

# Éliminer les botnets de demain

Cet article est extrait de *Understanding and Blocking the New Botnets*, un livre blanc rédigé par Scott Pinzon (CISSP) et Corey Nachreiner (CISSP) de l'équipe LiveSecurity® de WatchGuard®. Pour profiter d'un regard éclairé sur les botnets et la façon dont ils agissent et évoluent aujourd'hui, téléchargez notre livre blanc sur [www.watchguard.com/whitepapers.asp](http://www.watchguard.com/whitepapers.asp).

Les botnets constituent la menace mixte ultime. Le code botnet contient toutes les formes possibles de logiciels malveillants : spywares, chevaux de Troie « downloaders », rootkits, moteurs spam et autres. Pour se défendre, de multiples couches de sécurité sont nécessaires. Heureusement, les techniques consacrées sont encore très efficaces contre les botnets. Vous trouverez ci-dessous les mesures que nous vous recommandons pour réduire sérieusement l'éventualité d'une infection de votre réseau par des bots.

## 1. Déployez rapidement les patches

Les bots s'appuient sur une grande diversité d'exploits pour infecter leurs victimes, les plus importants et réussis exploitant des vulnérabilités *corrigées par les fournisseurs il y a déjà six à dix-huit mois*. Dans les cas extrêmes, on a vu des bots tenter des exploits contre des vulnérabilités patchées jusqu'à quatre ans auparavant. On ne peut expliquer pourquoi les communications entre bots et les systèmes de back-end innovent à une vitesse prodigieuse, alors que le bot utilise des exploits anciens connus. D'après nous, les botmasters trouvent les exploits en attendant que les fournisseurs corrigent la vulnérabilité, puis procèdent à une ingénierie inverse du patch pour trouver la défaillance.

Nous pensons que l'exploitation des défaillances plus récentes est l'un des aspects sur lesquels les botmasters ont des progrès à faire. Pour le moment, c'est plutôt une bonne chose pour l'administrateur de réseau lambda car, si vous patchez dès que les fabricants sortent les correctifs des logiciels de votre réseau, cela vous permet d'être plus rapide que les botmasters et de résister à leurs exploits.

## 2. Bloquez JavaScript

Lorsqu'un bot utilisant des exploits sur Internet attaque un ordinateur, il le fait invariablement en exécutant JavaScript. Si vous paramétrez vos navigateurs de façon à demander l'autorisation avant d'exécuter les JavaScript, vous éliminerez une kyrielle de facteurs d'infection par bot. Nous vous recommandons vivement de faire du Firefox le navigateur principal de vos utilisateurs et d'employer le [module NoScript](#) pour autoriser ou non les scripts qui tentent de s'exécuter.

## 3. Surveillez les ports ci-dessous

1) Même si les derniers bots peuvent communiquer par des ports que tout administrateur doit laisser ouverts, la plupart d'entre eux communiquent encore avec IRC (port 6667) ou d'autres ports à chiffre élevé (comme 31337 et 54321). Tous les ports au-dessus de 1024 doivent être configurés de façon à être bloqués en émission et en réception, sauf si votre entreprise a une application sur mesure ou un besoin spécial d'ouvrir un port donné. Même dans ce cas, vous pouvez le faire avec prudence, à l'aide de règles comme « Ouvrir uniquement pendant les heures ouvrées » ou « Refuser tout, sauf le trafic de la liste d'adresses IP de confiance ». Il s'agit d'une mesure simple qui empêche les bots « garden variety » et « slow-adopter » d'atteindre leur centre de commande et de contrôle (C&C), et de recevoir les instructions et mises à jour, ce qui les élimine à l'arrivée.

2) Le trafic botnet qui voyage sur les ports indispensables comme le 80 ou le 7 se trahit souvent lui-même en générant du trafic là où il ne devrait pas y en avoir. Souvent, les botmasters procèdent à la mise à jour de leurs zombies entre 1h00 et 5h00, quand ils pensent ne pas être observés. Prenez l'habitude de vérifier les journaux de vos serveurs le matin. Si vous constatez une navigation sur Internet alors que personne n'était là, faites une recherche.

Les administrateurs qui utilisent les modèles WatchGuard Firebox® seront heureux d'apprendre que les proxies du Firebox bloquent le trafic non standard tentant d'utiliser des ports standard. Ainsi, le botnet de spamming Mega-D fait passer un trafic non standard ou « maison » sur le port HTTP 80, mais le proxy HTTP du Firebox l'identifie et le bloque instantanément par défaut.

