CSRIC III

Communications Security, Reliability and Interoperability Council

Mars 2012

Rapport final

Code de conduite anti-robot américain (ABC) pour les fournisseurs d'accès à Internet (FAI)

(Un code volontaire)

"Ce code de conduite serait un grand pas en avant et un complément important aux efforts plus larges de l'administration contre les botnets."

Julius Genachowski, président de la FCC
22 février 2012

GROUPE DE TRAVAIL 7 - Remédiation des botnets

Table des matières

1 Résultats en bref

1.1 Résumé exécutif

Un "bot" malveillant est un programme installé sur un système afin de permettre à ce dernier d'exécuter automatiquement une tâche ou un ensemble de tâches, généralement sous la commande et le contrôle d'un administrateur distant malveillant. L'augmentation du nombre de dispositifs d'utilisateurs finaux infectés par des robots1 représente une menace significative pour la vitalité et la résilience de l'internet et de l'économie en ligne.
Les réseaux de zombies sont des réseaux de dispositifs informatiques d'utilisateurs finaux connectés à l'Internet et infectés par des logiciels malveillants de zombies, qui sont contrôlés à distance par des tiers à des fins malveillantes. Les bots et les réseaux de bots peuvent entraîner le vol d'informations personnelles, des attaques contre des réseaux publics et privés, ainsi que l'exploitation de la puissance de calcul et de l'accès à l'internet des utilisateurs finaux.

Le CSRIC III a chargé le groupe de travail 7, Botnet Remediation, de proposer un ensemble de pratiques volontaires convenues qui constitueraient le cadre d'un modèle de mise en œuvre opt-in à suivre par les FAI pour atténuer la menace des botnets. En réponse à cette proposition, le code de conduite anti-bot américain pour les FAI a été élaboré pour répondre à la menace des bots et des botnets dans les réseaux résidentiels à large bande par une participation volontaire. Lors de l'élaboration du code, il a été déterminé que les composantes de l'ensemble de l'écosystème Internet ont un rôle important à jouer dans la lutte contre la menace des botnets et que les FAI dépendent du soutien des autres parties de l'écosystème.

Le Code encourage les ISP à participer à des activités visant à soutenir l'éducation des utilisateurs finaux afin de prévenir les infections par des bots, la détection des bots, la notification des infections potentielles par des bots, la remédiation des bots, ainsi que la collaboration et le partage des informations provenant des participants au Code. Le Code est inclus dans l'annexe.

Le groupe de travail a proposé un ensemble de pratiques volontaires convenues qui constitueraient le cadre d'un modèle de mise en œuvre opt-in pour les FAI afin de contribuer à la lutte contre la menace des botnets. Le groupe de travail recommande des mesures que les FAI offrant un accès Internet résidentiel à large bande peuvent prendre s'ils choisissent d'adopter le code. Le groupe de travail recommande également aux FAI et aux autres fournisseurs de services d'indiquer qu'ils acceptent de participer au code volontaire en contactant l'organisation industrielle qui gère la participation au code. Dans un premier temps, il est suggéré que les FAI et autres fournisseurs de services participants informent l'entité de leur choix de leur participation au code ou s'auto-affirment sur leur propre site Web. Les travaux futurs comprennent la détermination de l'administration à long terme de la participation au code, les mises à jour périodiques du code, l'identification des obstacles à la participation au code, la définition de paramètres et l'identification des meilleures pratiques et des leçons apprises parmi les participants au code et les contributeurs de l'écosystème de soutien.

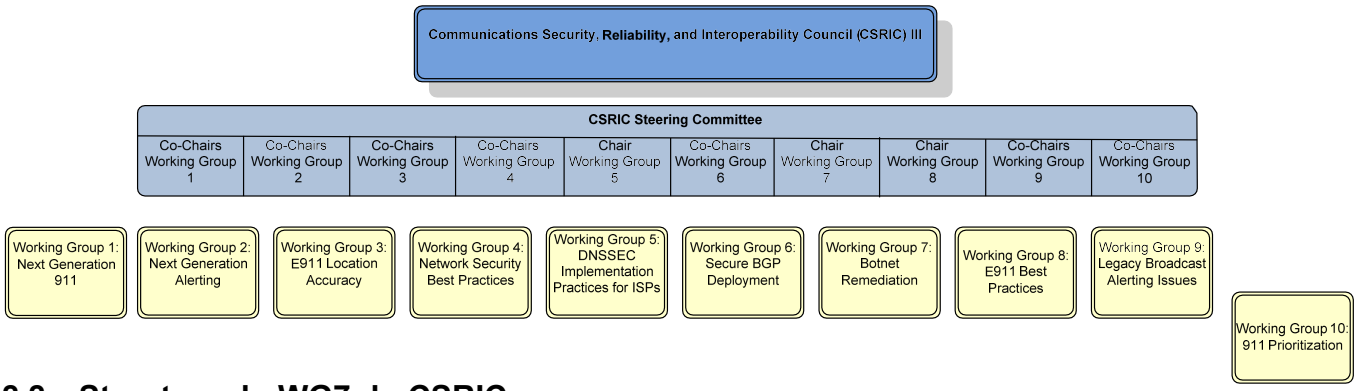
[1] Les termes "bot" et "infection par un bot" sont utilisés indifféremment dans ce document.

2 Introduction

Le CSRIC III a établi le groupe de travail 7 (WG7) pour aborder la remédiation des botnets dans les réseaux à large bande. Le WG7 a étudié les travaux sur la remédiation des botnet qui ont lieu à l'IETF, au Japon, en Australie, en Finlande, en Allemagne et ailleurs afin de déterminer la meilleure approche pour traiter la menace des botnet dans les réseaux à large bande des États-Unis.

Le résultat de ce travail est le code de conduite anti-bot volontaire des États-Unis pour les fournisseurs de services Internet, qui se trouve en annexe.

2.1 Structure du CSRIC



2.2 Structure du WG7 du CSRIC

Le WG7 est présidé par Michael O'Reirdan, président du Messaging Anti-Abuse Working Group (MAAWG), et vice-présidé par le Dr Peter Fonash, Chief Technology Officer, Office of Cybersecurity and Communications, Department of Homeland Security. Les membres du WG7 comprennent des représentants des FAI, des fournisseurs de logiciels et d'équipements de réseau, du monde universitaire, ainsi que d'autres organisations faisant partie de l'écosystème Internet.

2.3 Membres de l'équipe du groupe de travail 7

Le groupe de travail 7 est composé des membres énumérés ci-dessous.

