recherchant les ordinateurs vulnérables du réseau pour les infecter. Virus.Win32.Virut et Net-Worm.Win32.Kido en sont des exemples : le premier est un programme polymorphe qui infecte des fichiers, le second est un ver de réseau. L'efficacité de cette approche est difficile à évaluer : à l'heure actuelle, le réseau de zombies construit par le ver Kido est le plus étendu au monde.

Le créateur d'un réseau de PC zombies peut contrôler les ordinateurs infectés à l'insu des utilisateurs, grâce à un centre de commandes qui communique via un canal IRC, une connexion Internet, etc. Il suffit de réunir quelques dizaines de machines pour que ce réseau de zombies commence à engendrer un revenu pour son propriétaire. Ce revenu est directement proportionnel à la fiabilité du réseau de zombies et à son rythme de croissance.

## Comment les propriétaires de réseaux de PC zombies gagnent-ils de l'argent ?

Plusieurs possibilités existent pour rendre lucratifs les ordinateurs asservis : attaques par déni de service distribué, collecte d'informations confidentielles, diffusion de courrier indésirable, hameçonnage, courrier indésirable de recherche, augmentation du nombre de clics ou téléchargement de logiciels publicitaires et d'applications malveillantes. Il faut noter que quelle que soit l'activité choisie par l'individu mal intentionné, les bénéfices seront au rendez-vous. Et d'ailleurs, pourquoi choisir ? Un réseau de zombies est parfaitement capable de réaliser toutes ces activités... simultanément !

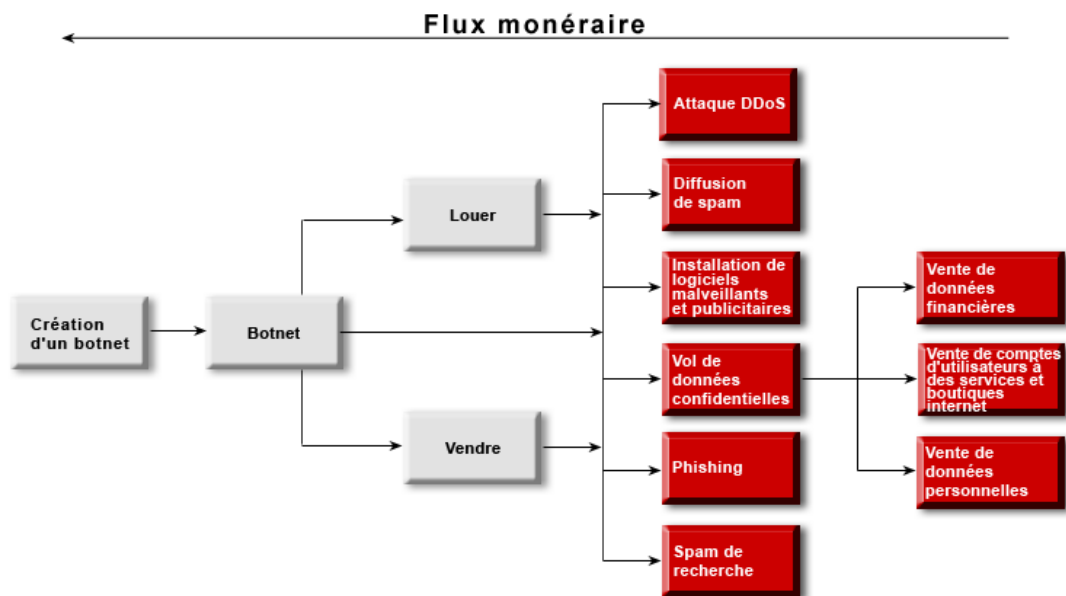


Figure 2. Réseaux de PC zombies et affaires

### Attaques par déni de service distribué

De nombreux chercheurs pensent que la fonction DDoS était déjà exploitée par les tous premiers réseaux de PC zombies. L'attaque par déni de service distribué est une attaque menée contre un système informatique dans le but de mettre celui-ci hors service, c'est-à-dire de le rendre incapable de recevoir et de traiter les requêtes d'utilisateurs légitimes. Une des méthodes les plus souvent utilisées consiste à envoyer un nombre élevé de requêtes à l'ordinateur de la victime, afin de le mettre hors service s'il ne dispose pas des ressources suffisantes pour traiter toutes les requêtes reçues. L'attaque par déni de service distribué est une arme précieuse pour les pirates, et le réseau de zombies est l'outil idéal pour exécuter ce genre d'attaque. Les attaques DDoS peuvent être employées aussi bien dans la lutte contre les concurrents que dans le cadre d'attaques de cyberterroristes.

