Les Botnets

Fiche de l'Internet Society sur les politiques publiques

Complexes et en évolution continuelle, les botnets sont un défi à la confiance des utilisateurs et à la sécurité sur l'Internet. Le combat contre les botnets exige une collaboration multidisciplinaire transfrontalière, des approches techniques innovantes, et le déploiement généralisé de mesures de mitigation qui respectent les principes fondamentaux de l'Internet.

Introduction

Un botnet est une collection d'ordinateurs d'utilisateurs connectés à l'Internet (bots) infectés par un logiciel malveillant qui permet à ces ordinateurs d'être contrôlés à distance par un opérateur (appelé parfois bot herder) par l'intermédiaire d'un serveur de Commande-et-contrôle (C&C) pour exécuter certaines tâches comme voler de l'information ou lancer des attaques contre d'autres ordinateurs. Le logiciel malveillant des botnets est conçu pour donner à ses opérateurs le contrôle sur de nombreux ordinateurs en même temps. Ceci permet aux opérateurs de botnets d'utiliser des ressources informatiques et de bande passante à travers de nombreux réseaux pour des activités malveillantes.

Historiquement, les botnets ont été surtout utilisés pour générer et propager des courriels indésirables. Ils peuvent être utilisés dans de nombreux buts malveillants, dont le vol de données personnelles et de mots de passe, l'attaque de réseaux publics et privés, l'exploitation de la puissance informatique et de l'accès à Internet des utilisateurs, et la mise en œuvre d'attaques de déni de service distribué (DDoS).[1] En résumé, les botnets sont un problème complexe et en évolution continuelle qui constitue une menace à la confiance des utilisateurs en l'Internet.

Diverses techniques sont utilisées pour infecter les ordinateurs pour en faire des bots, entre autres convaincre les utilisateurs de télécharger des logiciels malveillants, exploiter les vulnérabilités des navigateurs, persuader les utilisateurs d'enregistrer un logiciel malveillant (par ex. à la suite de l'ouverture d'une pièce jointe à un e-mail infectée). Le logiciel malveillant d'un botnet est conçu pour fonctionner en arrière plan, de sorte que les utilisateurs ne savent pas que leurs systèmes sont infectés.

Bien que les botnets constituent une menace aux utilisateurs de l'Internet et soient difficiles à éliminer, on peut prendre des mesures pour réduire leur impact et les risques associés.

Considérations clés

Les botnets imposent des coûts sociaux et économiques aux utilisateurs et entreprises affectés, aux fournisseurs de services, aux opérateurs de réseaux et à la société dans son ensemble. Si on ne se livre à aucun effort de mitigation, les botnets ont le potentiel de nuire à l'ensemble des bénéfices économiques et sociaux de l'Internet. Plusieurs questions doivent être considérées pour aborder le problème des botnets. Entre autres :

[1] https://en.wikipedia.org/wiki/Denial-of-service_attack

- **La dispersion géographique.** Les botnets peuvent se propager sur de grandes distances et dans plusieurs régions du globe, avec des ordinateurs infectés et des opérateurs de botnets opérant dans des endroits et pays divers. La même chose s'applique aux serveurs C&C. En soi, les botnets sont transnationaux et exigent une approche collaborative pour la détection, la mitigation et la mise en application des lois.
- **L'influence sur les droits des utilisateurs.** Il est important de considérer l'influence sur les droits fondamentaux des utilisateurs lors de l'approche de stratégies pour combattre les botnets. Les stratégies de mitigation des botnets excessivement étendues, comme le blocage de tout le trafic d'un réseau infecté, peut empêcher involontairement des utilisateurs innocents d'accéder à l'Internet et d'exercer leurs droits, comme la liberté d'expression et d'opinion. De plus, certaines méthodes pour détecter et repérer les botnets, comme la collecte indiscriminée de données qui transitent sur les réseaux, peuvent être une violation de la confidentialité légitime des utilisateurs de l'Internet.
- **L'influence sur l'utilisation de la technologie et sur l'innovation.** Certaines stratégies de mitigation technique et légale, telles que la restriction de l'accès aux réseaux soupçonnés d'être infectés, peuvent avoir des conséquences négatives sur l'ouverture, le potentiel d'innovation et la portée globale de l'Internet. De plus, les stratégies spécifiquement technologiques sont moins susceptibles d'attaquer le problème des botnets dans son ensemble, car leurs créateurs peuvent changer de tactique pour éviter les nouveaux obstacles.