Nom	Entreprise
Michael O'Reirdan - Président	MAAWG
Peter Fonash - Vice-Président	Département de la sécurité intérieure
Neil Schwartzman - Secrétaire	CAUCE
Robert Thornberry - Rédacteur en chef	Bell Labs, Alcatel-Lucent
Paul Diamond - Rédacteur en chef	CenturyLink
Vernon Mosley - Liaison	FCC
Alex Bobotek	AT&T
Adam O'Donnell	Sourcefire
Alfred Huger	Sourcefire
Barry Greene	ISC
Bill McInnis	IID
Bill Smith	PayPal
Brian Done	Département de la sécurité intérieure
Chris Roosenraad	Time Warner Cable
Chris Sills	IID
Craig Spiezle	Alliance pour la confiance en ligne (OTA)
Daniel Bright	EMC
Eric Osterweil	Verisign
Gabe Iovino	REN-ISAC
Greg Holzapfel	Sprint
Gunter Ollmann	Damballa
James Holgerson	Sprint
Jay Opperman	Comcast
Joe St Sauver	Université de l'Oregon et Internet2
Johannes Ullrich	Institut SANS
John Denning	Banque d'Amérique
John Griffin	Telecommunication Systems Inc.
John St. Clair	Verizon
Jon Boyens	Institut national des normes et de la technologie
Kevin Sullivan	Microsoft
Kurian Jacob	FCC
Matt Carothers	Cox
Maxim Weinstein	StopBadware
Merike Kaeo	ISC
Michael Fiumano	Sprint
Michael Glenn	CenturyLink
Robert Mayer	USTelecom
Tice Morgan	T-Mobile
Tim Rohrbaugh	Intersections
Timothy Vogel	Verizon

Tableau 1 - Liste des membres du groupe de travail 7

3 Objectif, portée et méthodologie

2.3 Objectif

Le CSRIC a chargé le groupe de travail 7, Botnet Remediation, de proposer un ensemble de pratiques volontaires convenues qui constitueraient le cadre d'un modèle de mise en œuvre opt-in à suivre par les FAI afin d'atténuer la menace des botnets. En réponse, le code de conduite anti-bot américain pour les FAI a été développé pour répondre à la menace des bots et des botnets dans les réseaux résidentiels à large bande par une participation volontaire.

2.4 Portée

Cette section identifie l'énoncé du problème, la description du groupe de travail, et les livrables décrits dans la charte CSRIC III pour le groupe de travail 7.

Énoncé du problème : La croissance des dispositifs d'utilisateurs finaux infectés par des robots2 représente une menace significative pour la vitalité et la résilience de l'Internet et de l'économie en ligne. Les réseaux de zombies sont des réseaux de dispositifs informatiques d'utilisateurs finaux connectés à l'internet et infectés par des logiciels malveillants, qui sont contrôlés à distance par des tiers à des fins malveillantes. Les bots et les réseaux de bots peuvent entraîner le vol d'informations personnelles, des attaques contre des réseaux publics et privés et l'exploitation de la puissance de calcul et de l'accès à l'internet des utilisateurs finaux.

Afin de réduire les infections par des bots dans les appareils des utilisateurs finaux résidentiels et d'atténuer l'exploitation potentielle des bots, les membres du groupe de travail 7 ont élaboré le code de conduite anti-bot volontaire des États-Unis pour les fournisseurs de services Internet.

Groupe de travail 7 Description : Ce groupe de travail examinera les efforts entrepris au sein de la communauté internationale, tels que le code de pratique australien de l'industrie de l'Internet, et parmi les groupes d'intervenants nationaux, tels que l'IETF et le Messaging Anti-Abuse Working Group, pour leur applicabilité aux ISP américains. En s'appuyant sur les travaux du groupe de travail 8 du CSRIC II sur les pratiques de protection des réseaux des FAI, le groupe de travail sur la remédiation des botnets proposera un ensemble de pratiques volontaires convenues qui constitueront le cadre d'un modèle de mise en œuvre opt-in pour les FAI. Le groupe de travail proposera une méthode permettant aux FAI d'exprimer leur intention d'adhérer au cadre proposé par le groupe de travail. Le groupe de travail identifiera également les obstacles potentiels à la mise en œuvre du code nouvellement rédigé par les FSI et identifiera les mesures que la FCC peut prendre pour aider à surmonter ces obstacles. Enfin, le groupe de travail identifiera des mesures de performance pour évaluer l'efficacité du code à freiner la propagation des infections par les zombies.

[2] Les termes "bot" et "infection par un bot" sont utilisés indifféremment dans ce document.

Livrables du rapport :

1. Code de conduite anti-bot pour les FAI des États-Unis : 22 mars 2012
2. Obstacles à la participation au code : 12 septembre 2012
3. Mesures de performance de la remédiation des bot : 5 décembre 2012

Ce rapport, intitulé U.S. Anti-Bot Code of Conduct for ISPs, est le premier de trois rapports livrables pour le groupe de travail 7.

2.5 Méthodologie

Le groupe de travail 7 a commencé ses recherches sur l'élaboration d'un code de conduite anti-bot volontaire américain pour les FAI en réunissant une équipe d'experts de l'industrie, du gouvernement et du milieu universitaire, représentant diverses parties prenantes dans l'élaboration et la mise en œuvre du code. Le groupe de travail 7 a examiné les efforts entrepris au sein de la communauté internationale, y compris le code de pratique australien de l'industrie de l'Internet et le centre japonais Cyber Clean, et parmi les groupes de parties prenantes nationales, y compris l'Internet Engineering Task Force (IETF) et le Messaging Anti-Abuse Working Group, pour l'applicabilité aux ISP américains. S'appuyant sur les travaux du groupe de travail 8 du CSRIC II, Pratiques de protection du réseau des ISP, le groupe de travail 7 du CSRIC III a établi des conférences téléphoniques bihebdomadaires entre ses membres pour discuter du développement, du contenu et de la pertinence des efforts connexes en vue de l'établissement d'un code de conduite anti-bot américain pour les ISP. Le groupe de travail 7 a coordonné ses efforts d'élaboration du code avec le département du commerce et le personnel de la sécurité nationale de la Maison Blanche par le biais de conférences téléphoniques régulières afin de discuter des domaines d'intérêt commun en matière de remédiation des botnets. Le groupe de travail 7 a organisé deux réunions en face à face avec ses membres, l'une en novembre 2011 pour développer la structure et discuter du contenu des sections du projet de code, et une dernière réunion en face à face en février 2012 pour examiner le projet de code final. Le code de conduite anti-bot américain pour les fournisseurs de services Internet qui en résulte est basé sur la contribution collective des membres du groupe de travail 7 et sur les discussions que ces membres et leurs entreprises ont eues avec d'autres parties prenantes pour réduire l'incidence des infections par les robots.