Le propriétaire d'un réseau de zombies peut mener pour le compte de clients peu scrupuleux des attaques DDoS à l'encontre des sites de ses concurrents, qui sont ainsi rendus inopérables. Le cybercriminel peut alors exiger une rançon, plus ou moins importante. De la même manière, les propriétaires de réseaux de zombies peuvent utiliser à leur propre compte les attaques par déni de service distribué, afin d'extorquer de l'argent à de grandes entreprises. L'entreprise préfère souvent accéder aux demandes du cybercriminel, car la réparation des dégâts provoqués par une telle attaque coûterait encore plus cher.

En janvier 2009, une attaque menée contre l'un des plus importants hébergeurs, godaddy.com, a entraîné la mise hors ligne de plusieurs milliers de sites hébergés sur les serveurs de la société pendant près de 24 heures. Que s'était-il passé ? Une autre société d'hébergement avait-elle appliqué cette tactique illégale pour affaiblir son concurrent, ou l'hébergeur Go Daddy avait-il été la victime du chantage d'un groupe de cybercriminels ? Les deux scénarios sont possibles. Cet hébergeur avait d'ailleurs déjà été victime d'une attaque similaire en novembre 2005. A l'époque, le service avait été suspendu pendant une heure seulement. L'attaque la plus récente, bien plus terrible que la première, témoigne de la croissance incontestée des réseaux de PC zombies.

En février 2007, plusieurs attaques ont été lancées contre des serveurs DNS racines, dont dépend directement le fonctionnement normal de l'ensemble d'Internet. Il est peu probable que ces attaques visaient à détruire Internet car sans lui, les réseaux de zombies ne pourraient exister. Il s'agissait plutôt d'une démonstration de la force et des possibilités des réseaux de zombies.

Des publicités pour la réalisation d'attaques par déni de service distribué s'affichent ouvertement sur de nombreux forums consacrés au sujet. Concernant les tarifs, on observe que le prix à payer pour une attaque oscille entre 50 dollars et plusieurs milliers de dollars par journée complète d'utilisation d'un réseau de zombies. Cet écart au niveau des prix est compréhensible et justifié : l'utilisation d'un petit réseau de zombies (environ 1 000 ordinateurs) suffit pour perturber les ventes du magasin en ligne non protégé d'un concurrent pendant une journée, et cela ne coûtera pas très cher au contrevenant. La situation est toute autre si le concurrent est une grande société multinationale dont le site est protégé, ce qui impliquera l'utilisation d'un nombre bien plus élevé d'ordinateurs pour mener une attaque DDoS concluante. Le prix sera évidemment plus élevé.

Selon les données recueillies par shadowserver.org, près de 190 000 attaques par déni de service distribué ont été organisées en 2008, ce qui aurait rapporté aux cybercriminels près de 20 millions de dollars. Cette estimation ne tient pas compte des revenus du chantage, qu'il est tout simplement impossible d'évaluer.

## Collecte d'informations confidentielles

Les informations confidentielles enregistrées sur le disque dur des ordinateurs intéresseront toujours les individus mal intentionnés. Les informations les plus prisées sont les numéros de cartes de crédit, les données financières et les mots de

passé d'accès à divers services : courrier électronique, FTP, clients de messagerie FTP.

Les programmes malveillants modernes sont capables de sélectionner les données nécessaires aux cybercriminels. Il suffit pour cela de charger le module adéquat sur l'ordinateur infecté.

Les cybercriminels peuvent soit revendre les informations volées, soit les utiliser dans leur propre intérêt. Chaque jour, des annonces pour la vente de codes d'accès à des comptes en banque sont publiées sur les forums clandestins. Le coût dépend de la quantité d'argent disponible sur le compte de l'utilisateur, et est compris entre 1 et 1 500 dollars par compte. La limite inférieure indique que la concurrence qui règne entre les différents cybercriminels du milieu pousse ces derniers à réduire les prix. Pour pouvoir gagner beaucoup d'argent, ils doivent pouvoir compter sur un flux stable de nouvelles données, ce qui implique une croissance stable des réseaux de zombies.