Défis

Un certain nombre de facteurs contribuent au combat permanent contre les botnets, dont:

- Les stratégies, technologies et techniques des botnets sont en évolution constante et s'adaptent en réponse aux mesures de mitigation.
- Les botnets sont devenus des outils populaires auprès des cybercriminels parce que leurs coûts de déploiement et d'exploitation sont modestes, et parce qu'ils sont difficiles à découvrir et disponibles à l'achat ou en location par le biais des réseaux criminels.[2]
- Les créateurs et opérateurs de botnets sont dispersés géographiquement par rapport aux bots incriminés et sont habiles pour dissimuler leurs emplacements et identités.
- Il y a des ordinateurs vulnérables connectés à l'Internet (par ex. ceux qui ne sont pas suffisamment sécurisés ou ceux dont les utilisateurs sont susceptibles d'être persuadés d'introduire le logiciel malveillant des botnets dans leurs ordinateurs). Les opérateurs de botnets recherchent les systèmes vulnérables à infecter.
- Les botnets sont conçus pour profiter des propriétés fondamentales de l'Internet (les Invariants de l'Internet[3]) et de sa conception architecturale, où l'intelligence se trouve dans les appareils périphériques (par ex.les serveurs de commande et contrôle du botnet et les ordinateurs infectés) plutôt que dans le réseau lui-même.

[2] Pour des exemples, voir http://www.wired.co.uk/news/archive/2012-11/02/russian-cybercrime et http://www.zdnet.com/article/study-finds-the-average-price-for-renting-a-botnet/

[3] Voir les Invariants de l'internet : ce qui compte réellement http://www.internetsociety.org/internet-invariants-what-really-matters

Principes directeurs

L'Internet Society pense qu'une approche collaborative de toutes les parties prenantes concernées est la meilleure solution de mitigation des botnets et de protection de la sécurité. Cette approche est intégrée aux principes de Sécurité collaborative de l'Internet Society, lesquels mettent l'accent sur une responsabilité partagée et collective pour atteindre les objectifs désirés.[4] Cette approche de sécurité collaborative comprend les principes suivants :

Encourager la confiance et protéger les opportunités. L'objectif de sécurité est destiné à promouvoir la confiance en l'Internet et à assurer son succès permanent de moteur d'innovation économique et sociale.

- *Promouvoir la prise de conscience.* Promouvoir la prise de conscience générale selon laquelle les parties prenantes sont engagées à travailler ensemble pour démonter et décourager la création de nouveaux botnets par le biais de mesures efficaces et raisonnables.
- *Promouvoir des systèmes sécurisés.* Promouvoir une expérience d'utilisateur de l'Internet plus sûre en encourageant les pratiques de conception de logiciels sécurisés, les composants de sécurité communs de haute qualité, la détection sans délai des vulnérabilités, la distribution de mises à jour et des systèmes semblables.
- *Promouvoir les appareils sûrs.* Promouvoir l'utilisation de systèmes configurés correctement pour résister aux botnets. Par exemple, au niveau de l'ordinateur individuel, l'utilisation de logiciels de protection contre les logiciels malveillants et pour la détection des logiciels espions réduit le risque d'infection par les botnets.
- *Promouvoir le confinement.* Promouvoir l'amélioration de la capacité technique de la communauté de l'Internet dans son ensemble pour contenir la propagation, l'exploitation et l'impact des botnets. Ceci inclut l'amélioration des capacités pour désactiver les botnets et réduire les dommages.

Responsabilité collective. Les participants de l'Internet partagent une responsabilité du système dans son ensemble.

- *Responsabilité partagée.* Des efforts doivent être faits pour partager la responsabilité afin que toutes les parties prenantes participent à la lutte contre les botnets, y compris les gouvernements, opérateurs de réseaux, fournisseurs de logiciels, fournisseurs de services en ligne, la communauté technique, et les utilisateurs finaux. Par exemple, bien qu'un réseau qui héberge un botnet sans le savoir puisse ne pas être directement affecté, l'opérateur de ce réseau doit être responsable de s'assurer qu'il ne devienne pas une rampe de lancement pour des activités malveillantes. Un « code » pour une telle gestion responsable de réseau est consigné dans le « Code de conduite anti-bot pour les Fournisseurs d'accès à Internet, un code volontaire de l'industrie pour aider à réduire les bots des utilisateurs finaux »[5]. Généralement, compter sur un petit nombre de parties pour implémenter des politiques sur les botnets ou imposer artificiellement la responsabilité légale, plutôt que d'implémenter une approche collective, place une charge injuste sur certains et a le potentiel de perturber le modèle de responsabilité collective de l'Internet.
- *Approche collaborative.* Les activités collaboratives sont essentielles quand il s'agit de gérer les botnets. Ceci inclut le partage du renseignement et des données sur les attaques opérationnelles, le partage des bonnes pratiques et des méthodes de mitigation, et la coordination des activités anti-botnets. Il est aussi important que la collaboration soit proactive et non réactive.

[4] Principes de sécurité collaborative de l'Internet Society, http://www.internetsociety.org/collaborativesecurity.
[5] Voir https://www.m3aawg.org/abcs-for-ISP-code

- *Application et contrôle transfrontaliers.* La collaboration transfrontalière peut être facilitée par des lois qui rendent les botnets et leur activité malveillante illégaux et permettent la collecte appropriée d'informations et leur partage pour la mitigation et le contrôle. Il faut penser avec soin à la manière dont les mesures techniques qui détectent et atténuent l'effet des botnets par-delà les frontières sont mises en place : qui est impliqué et qu'est-ce qui est raisonnable et permis.