3 Contexte3

Un "bot" malveillant ou potentiellement malveillant est un programme installé sur un système afin de permettre à ce système d'exécuter automatiquement (ou semi-automatiquement) une tâche ou un ensemble de tâches, généralement sous le commandement et le contrôle d'un administrateur distant malveillant, ou "bot master". Les bots sont également connus sous le nom de "zombies". Ces robots peuvent avoir été installés subrepticement, sans que l'utilisateur comprenne bien ce qu'ils feront une fois installés, à son insu, dans le cadre de l'installation d'un autre logiciel, sous de faux prétextes ou de diverses autres manières.

Les appareils utilisés par les internautes peuvent être infectés par des logiciels malveillants qui peuvent contenir ou installer un ou plusieurs bots sur un appareil. Ils peuvent poser un problème majeur pour plusieurs raisons. Tout d'abord, ces bots peuvent être utilisés pour envoyer du spam, dans certains cas de très gros volumes de spam. Ce spam peut entraîner des coûts supplémentaires pour les FAI en termes de gaspillage de ressources réseau, de serveurs ou de personnel, entre autres.

[3] Voir les recommandations pour la remédiation des bots dans les réseaux des FAI, http://tools.ietf.org/rfc/rfc6561.txt.

de nombreux autres coûts et effets secondaires potentiels. Ces spams peuvent également nuire à la réputation du fournisseur d'accès, de ses clients et de l'espace d'adressage IP utilisé par le fournisseur d'accès (souvent appelé simplement "réputation IP").

En outre, ces bots peuvent servir de plates-formes pour diriger, participer ou mener des attaques sur des infrastructures Internet critiques. Les bots sont fréquemment utilisés dans le cadre d'attaques coordonnées par déni de service distribué (DDoS) pour des motifs criminels, politiques ou autres.

Le rôle des FAI dans la fourniture de services aux utilisateurs d'Internet les place en position de pouvoir tenter de détecter et d'observer les botnets opérant sur leurs réseaux. En outre, les FAI peuvent également être en mesure d'informer leurs clients d'une infection réelle, potentielle ou probable par des bots.

Du point de vue de l'utilisateur final, le fait d'être informé qu'un dispositif infecté se trouve sur son réseau constitue une information importante. Une fois qu'ils le savent, ils peuvent prendre des mesures pour supprimer les bots, résoudre les problèmes qui peuvent résulter de l'infection par le bot et se protéger contre les menaces futures.

Le groupe de travail 7 a élaboré le code de conduite anti-bot volontaire des États-Unis à l'intention des FAI afin de lutter contre la menace des bots et des botnets, décrite ci-dessus, dans les réseaux résidentiels à large bande. L'adoption de ce code par les ISP est volontaire. Elle n'est pas obligatoire.

4 Recommandations

4.1 Recommandations

Le groupe de travail a proposé un ensemble de pratiques volontaires convenues qui constitueraient le cadre d'un modèle de mise en œuvre opt-in pour les FAI afin de contribuer à la lutte contre la menace des botnets. Le groupe de travail recommande des mesures que les FAI offrant un accès Internet résidentiel à large bande peuvent prendre s'ils choisissent d'adopter le code. Le groupe de travail recommande en outre aux FAI et aux autres fournisseurs de services d'indiquer qu'ils acceptent de participer au code volontaire en contactant l'organisation industrielle qui gère en dernier ressort la participation au code. En tant que code de conduite volontaire élaboré par l'industrie et pour l'industrie, l'objectif est qu'un forum industriel neutre reçoive et rassemble les rapports relatifs à la participation au code.
Dans un premier temps, pour indiquer leur participation, il est suggéré aux ISP et autres fournisseurs de services participants de notifier à l'entité de leur choix leur participation au Code ou de s'auto-affirmer sur leur propre site web.

5.1.1 Travaux futurs

Ce rapport, le code de conduite anti-bot volontaire des États-Unis pour les fournisseurs de services Internet, est le premier de trois rapports livrables pour le groupe de travail 7. Il reste à aborder l'administration à long terme du code et les mises à jour périodiques. Ensuite, le groupe de travail identifiera les obstacles potentiels à la participation au code. Enfin, le groupe de travail identifiera les mesures de performance potentielles en matière de lutte contre les robots.

Les travaux futurs devraient porter sur les mécanismes de diffusion des infections par les zombies à partir de sites web et de services d'hébergement infectés et malveillants, afin que les efforts du GT7 deviennent omniprésents et donc efficaces.

5.1.2 Remerciements

Le GT7 souhaite remercier Yurie Ito du CERT japonais pour sa présentation informative et sa discussion sur les leçons tirées du Japan Cyber Clean Center, le programme anti-botnet du Japon. Nous remercions également Ari Schwartz du National Institute of Standards (NIST) pour sa présentation sur la menace des botnets et les stratégies d'atténuation. Le GT7 remercie également Microsoft, le MAAWG et la FCC pour avoir accueilli les réunions du GT7.

Le GT 7 tient à remercier tout particulièrement les membres suivants du groupe dont les efforts soutenus ont contribué massivement au processus d'élaboration du Code :

Robert Thornberry, de Bell Labs, Alcatel-Lucent (éditeur) Paul
Diamond, CenturyLink (éditeur)
Joe St Sauver, Université de l'Oregon et Internet2 (Glossaire) Neil
Schwartzman, CAUCE (Secrétaire)

5 Conclusions

En réponse à la mission confiée par le CSRIC III au groupe de travail 7, le code de conduite anti-bot volontaire américain pour les FAI a été développé pour répondre à la menace des bots et des botnets dans les réseaux résidentiels à large bande par une participation volontaire. Lors de l'élaboration du code, il a été déterminé que les composants de l'ensemble de l'écosystème Internet ont des rôles importants à jouer dans la lutte contre la menace des botnets et que les FAI dépendent du soutien des autres parties de l'écosystème.

Ce rapport du 22 mars 2012, intitulé U.S. Anti-Bot Code of Conduct for ISPs, est le premier de trois rapports livrables pour le groupe de travail 7. Ensuite, le groupe de travail identifiera les obstacles potentiels à la participation au code, avec un rapport à venir en septembre 2012. Enfin, le groupe de travail identifiera les paramètres de performance de l'élimination des botnets et soumettra son rapport sur ce sujet en décembre 2012.