Les informations financières intéressent tout particulièrement les cybercriminels spécialisés dans la fabrication de fausses cartes bancaires. Pour se rendre compte de la rentabilité de ces opérations, il suffit de se souvenir de l'histoire de ce groupe de cybercriminels brésiliens arrêtés il y a deux ans. Ils avaient réussi à retirer 4,74 millions de dollars de divers comptes en banque en utilisant des données dérobées sur des ordinateurs.

Les données confidentielles qui n'ont aucun rapport direct avec l'argent des victimes (le prénom et le nom de famille complet, la date naissance, le domicile, le SSN (numéro de sécurité social, très recherché) pour les Américains sont toutes les informations nécessaires pour fausser des documents, obtenir des crédits et ouvrir des comptes en banque) intéressent les criminels qui se consacrent à la création de faux documents, à l'ouverture de faux comptes en banque, à des affaires illégales, etc.

Le coût des données personnelles dérobées dépend directement du pays où vit le détenteur légitime de ces données. Par exemple, les données complètes de résidents des États-Unis valent entre 5 et 8 dollars. Sur le marché noir, les données d'habitants de l'Union européenne sont particulièrement recherchées : elles coûtent deux à trois fois plus cher que les données de résidents des États-Unis et du Canada. Ceci s'explique par le fait que les criminels peuvent utiliser ces données dans n'importe quel pays de l'Union européenne. La moyenne sur le marché mondial pour un kit complet de données relatives à un individu est de 7 dollars.

Les adresses de courrier électronique figurent parmi les données recueillies par les réseaux de zombies. À la différence des numéros de carte de crédit et des codes d'accès à des comptes bancaires, il est possible de récolter une multitude d'adresses depuis un seul ordinateur. Les adresses récoltées sont ensuite vendues, parfois « en gros », au mégaoctet. Les diffuseurs de courrier indésirable sont les principaux acheteurs. Une liste contenant un million d'adresses électroniques coûte entre 20 et 100 dollars, et la diffusion de messages aux adresses de la liste est comprise entre 150 et 200 dollars. La rentabilité est évidente.



Pour un hébergement Fast-flux, les cybercriminels, le plus souvent des phishers, paient mensuellement les propriétaires de botnets entre 1000 et 2000 dollars.

Le revenu moyen d'une attaque de hameçonnage est comparable au revenu rapporté par le vol de données confidentielles à l'aide de programmes malveillants, et peut atteindre des millions de dollars par an.

## Courrier indésirable

Des millions de messages non sollicités sont envoyés chaque jour dans le monde. La diffusion de ce courrier indésirable est une des fonctions principales des réseaux de zombies modernes. Selon les données de Kaspersky Lab, près de 80 % de l'ensemble des messages non sollicités sont envoyés via les réseaux de zombies.

Les ordinateurs des utilisateurs sont utilisés pour envoyer des milliards de messages faisant la publicité du viagra, de fausses montres, de casinos en ligne, etc. Ces messages surchargent les canaux de diffusion et encombrant les boîtes aux lettres. Les adresses à l'origine de la diffusion sont ajoutées aux listes noires des éditeurs de logiciels antivirus.

On a observé ces dernières années un élargissement de la gamme de services offerts par le spam : il existe désormais les messages non sollicités sur ICQ, les messages non sollicités sur les réseaux sociaux, les forums ou les blogs. Il s'agit d'une vraie « prouesse » des propriétaires de botnets : il est très facile de programmer un module complémentaire pour le client « bot », générant de nouvelles opportunités avec des messages tels que : « Courrier indésirable sur Facebook. C'est pas cher ».

Les tarifs du courrier indésirable varient en fonction du public visé et du nombre d'adresses qui reçoivent les messages. Les prix pour une diffusion ciblée sont compris entre 70 dollars pour des centaines de milliers d'adresses et 1 000 dollars pour quelques dizaines de millions d'adresses.

L'an passé, les diffusions de spams ont rapporté aux spammeurs la somme astronomique de 780 000 000 dollars.

## Courrier indésirable de recherche

Il existe une autre application des réseaux de zombies, à savoir l'optimisation des recherches. Avec ce procédé, les responsables de sites tentent d'améliorer leur position dans les résultats de recherches. Plus un site se positionne en haut du classement, plus il recevra de visiteurs via les moteurs de recherche.