#### 4. Redoublez la formation des utilisateurs

Certains bots exécutent des scans en masse d'Internet, identifient les machines vulnérables et les infectent. Cette pratique diminue aujourd'hui. Plus souvent, les bots recourent à l'ingénierie sociale pour pénétrer dans les réseaux en incitant la victime à cliquer sur un lien ou à ouvrir un fichier. Ces bots ont les mêmes limitations que celles de certains vampires légendaires : ils ne peuvent franchir votre porte que si vous les y invitez.

Cette approche de séduction s'est resserrée peu à peu. Les attaquants avaient l'habitude d'envoyer un code exécutable malveillant en pièce jointe à un e-mail. Une pratique qui tombe en désuétude. L'action est désormais basée sur Internet. Les e-mails malveillants qui auraient contenu une pièce jointe il y a deux ans, présentent maintenant un lien vers un site malveillant. Des sites Internet inoffensifs peuvent être infectés par Mpack ou d'autres malwares clandestins afin d'infecter les visiteurs ayant cliqué témérairement sur ce lien.

C'est votre rôle d'expliquer aux utilisateurs, dans des termes compréhensibles, pourquoi ils ne doivent jamais laisser entrer un vampire. Recommandez-leur de ne pas ouvrir de pièces jointes non sollicitées ou inattendues, de ne pas cliquer sur un lien dans un e-mail et de réfléchir à deux fois avant de cliquer sur des liens inhabituels. En guise de point de départ, faites circuler notre vidéo non technique montrant le fonctionnement des téléchargements intempestifs : <http://video.google.com/videoplay?docid=-4094518401580008932>. L'application méticuleuse de contrôles tels que ceux cités ci-dessus a permis à des réseaux de fonctionner sans bots pendant des années.

#### 5. Restez vigilant

Cette recommandation semble aller de soi – un peu comme dire « Essayez d'éviter d'être infecté ! ». Pourtant, nous rencontrons sans cesse des administrateurs informatiques qui passent tellement de temps à parer au plus pressé et à maintenir une ligne d'assistance en sous-effectif, qu'ils ne regardent jamais leurs journaux système. Ils ne contrôlent pas l'utilisation de la bande passante. Ils sont incapables de vous dire qui se connecte à quoi sur leur réseau et ils ont des appareils connectés sur leur réseau, sans le savoir.

Si vous vous reconnaissez dans cette description, vous allez au-devant d'ennuis. Votre réseau est peut-être déjà infecté par des bots. Si vous vérifiez rarement les journaux, mettez-vous y. Maintenant. Une fois que vous connaîtrez l'état « normal » de votre réseau, il vous faudra 30 minutes pour effectuer un contrôle. Bien sûr, ceci est dû à un manque de ressources et de personnel, et non à une quelconque paresse de votre part. Expliquez la menace à vos supérieurs et voyez s'ils vous aideront à bloquer une demi-heure chaque matin pour vérifier l'état du réseau. Cette demi-heure doit avoir la priorité sur les demandes de réunions, les téléconférences et autres interruptions de ce type. C'est une forme d'assurance extrêmement bon marché par rapport au coût de l'altération de votre réseau.

---

Nous pensons que les émergences récentes et sans précédent de bots annoncent les innovations à venir. Plus que jamais auparavant, chaque mois semble apporter des exploits inédits *que les chercheurs ne peuvent expliquer entièrement*.

Il s'avère que les botnets sont des menaces mixtes, mais ce ne sont pas encore *les dernières*. Les botmasters complètent librement leur architecture traditionnelle par des composants qui renforcent l'automatisation, l'administration et l'évasion. Ces combinaisons technologiques sont effroyablement sophistiquées et incroyablement affinées, et n'importe quel observateur vous dira que cette tendance ne fera que s'amplifier.

Les méchants sont-ils en train de gagner la partie ? Manifestement non, puisque l'on fait encore des achats et des transactions bancaires via Internet. Mais l'activité des bots augmente et nous devons la repousser, l'endiguer et révéler les techniques des botmasters. Le moyen le plus simple pour saper le pouvoir d'un botmaster est de rendre difficile le recrutement des victimes. Les appliances WatchGuard utilisent de nombreuses couches de sécurité et les appliquent intelligemment à de nombreux protocoles, avec une technologie de proxy avancée qui nettoie le trafic entrant et sortant pour protéger votre réseau.

Pour en savoir plus sur les solutions de sécurité WatchGuard et la protection qu'elles offrent contre les botnets et autres menaces réseau, rendez-vous sur [www.watchguard.com](http://www.watchguard.com) ou contactez votre revendeur.

©2008 WatchGuard Technologies, Inc. Tous droits réservés. WatchGuard, le logo WatchGuard, Firebox et LiveSecurity sont des marques non déposées ou déposées de WatchGuard Technologies, Inc. aux États-Unis et/ou dans d'autres pays. Tous les autres noms de marques et marques sont la propriété de leurs propriétaires respectifs. Numéro de référence : WGCE66528\_050608