6 Annexe

Code de conduite anti-bot (ABC) des États-Unis à l'intention des fournisseurs de services Internet (FSI) pour lutter contre l'activité des robots dans les réseaux à large bande

Final 22
mars 2012

1. Introduction

La croissance des *dispositifs d'utilisateurs finaux *infectés par des bots représente une menace significative pour la vitalité et la résilience de l'Internet et de l'économie en ligne. Notez que les termes "infection par un bot" et "bot" sont utilisés comme synonymes dans ce document pour désigner un dispositif d'utilisateur final infecté par un logiciel malveillant de type bot. Les réseaux de zombies sont des réseaux d'appareils informatiques d'utilisateurs finaux connectés à Internet et infectés par des logiciels malveillants de zombies.*qui sont contrôlés à distance par des tiers à des fins malveillantes.

Les bots et les réseaux de bots peuvent entraîner le vol d'informations personnelles, des attaques contre des réseaux publics et privés et l'exploitation de la puissance de *calcul et de l'accès à l'internet des utilisateurs finaux. Le public est peu sensibilisé aux bots, à leur impact et aux problèmes de sécurité et de confidentialité qui en découlent. Ce code de conduite volontaire (le "Code") fournit un ensemble de principes et d'activités recommandés que les fournisseurs de services Internet peuvent adopter pour aider à faire face aux menaces présentées par la présence de bots et de botnets dans les réseaux résidentiels à large bande.

Il convient de reconnaître que les bots ont un impact sur l'ensemble de l'écosystème Internet *et que pour réussir à les réduire ou à atténuer leur impact, il faudra une action collective de toutes les parties de cet écosystème, notamment les utilisateurs finaux, les développeurs de logiciels, les fournisseurs de services de recherche, les sites Web, les sites de commerce électronique, etc. Les dispositifs des utilisateurs finaux échappent au contrôle des FAI, c'est *pourquoi tous les participants de l'écosystème Internet doivent travailler ensemble pour résoudre ce problème. Le présent Code vise à jeter les bases d'une future coordination entre les différentes parties prenantes en définissant un ensemble d'actions adaptées au rôle limité que les FAI peuvent jouer pour contribuer à résoudre ce problème important.
Le Code reconnaît la variabilité substantielle de la taille, des ressources, des modèles et environnements commerciaux, de l'expertise et des capacités des FAI aux États-Unis. Le succès des activités des FSI repose sur des efforts similaires de la part des autres acteurs de l'Internet.

Les exigences fondamentales de la participation à ce code sont énoncées à la section 5. Les autres sections de ce document contiennent des informations de base ou des explications supplémentaires.

---

* Définition trouvée dans le glossaire

2. Définitions des termes clés

Note au lecteur :

Toute discussion sur les bots implique inévitablement un vocabulaire technique unique. Sachant que de nombreux lecteurs peuvent ne pas être familiers avec certains de ces termes spécialisés, le Code comprend un glossaire à l'annexe 2. Tout terme apparaissant dans le glossaire sera marqué d'un astérisque "*" dans le corps du texte du Code la première fois qu'il apparaîtra afin d'avertir le lecteur qu'une définition est disponible dans le glossaire.

3. Objectifs et principes

a. Les objectifs de ce code sont les suivants :

1. Fournir un cadre initial permettant aux FAI de mieux comprendre et d'aider à résoudre le problème des bots ; et

2.

• Informez les utilisateurs finaux de la menace que représentent les bots et des mesures qu'ils peuvent prendre pour prévenir les infections par les bots ;

• Détecter les activités des robots ou obtenir des informations, y compris auprès de tiers crédibles, sur les infections par des robots dans leur base d'utilisateurs finaux ;

• notifier aux utilisateurs finaux les infections suspectées par des bots ou aider les utilisateurs finaux à déterminer s'ils sont potentiellement infectés par des bots ; et

• Fournir des informations et des ressources, directement ou par référence à d'autres sources, aux utilisateurs finaux pour les aider à remédier aux infections par des robots.

b. La mise en œuvre du code sera guidée par les principes suivants :

1. Volontaire - la participation est volontaire et encourage les types d'actions à entreprendre par les ISP, cependant ce code n'exige aucune activité particulière.

2. Neutralité technologique - ce code ne prescrit pas de moyens ou de méthodes particuliers.

3. Neutralité de l'approche - ce code ne prescrit aucune approche particulière pour la mise en œuvre d'une partie de ce code.

4. Respect de la vie privée - Les FAI doivent traiter les questions de vie privée d'une manière appropriée et conforme aux lois applicables.

5. Conformité juridique - les activités doivent être conformes au droit applicable.

6. Une responsabilité partagée - Les FAI, agissant seuls, ne peuvent pas répondre entièrement à la menace posée par les bots. Les autres participants de l'écosystème Internet doivent également faire leur part.

7. Durabilité - Les ISP doivent rechercher des activités qui sont rentables et durables dans le contexte de leurs modèles économiques.

8. Partage d'informations - Les FSI doivent indiquer comment ils participent au Code et partager les enseignements tirés de leurs activités avec les autres parties prenantes appropriées. Tout partage d'informations entre les ISP et les autres parties concernées doit être effectué conformément aux lois applicables, y compris, mais sans s'y limiter, les lois antitrust et sur la protection de la vie privée.

9. Efficacité - Les PSI doivent être encouragés à s'engager dans des activités qui ont été démontrées comme étant appropriées et efficaces.

10. Communication efficace - La communication avec les clients *doit tenir compte de diverses questions telles que la langue et s'assurer que les informations sont fournies d'une manière dont on peut raisonnablement penser qu'elle sera comprise et accessible par les destinataires.

4. Champ d'application et rôles

Ce Code a été rédigé spécifiquement pour les ISP et autres fournisseurs de services offrant un service d'accès Internet à large bande aux utilisateurs finaux résidentiels. Les activités de ce Code peuvent être adaptées pour être utilisées par d'autres fournisseurs d'accès Internet et participants.