Les robots de recherche tiennent compte de plusieurs facteurs pour évaluer la pertinence d'un site. Un des principaux paramètres est le nombre de liens vers d'autres pages ou domaines. Plus le nombre de ces liens est élevé, plus le classement du site du point de vue du robot sera élevé. Le classement est également influencé par les mots qui composent les liens. Par exemple le lien « achetez nos ordinateurs » sera très pertinent pour la recherche « achat ordinateur »

L'optimisation pour les moteurs de recherche (Search Engine Optimization) est économiquement rentable. De nombreuses sociétés paient des sommes astronomiques à des webmasters afin qu'ils placent leur site en première position dans les résultats de recherche. Les propriétaires de réseaux de zombies ont étudié quelques astuces et ont automatisé le processus d'optimisation de la recherche.

Une multitude de liens, créés par un inconnu ou un ami, peuvent apparaître dans les commentaires d'une entrée sur un blog, ou d'une photo en ligne. C'est la technique utilisée pour promouvoir son site via un réseau de zombies. Le programme spécialement développé à cet effet est installé sur l'ordinateur zombie, et il laisse au nom du propriétaire de l'ordinateur asservi des commentaires sur des sites fréquentés, comportant des liens vers le site promu.

Le prix moyen pour ces services illégaux de courrier indésirable de recherche est d'environ 300 dollars par mois.

## Installation de logiciels publicitaires et de programmes malveillants

Imaginez-vous un instant en train de lire votre magazine en ligne favori sur l'automobile, quand soudain une fenêtre s'ouvre et vous invite à acheter des accessoires d'origine pour votre véhicule. A priori, il n'y a rien de mal à cela et vous seriez même disposé à réaliser cet achat. Par contre, vous savez pertinemment bien que vous n'avez installé aucune application pour la recherche d'objets dont vous avez besoin (ou pas). L'explication est simple : les propriétaires d'un réseau de zombies ont « pensé à vous ».

Les nombreux éditeurs qui proposent des services de publicité en ligne sont payés pour chaque installation de leur application. Il s'agit en général d'une somme modeste, de 30 cents à 1,5 dollars pour une installation. Toutefois, si l'individu mal intentionné dispose d'un réseau de zombies, il peut installer en quelques clics n'importe quelle application sur des milliers d'ordinateurs et gagner ainsi une somme importante.

Le célèbre cybercriminel D. K. Schifer, jugé en 2007, a gagné en un mois plus de 14 000 dollars en installant un logiciel publicitaire sur 10 000 ordinateurs à l'aide d'un réseau de PC zombies de plus de 250 000 machines.

Les représentants d'activités cybercriminelles qui diffusent des applications malveillantes suivent souvent le même modèle en se faisant payer pour chaque installation de leur logiciel. De plus, l'installation d'applications sur des ordinateurs dans différents pays n'a pas le même coût. Ainsi, l'installation d'un programme malveillant sur mille ordinateurs en Chine coûtera en moyenne 3 dollars alors qu'il faudra compter 120 dollars aux Etats-Unis. Ceci est tout à fait compréhensible dans la mesure où les utilisateurs des pays développés ont des données qui valent beaucoup plus d'argent.

## Augmentation du nombre de clics

Les agences de publicité qui travaillent en ligne selon le modèle PPC (Pay-per-Click) versent de l'argent pour chaque clic unique sur les annonces. Pour les propriétaires de réseaux de zombies, tromper ces compagnies peut rapporter gros.

Prenons par exemple le célèbre réseau Google AdSense. Les annonceurs paient Google pour les clics sur les annonces, en espérant que le visiteur achètera quelque chose chez eux.

Google de son côté place des publicités contextuelles sur divers sites participant au programme AdSense et paie un pourcentage pour chaque clic au propriétaire du site. Malheureusement, tous les propriétaires de sites ne sont pas honnêtes. Ainsi, le pirate ayant accès à un réseau de zombies peut générer des milliers de clics uniques par jour, un par machine afin de ne pas éveiller les soupçons de Google. L'argent dépensé en publicité par la société arrive dans les poches du pirate. Malheureusement, il n'existe à ce jour aucun cas où les auteurs ont dû répondre de leurs actes.

Selon les données de Click forensics en 2008, 16 à 17% des clics sur les liens publicitaires étaient contrefaits, dont un tiers était généré par les botnets. Un calcul rapide nous montre que sur un an les propriétaires des botnets ont récolté grâce aux liens commerciaux 33 000 000 de dollars.