Propriétés et valeurs fondamentales. Les solutions de sécurité doivent être compatibles avec les droits de l'Homme fondamentaux et préserver les propriétés fondamentales de l'Internet, Les Invariants de l'Internet.

- *Respecter les droits des utilisateurs.* Les approches des politiques doivent tenir compte des effets involontaires potentiels sur l'accès et la confidentialité des utilisateurs lors de l'implémentation des actions destinées à gérer les botnets. Les solutions bien intentionnées contre les botnets peuvent par inadvertance porter atteinte aux usages légitimes de l'Internet ou exposer sans raison l'information d'utilisateurs privés.
- *Préserver les propriétés fondamentales de l'Internet.* Les approches des politiques doivent tenir compte de l'impact potentiel sur l'architecture sous-jacente de l'Internet et s'assurer qu'elles n'ont pas une influence négative sur l'ouverture, l'innovation sans permission ou la portée globale de l'Internet. Par exemple, annuler un domaine peut par inadvertance rendre inaccessibles des sites web légitimes et non infectés.[6]

Évolution et consensus. La sécurité efficace compte sur des étapes agiles d'évolution basées sur l'expertise d'un vaste ensemble de parties prenantes.

- *Agilité.* Les politiques et les solutions doivent être assez agiles pour rester efficaces en prenant en compte l'évolution rapide des botnets. Par exemple, les politiques qui empêchent les chercheurs en sécurité d'enquêter sur le comportement des botnets peuvent retarder le développement de nouveaux outils et techniques anti-botnets. De plus, les politiques doivent s'efforcer de s'opposer à la création, à la propagation, et au fonctionnement des bots et des serveurs de commande et contrôle ainsi qu'aux individus qui en sont propriétaires et qui les exploitent.
- *Solutions indépendantes des technologies.* Les approches à long terme doivent être conçues pour être indépendantes des technologies, ce qui signifie qu'elles ne prescrivent pas une solution technique détaillée. Les solutions doivent plutôt spécifier une stratégie générale, qui s'implémente et s'adapte aux nouvelles technologies.
- *Se concentrer sur les causes fondamentales.* Les stratégies doivent se concentrer sur le traitement des causes fondamentales du problème. Traiter les symptômes (par ex. le courrier indésirable) sans traiter aussi la cause fondamentale (le botnet) peut amener à négliger d'autres activités malveillantes du botnet (par ex. le vol de données personnelles).
- *Solutions partielles.* Les décideurs de politiques doivent considérer que les solutions partielles pour combattre les botnets peuvent avoir certains mérites. Les mesures par incréments pour détecter et désactiver les botnets n'éliminent pas la menace complètement, mais elles aident à contenir le problème et érodent la rentabilité des botnets.

Penser globalement, agir localement. Les solutions les plus efficaces seront probablement atteintes par une auto-organisation de bas en haut.

[6] Voir, par exemple, http://www.pcworld.com/article/2452460/microsoft-settles-with-noip-in-botnet-hunt-after-seizing-its-domains.html

- *Renforcer la confiance.* En général, les stratégies les plus efficaces contre les botnets sont implémentées par des groupes non officiels et auto-organisés qui sont basés sur la confiance parmi les experts dans ce domaine.[7]

Ressources supplémentaires

L'Internet Society a publié plusieurs articles et du contenu supplémentaire en rapport avec cette question. Ils sont librement accessibles sur le site Web de l'Internet Society.

- *Sécurité collaborative : une approche pour attaquer les problèmes de sécurité sur l'Internet,* http://www.internetsociety.org/collaborativesecurity
- Collaboration globale multilatérale pour réaliser un cyberespace sûr, sécurisé et tolérant : Permettre un développement et une croissance durables grâce à des principes de cyber-éthique, http://internetsociety.org/doc/global-multi-stakeholder-collaboration-achieving-safe-secure-and-tolerant-cyberspace-enabling.
- Comprendre la sécurité et la résilience de l'Internet, http://www.internetsociety.org/doc/understanding-security-and-resilience-internet et infographique : Collaboration pour un internet sécurisé et résilient, http://internetsociety.org/doc/infographic-collaboration-secure-and-resilient-internet
- Cybersécurité : Placer les pièces du puzzle de la cybersécurité, http://internetsociety.org/cybersecurity-laying-out-pieces-cybersecurity-puzzle.
- *Vers l'amélioration de la sécurité, stabilité et résilience des DNS,* http://internetsociety.org/towards-improving-dns-security-stability-and-resiliency-0.

Internet Society
Galerie Jean-Malbuisson, 15
CH-1204 Genève, Suisse
Tél : +41 22 807 1444 • Fax : +41 22 807 1445
www.internetsociety.org

1775 Wiehle Ave., Suite 201
Reston, VA 20190 USA
Tél : +1 703 439 2120 • Fax : +1 703 326 9881
E-mail : info@isoc.org

[7] Voir par exemple, http://www.cfr.org/cybersecurity/defending-open-global-secure-resilient-internet/p30836