Ce code n'est pas censé être une approche globale de la sécurité en ligne, mais il est destiné à coexister avec d'autres efforts actuels et futurs. Il prévoit un rôle important pour les autres participants de l'écosystème Internet, y compris, mais sans s'y limiter :

- Vendeurs de logiciels de sécurité
- Développeurs de systèmes d'exploitation
- Organisations axées sur l'utilisateur final
- Fournisseurs de contenu, d'applications et de services Internet

La sécurité en ligne doit inclure une approche flexible et à multiples facettes, utilisant des conseils et des outils provenant de diverses sources réputées.

a. Définition du succès

Le succès initial de ce code sera évalué en fonction de la participation de la communauté des FAI. Cependant, le soutien de l'écosystème Internet dans son ensemble est considéré comme primordial pour le succès final de la lutte contre les bots.

b. Avantages de la participation au code

Les avantages de haut niveau suivants peuvent résulter d'une participation significative des PSI à ce code :

- Sécurité accrue des informations et des appareils des utilisateurs finaux et de l'infrastructure américaine ;
- Sensibilisation accrue des utilisateurs finaux, des fournisseurs d'accès à Internet et des autres acteurs du secteur de l'Internet à la menace des robots et à la manière de la combattre ;

---

* Définition trouvée dans le glossaire

- Notification* et remédiation* de l'activité des robots sur les appareils des utilisateurs finaux infectés par des robots ;
- Création d'un environnement dans les réseaux résidentiels à large bande américains qui est encore plus hostile au déploiement et à l'utilisation des bots ; et
- Développement et utilisation plus large d'architectures et d'outils de notification et de remédiation efficaces chez les utilisateurs finaux et les FAI.

Certains FAI participant au processus d'élaboration du Code et ayant déjà mis en œuvre certains de ses aspects ont obtenu des résultats bénéfiques dans des domaines tels que la diminution du nombre d'appels aux services d'assistance de la part de clients dont les machines sont infectées, la réduction de la consommation de la bande passante en amont par les attaques par déni de service et le spam*une augmentation de la clientèle et une diminution du taux de désabonnement, ainsi qu'une réduction des plaintes liées au spam de la part d'autres FAI. Bien que les résultats individuels puissent varier, les FAI sont encouragés à rechercher les moyens spécifiques par lesquels la participation au Code renforce leur activité globale en matière de large bande, et à partager ces expériences avec d'autres FAI. En outre, la participation des ISP à ce Code peut permettre aux ISP de générer des mesures tangibles relatives à l'impact d'activités spécifiques sur les opérations commerciales à large bande globales des ISP, ce qui peut à son tour soutenir le développement ou le déploiement d'autres activités anti-bot.

* Définition trouvée dans le glossaire

5. Paramètres de participation

La participation à ce code est volontaire.

Exigences de participation au Code de Conduite Volontaire

Pour participer à ce Code, un ISP s'engagera dans au moins une activité (c'est-à-dire qu'il prendra des mesures significatives) dans chacun des domaines généraux suivants :

- Éducation - activité visant à sensibiliser les utilisateurs finaux aux problèmes des botnets et à la manière de prévenir les infections par ces derniers ;
- Détection - activité visant à identifier l'activité des botnets dans le réseau du FAI, à obtenir des informations sur l'activité des botnets dans le réseau du FAI ou à permettre aux utilisateurs finaux de déterminer eux-mêmes les infections potentielles par des botnets sur leurs appareils ;
- Notification - activité destinée à informer les clients des infections suspectes par des robots ou à permettre aux clients de déterminer s'ils sont infectés par un robot ;
- Remédiation - activité destinée à fournir des informations aux utilisateurs finaux sur la façon dont ils peuvent remédier aux infections par des robots, ou à aider les utilisateurs finaux à remédier aux infections par des robots.
- Collaboration - une activité visant à partager avec d'autres PSI le retour d'information et l'expérience acquise dans le cadre des activités du Code du PSI participant.

La notion d'"au moins une activité" dans chacun de ces domaines généraux vise à encourager un certain niveau d'activité dans chacun des cinq domaines susmentionnés dans le cadre d'un processus national global visant à créer un environnement dans les réseaux résidentiels à large bande américains qui soit encore plus hostile au déploiement et à l'utilisation des bots. L'objectif est de soutenir et d'encourager un large éventail d'efforts flexibles pour expérimenter et innover avec diverses méthodes d'éducation, de détection, de notification et de remédiation.*de détection, de notification et de remédiation. Dans le même ordre d'idées, l'obligation de partager le retour d'information avec d'autres FAI ne vise pas à imposer des moyens ou des méthodes spécifiques de partage de ce retour d'information.

* Définition trouvée dans le glossaire

6. Éducation des utilisateurs finaux

a. Vue d'ensemble

Les utilisateurs finaux sont responsables en dernier ressort de la protection de leurs appareils et de l'élimination d'un appareil infecté. Les FAI, comme de nombreux autres participants à l'Internet et acteurs gouvernementaux, peuvent aider à éduquer les utilisateurs finaux sur les menaces présentées par les bots et les mesures que les utilisateurs finaux peuvent prendre pour protéger leurs appareils et remédier aux infections.

b. Action recommandée :

1. Éducation à la prévention du bot*:

Les fournisseurs de services Internet doivent mettre à disposition des informations sur la prévention des infections par les robots et les questions connexes. Au minimum, ces informations devraient inclure :

- Comment et pourquoi les utilisateurs finaux doivent maintenir leurs logiciels à jour pour les ordinateurs et les appareils dont les mises à jour logicielles sont facilement accessibles.
- L'importance d'utiliser un logiciel de sécurité efficace et à jour provenant d'un fournisseur réputé.
- L'importance de sauvegarder les données et les logiciels des utilisateurs et comment le faire efficacement.
- Actions de base de l'utilisateur final pour minimiser l'exposition aux infections par des robots lors de l'utilisation d'Internet.

On s'attend à ce que de nombreux ISP puissent atteindre cet objectif en fournissant ces informations directement à leurs abonnés ou en établissant des liens avec des sources existantes et accessibles au public.

2. Soutien aux efforts de remédiation des bots des utilisateurs finaux :

En plus des informations sur la prévention, les FAI devraient mettre à disposition (par exemple, par le biais de leurs publications, de publications de tiers ou de liens Internet) des informations sur la manière dont les utilisateurs finaux peuvent généralement remédier aux infections par des robots. Dans ce domaine, les FAI devraient être en mesure d'atteindre cet objectif en créant des liens vers des sources d'information existantes et accessibles au public ou en créant de nouvelles sources d'information, soit individuellement, soit en collaboration avec d'autres.

Dans le cadre de leurs activités de notification aux utilisateurs finaux, les FAI devraient inclure dans ces notifications ou par d'autres moyens des informations sur les endroits où le destinataire peut se tourner pour obtenir des informations et une assistance supplémentaires. Ces informations peuvent inclure des liens vers des informations en ligne accessibles au public, des outils de sécurité ou des suggestions pour obtenir l'aide d'un professionnel de l'informatique. Les sujets et références supplémentaires qu'un ISP pourrait souhaiter inclure sont les suivants :

---

* Définition trouvée dans le glossaire

- Risques pour l'utilisateur final et la communauté Internet d'utiliser un appareil que l'on pense infecté,
- Comment identifier et supprimer les formes courantes d'infections par des robots,
- des outils ou des services accessibles au public (gratuits ou payants) pour faciliter la détection et la suppression des infections par des robots, et
- Des conseils pour savoir où trouver une assistance supplémentaire (gratuite ou payante).