## Location et vente de réseaux zombies

La célèbre formule « marchandise-argent-marchandise » énoncée par Marx devient, pour les propriétaires de réseaux de zombie importants, « réseau de zombies-argent-réseau de zombies ». Il est vrai que le maintien du réseau de zombies, la recherche de nouveaux zombies, la protection contre la détection des bots par les logiciels antivirus et la mise en place de centres de contrôle et de commande nécessitent des investissements aussi bien en temps qu'en argent de la part des pirates. Ils n'ont ainsi tout simplement pas le temps de diffuser eux-mêmes les messages, d'installer une application quelconque ou de voler des données et de les revendre. Il est plus simple de louer le réseau de zombies ou de le vendre à toute personne intéressée.

La location d'un réseau de zombies de messagerie dont la vitesse de diffusion est de 1 000 messages par minute (lorsque 100 zombies sont en ligne) revient à environ 2 000 dollars par mois. Le coût de la location d'un réseau de zombies « clé en main » dépend du nombre d'ordinateurs infectés. Les petits réseaux comptant quelques centaines de bots sont compris entre 200 et 700 dollars, un bot revenant en moyenne à 0,5 dollar. Les réseaux plus développés coûtent bien plus cher. Ainsi, le réseau Shadow, créé par un jeune pirate hollandais de 19 ans, comptant plus de 100 000 ordinateurs à travers le monde, a été vendu 36 000 dollars. C'est le prix d'une petite maison en Espagne, mais un criminel brésilien a préféré s'acheter un réseau de PC zombies.

## Conclusion

Chaque jour, les personnes à la tête de réseaux de zombies empochent des sommes astronomiques. La lutte contre cette activité exploite tous les moyens possibles, mais est loin d'être efficace devant la loi. L'application de législations contre le courrier indésirable, contre la création et la diffusion de programmes malveillants, ou contre la violation de l'intégrité de réseaux informatiques, n'est pas une pratique adoptée dans tous les pays, et tous les pays ne possèdent d'ailleurs pas nécessairement une législation en la matière. Les propriétaires ou les créateurs de réseaux de zombies qui ont été traduits en justice se comptent sur les doigts de la main. Paradoxalement, le nombre de réseaux de zombies opérationnels sur Internet est élevé : on en recensait récemment 3 600. En réalité, le décompte du nombre de réseaux opérationnels n'est pas une mince affaire car il existe quelques dizaines de réseaux de zombies importants dont il est impossible de remarquer l'activité et une multitude de réseaux plus petits particulièrement difficiles à découvrir et à scinder.

A l'heure actuelle, la méthode la plus efficace pour lutter contre les réseaux de PC zombies consiste à jouer sur une collaboration étroite entre les spécialistes de la lutte contre les virus, les fournisseurs d'accès Internet et les autorités judiciaires. C'est peut-être cette coopération qui a entraîné la fermeture de trois sociétés : EstDomains, Atrivo et McColo. Il faut noter que la fermeture de la société McColo, dont les serveurs hébergeaient les centres de commande de plusieurs réseaux de zombies importants, spécialisés dans la diffusion de courrier indésirable, a entraîné une réduction de 50 % du nombre de messages non sollicités en circulation.

Les spécialistes étudient des milliers de réseaux de zombies, les logiciels antivirus détectent et neutralisent les bots dans le monde entier mais seules les autorités judiciaires peuvent interrompre l'activité des centres de commandes et capturer les criminels, ce qui « désactiverait » les réseaux de zombies à long terme. Les effets de la fermeture de McColo ont été de courte durée : quelques semaines plus tard, le volume de courrier indésirable avait à nouveau atteint son niveau habituel. Les propriétaires de réseaux de zombies ont déplacé leurs centres de commande chez d'autres hébergeurs, et ils ont poursuivi leur activité comme auparavant. Aussi, il est primordial de mener une lutte de tous les instants, et non pas seulement des vérifications ponctuelles. Malheureusement, les réseaux de zombies s'apparentent bien souvent à une hydre des temps modernes !

La lutte ne peut être efficace si elle ne compte pas l'appui des utilisateurs. Ce sont en effet les ordinateurs des particuliers que l'on retrouve majoritairement dans les réseaux de zombies. Le non-respect de règles de sécurité élémentaires, telles que l'utilisation d'un logiciel antivirus, l'utilisation de mots de passe robustes, ou la désactivation du lancement automatique des fichiers depuis les supports amovibles, peut transformer votre ordinateur en nouveau membre d'un réseau de zombies, ce qui mettrait vos données et vos ressources à disposition d'individus mal intentionnés. Pourquoi faciliter la tâche des cybercriminels ?