3. Directives :

Pour répondre aux exigences ci-dessus, les FAI doivent tenir compte des directives suivantes :

- Offrir des informations et des ressources éducatives directement ou en renvoyant à des services tiers.
- Faites en sorte que le contenu éducatif soit concis et se concentre sur les éléments les plus importants que les utilisateurs doivent connaître.
- S'assurer que les instructions peuvent être suivies par un public d'utilisateurs non techniques.
- Utilisez plusieurs médias, par exemple des images, des vidéos, du texte, des légendes, etc., et, le cas échéant, plusieurs langues pour optimiser la compréhension et l'accessibilité des clients.
- Aidez les utilisateurs finaux à déterminer s'ils sont infectés par un bot en fournissant des informations ou en pointant vers des ressources qui décrivent les comportements anormaux des appareils infectés par un bot et la disponibilité et l'utilisation d'outils ou de services logiciels de détection des bots.

7. Détection de bot

a. Vue d'ensemble

Les outils et techniques utilisés pour détecter les bots évoluent au même rythme que ceux-ci. Le défi de la détection réside dans la polyvalence que le trafic des bots a atteint pour éviter de nombreuses techniques singulières utilisées pour les mécanismes de détection, comme la simple correspondance de motifs. La détection peut être compliquée par le fait que certaines applications Internet, comme les réseaux de diffusion de contenu en cache basés sur l'hôte distribué, les applications de jeux en ligne et d'autres services de ce type, peuvent avoir un comportement similaire à celui des bots malveillants et utiliser des technologies similaires. Les fournisseurs d'accès à Internet doivent veiller à identifier les parties touchées afin de les notifier et d'y remédier.

b. Action recommandée :

Les FAI peuvent s'informer sur les activités malveillantes et les appareils d'utilisateurs finaux compromis par des robots de différentes manières :

1. Recevoir des notifications d'entités externes, notamment celles conçues pour aider à la compréhension globale et à la diffusion en temps réel des données relatives aux bots. Une liste de ressources est présentée à l'annexe 2.

2. Déployer au sein de leurs réseaux des capacités permettant d'identifier les infections potentielles par des robots.

3. Orienter les clients vers des outils, un portail web ou d'autres ressources qui leur permettent d'identifier eux-mêmes une infection potentielle par un bot.

8. Notification à l'utilisateur final d'une infection potentielle par un bot

a. Vue d'ensemble :

De nombreux utilisateurs finaux ne savent pas que leurs appareils sont infectés et fonctionnent comme des robots. Par conséquent, ces utilisateurs et leurs données restent à risque, et les bots peuvent rester actifs indéfiniment. Les fournisseurs de services Internet devraient tirer parti des efforts de détection décrits à la section 7 pour informer les clients des infections actives.

Les notifications doivent être conçues pour aider à limiter les bots et les dommages qu'ils causent. Les notifications peuvent contenir des informations sur ce qu'est un bot, les moyens d'infection, le fait que les bots peuvent ne présenter aucun symptôme visible et la signification de la notification. Les notifications peuvent également contenir ou identifier d'autres ressources telles que des outils, des guides et des services qui facilitent la prévention, la vérification et l'atténuation des infections.*. Elles peuvent également fournir des informations sur un ou plusieurs bots spécifiques détectés.

La notification à l'utilisateur final peut prendre de nombreuses formes différentes. Elle peut être effectuée directement par le FAI ou par des tiers pour le compte du FAI. Les FAI peuvent alerter directement les utilisateurs finaux ou fournir des mécanismes permettant aux utilisateurs finaux de demander et de recevoir des informations sur l'état de leur infection. De même, les FAI peuvent conclure des accords pour que les notifications soient transmises aux utilisateurs finaux par d'autres participants de l'écosystème avec lesquels l'utilisateur final est en relation, comme un fournisseur d'applications ou de services Internet.

Le fournisseur de services Internet devrait envisager des mécanismes qui garantissent que le client peut facilement authentifier l'authenticité des notifications et que ces notifications seront difficiles à falsifier.

Dans la mesure du possible, le PSI peut souhaiter suivre la réception des notifications. Cela peut aider le FAI à mieux comprendre l'efficacité des différents mécanismes de notification.

Chaque fournisseur de services Internet devra évaluer différentes méthodes de notification afin de trouver celle qui est la mieux adaptée à son cas particulier et à la menace que représentent les robots. La méthode de notification choisie devra peut-être s'intégrer aux processus opérationnels et au réseau existants.

---

* Définition trouvée dans le glossaire

l'infrastructure. Des recherches et des analyses peuvent être nécessaires pour développer et maintenir des systèmes et des politiques de notification appropriés.

b. Action recommandée :

Communiquer au client une suspicion d'infection par un bot ou aider les clients à déterminer s'ils sont potentiellement infectés par des bots. De nombreuses méthodes de notification sont décrites dans les références de l'annexe 2 ; toutefois, d'autres méthodes peuvent être utilisées.

9. Remédiation du bot

a. Vue d'ensemble

L'atténuation et l'élimination des zombies sont l'objectif ultime de tout programme de notification d'infection par des zombies et relèvent en fin de compte de la responsabilité de l'utilisateur final. La notification seule peut être suffisante pour les utilisateurs techniques, mais la majorité des utilisateurs ont généralement besoin d'une certaine forme d'assistance pour supprimer les logiciels malveillants de leurs appareils infectés. La remédiation peut toutefois s'avérer difficile et impliquer d'autres fonctions complexes, telles que l'isolement de la source de l'infection parmi de nombreux appareils partageant une connexion Internet, la sauvegarde préalable de toutes les données et de tous les logiciels système de manière à préserver la capacité de récupération de l'utilisateur final (sans toutefois sauvegarder également les fichiers ou programmes infectés) et la garantie que l'utilisateur final dispose de disques sources et d'autres éléments permettant de reconstruire l'image de son appareil si nécessaire au cours du processus de remédiation.

Il est entendu que certains fournisseurs de services Internet ne disposent pas des ressources nécessaires pour fournir ce niveau de service, ni ne sont en mesure de prendre en charge ces activités gratuitement ou même contre rémunération. Dans de nombreux cas, les utilisateurs finaux devront être orientés vers des fournisseurs de services professionnels d'assistance informatique pour remédier complètement à leurs machines. Les notifications des FAI peuvent anticiper ce fait et suggérer aux clients de rechercher l'assistance d'un tiers afin d'éviter de frustrer les utilisateurs finaux avec des services d'assistance limités ou des lignes d'assistance qui ne sont pas capables ou équipés pour résoudre complètement les problèmes de remédiation.

b. Action recommandée :

1. Les bots sont conçus pour être furtifs et difficiles à supprimer. Dans le cadre de la notification, les FAI devraient offrir des conseils, comme décrit ci-dessus. Il peut s'agir de liens vers diverses sources d'information, de logiciels et d'outils en ligne ou provenant de tiers, accessibles au public. Il peut également s'agir de liens vers des services professionnels. Ceux-ci ne doivent pas nécessairement être proposés par le FAI lui-même, mais peuvent l'être par des tiers.

2. Un ISP peut fournir des outils de remédiation à l'utilisateur final, soit pendant, soit après le processus de notification. Cependant, le FAI ne doit pas obliger l'utilisateur final à exécuter les outils de remédiation. Si le FAI fournit des outils à l'utilisateur final, celui-ci doit être autorisé à quitter le processus sans exécuter les outils ou procédures suggérés.

3. Dans le cadre de la procédure de notification, les FAI peuvent souhaiter inclure des indications (en fonction de la nature du bot en question) selon lesquelles les paramètres des équipements de réseau appartenant aux clients, tels que les passerelles et les routeurs domestiques, peuvent avoir été modifiés.

a été altéré et doit être restauré dans un état sécurisé, selon la nature de l'infection par le bot.

c. Directives :

1. Les outils et services de suppression des robots doivent respecter la vie privée des utilisateurs.

2. Les méthodes possibles de remédiation aux infections sont décrites dans les meilleures pratiques du CSRIC II WG 8 et dans le bot remediation IETF RFC qui sont référencés dans l'annexe 2.

10. Collaboration ISP

a. Vue d'ensemble :

L'atténuation et la gestion du bot sont des activités dans lesquelles les FAI, les fournisseurs de recherche, les utilisateurs finaux, les services informatiques, les sociétés d'hébergement, les fournisseurs de blogs, les fournisseurs de sécurité, les chercheurs, les pouvoirs publics, les sociétés de services financiers, les fournisseurs de services en nuage et d'autres parties ont tous un rôle à jouer. Grâce à la contribution et à la collaboration de plusieurs parties prenantes, les résultats seront supérieurs à ceux que l'on pourrait obtenir par des actions indépendantes seules. La participation des FAI à ce code, ainsi que les approches complémentaires et collaboratives adoptées par d'autres segments de l'écosystème Internet, devraient permettre de réduire considérablement la menace que représentent les botnets.

b. Action recommandée :

La participation au code exige une collaboration au sein de l'ISP, de l'industrie ou de forums plus larges par le biais d'activités de collaboration, dont voici quelques exemples :

1. Partager les méthodes de détection, de notification ou d'atténuation prévues ou déployées dans les réseaux des FAI et, le cas échéant, une évaluation de leur efficacité.

2. Partage de renseignements ou de données opérationnelles sur les attaques qui peuvent être utiles à la prévention, à la défense ou à l'élimination des zombies.

3. Identification des données clés ou des ressources techniques qui sont nécessaires de la part des systèmes ou des acteurs au-delà du réseau des ISP.

4. Participation à la définition, au développement ou à l'exploitation de stratégies ou de systèmes de défense intégrés qui dépassent les limites du réseau ISP.

5. Autres activités de collaboration impliquant le partage d'informations avec des parties extérieures au PSI ou de données avec des systèmes extérieurs au réseau du PSI.

Tout partage d'informations entre les FAI et les autres parties concernées sera effectué conformément aux lois applicables, y compris, mais sans s'y limiter, les lois antitrust et les lois sur la protection de la vie privée.

11. Développement ultérieur du présent code

Ce code évoluera au fil du temps en raison de la nature dynamique de la menace des bots et de l'expérience et de l'évaluation des FAI.

12. Informations et ressources supplémentaires

Annexe 1 - Glossaire Annexe 2 -
Références

Annexe 1 - Glossaire :

1. Bot

La définition suivante s'inspire largement des "Recommandations pour la remédiation des bots dans les réseaux des fournisseurs de services Internet" (référencées à l'annexe 2) :

Un "bot" malveillant (ou potentiellement malveillant) (dérivé du mot "robot", ci-après simplement appelé "bot") désigne un programme installé sur un système afin de permettre à ce système d'exécuter automatiquement (ou semi-automatiquement) une tâche ou un ensemble de tâches, généralement sous le commandement et le contrôle d'un administrateur distant (souvent appelé "bot master" ou "bot herder").

Les systèmes informatiques et autres dispositifs d'utilisateur final qui ont été "botté" sont aussi souvent appelés "zombies".

Les robots malveillants sont généralement installés subrepticement, sans le consentement de l'utilisateur ou sans que celui-ci comprenne parfaitement ce que son système pourrait faire une fois le robot installé.

Les bots sont souvent utilisés pour envoyer des courriers électroniques indésirables ("spam"), pour reconnaître ou attaquer d'autres systèmes, pour écouter le trafic réseau ou pour héberger des contenus illégaux tels que des logiciels piratés, du matériel d'exploitation des enfants, etc.

De nombreuses juridictions considèrent l'infection involontaire des hôtes des utilisateurs finaux comme un exemple d'intrusion informatique illégale.

2. Botnet

Les botnets sont des réseaux d'appareils informatiques d'utilisateurs finaux connectés à l'internet et infectés par des logiciels malveillants, qui sont contrôlés à distance par des tiers à des fins malveillantes.
Un botnet est sous le contrôle d'un "botherder" ou "botmaster" donné. Un réseau de zombies peut compter une poignée d'hôtes zombifiés ou des millions.

3. Client (ou "client direct")

La partie qui passe un contrat avec un ISP pour un service. Distinguez le "client" de l'"utilisateur autorisé" : par exemple, un café peut acheter un service Internet à un ISP. Le café serait le client du FSI. Le café peut choisir d'offrir l'utilisation gratuite de sa connexion (si la politique d'utilisation acceptable du FSI l'autorise) à ceux qui lui achètent du café - les acheteurs de café seraient alors des utilisateurs autorisés de la connexion achetée par le café, mais pas le client direct du FSI.

4. Détection

La détection est le processus par lequel un fournisseur de services ou un utilisateur final prend conscience qu'un système ou un appareil particulier a été infecté par un logiciel malveillant. Un fournisseur de services peut détecter qu'un système a été infecté de différentes manières, notamment en recevant des plaintes de tiers concernant des spams, des analyses de réseau ou des attaques provenant de ce système. Les utilisateurs finaux peuvent détecter les infections du système au moyen d'outils logiciels ou d'autres moyens.

5. Écosystème

Ce terme est souvent utilisé pour décrire les relations entre les différents participants à l'internet, à savoir les fabricants de matériel, les développeurs de logiciels, les fournisseurs d'accès à Internet et les fournisseurs de contenu, d'applications et de services internet qui permettent à l'internet de fonctionner et d'être utile aux utilisateurs finaux.

L'écosystème Internet comprend des fournisseurs de systèmes d'exploitation, des organisations axées sur l'utilisateur final, des fournisseurs de contenu, d'applications et de services Internet, des FAI, des fournisseurs de recherche, des utilisateurs finaux, des services informatiques, des sociétés d'hébergement, des fournisseurs de blogs, des fournisseurs de sécurité, des chercheurs, des gouvernements, des sociétés de services financiers et d'autres parties.

L'économie dite "souterraine" est aussi souvent décrite comme un "écosystème", avec de multiples participants remplissant divers rôles spécialisés. Par exemple, certains participants peuvent se spécialiser dans l'écriture de logiciels malveillants, tandis que d'autres peuvent "récolter" des adresses électroniques à partir de pages Web et de listes de diffusion, et d'autres encore peuvent se spécialiser dans la distribution de logiciels malveillants aux adresses électroniques récoltées. L'écosystème des logiciels malveillants comprendra aussi normalement la population des victimes potentielles ciblées et les organismes chargés de l'application de la loi qui luttent contre la cybercriminalité.

6. Utilisateur final

Utilisateur final : dans un contexte informatique et de réseau, l'utilisateur final est la personne qui, en fin de compte, fait un usage autorisé d'un produit ou d'un service.

L'utilisateur final n'est souvent pas la même personne que celle qui a acheté le produit ou le service. Par exemple, le propriétaire d'un café peut acheter de la connectivité pour ses clients ; dans ce cas, ce sont les clients du café, et non le propriétaire, qui sont les véritables "utilisateurs finaux", même s'ils n'ont pas passé de contrat direct avec un FSI pour la connectivité qu'ils utilisent.

Une partie, telle qu'un hacker/cracker qui utilise un produit ou un service sans l'autorisation de l'acheteur, serait normalement considérée comme un cyber-intrus et non comme un "utilisateur final" en soi.

7. ISP

Un fournisseur d'accès à Internet (FAI) est une entreprise qui fournit un accès au détail à Internet pour les membres du public, ou pour les entreprises et autres organisations. Ces connexions peuvent se faire par câble, DSL, satellite, sans fil, par ligne commutée ou par d'autres technologies. Les FAI sont parfois aussi appelés "fournisseurs d'accès".

Une entreprise qui fournit un accès à l'Internet uniquement à ses propres employés ne serait normalement pas considérée comme un FSI. De même, un transporteur de réseau qui ne fournit qu'un accès en gros à l'Internet pour d'autres FSI serait normalement considéré comme un fournisseur de services de réseau (FRS), plutôt qu'un FSI.

8. Logiciel malveillant

"Malware" est l'abréviation de "logiciel malveillant".

Les robots malveillants sont un type de logiciels malveillants. Les autres formes de logiciels malveillants comprennent des catégories de logiciels connues sous le nom de virus, chevaux de Troie, vers, rootkits, crimeware, enregistreurs de frappe, composeurs, logiciels espions, logiciels publicitaires, etc. Les facteurs qui distinguent ces différents types de logiciels malveillants sont moins importants que la compréhension des raisons pour lesquelles les logiciels malveillants peuvent être considérés comme "malveillants".

Les logiciels malveillants violent souvent un ou plusieurs des principes fondamentaux suivants :

(a) Consentement : Un logiciel malveillant peut être installé même si l'utilisateur ne l'a pas demandé sciemment.

(b) Honnêteté : Les logiciels malveillants peuvent prétendre faire une chose, alors qu'ils font en réalité quelque chose de complètement différent.

(c) Vie privée-Respect de la vie privée : Les logiciels malveillants peuvent violer la vie privée d'un utilisateur, par exemple en capturant ses mots de passe ou ses informations de carte de crédit.

(d) Non-intrusivité : Les logiciels malveillants peuvent gêner les utilisateurs en faisant apparaître des publicités, en changeant la page d'accueil du navigateur, en rendant les systèmes lents ou instables et en les rendant susceptibles de tomber en panne, ou en interférant avec les logiciels de sécurité déjà installés.

(e) Inoffensivité : Les logiciels malveillants peuvent être des logiciels qui nuisent aux utilisateurs (par exemple, des logiciels qui endommagent notre système, envoient des spams ou désactivent les logiciels de sécurité).

(f) Respect de la gestion des utilisateurs : Si l'utilisateur tente de supprimer le logiciel, celui-ci peut se réinstaller ou passer outre les préférences de l'utilisateur.

Tout cela se résume à "un logiciel dont les utilisateurs ne veulent tout simplement pas".

Les utilisateurs peuvent installer des logiciels malveillants à leur insu en ouvrant une pièce jointe contaminée reçue par courrier électronique ou en visitant une page web au contenu malveillant. Les systèmes peuvent également être infectés directement par un attaquant à distance, ce dernier ayant ciblé une vulnérabilité connue qui peut être exploitée à distance, ou par l'utilisateur qui monte un CD, un DVD ou une clé USB infectés.

9. Atténuation

L'atténuation est le processus de gestion ou de contrôle des effets associés à un bot. Par exemple, si un système est infecté par un bot de spam et qu'il envoie des courriers électroniques commerciaux indésirables, l'atténuation peut consister à filtrer le spam émis par ce dispositif.

Notez que l'atténuation n'implique généralement pas la correction de la condition sous-jacente (ce serait la "remédiation") ; l'atténuation se contente de gérer les symptômes associés à une condition.

10. Notification

La notification est un processus par lequel les FAI communiquent avec leurs utilisateurs finaux concernant l'infection possible de l'appareil de l'utilisateur final par un bot malware ou la manière dont un abonné peut prévenir ou identifier une telle infection. La notification peut également impliquer un processus par lequel les utilisateurs finaux sont dirigés vers des outils qui leur permettront de découvrir eux-mêmes les infections par des robots. La notification peut prendre différentes formes, notamment une notification directe par le FAI à l'utilisateur final, ou une notification indirecte par le biais des outils d'autodécouverte disponibles ou d'un tiers. La notification peut être effectuée via plusieurs canaux potentiels, notamment (mais pas exclusivement) le courrier électronique, le courrier postal, un appel téléphonique, une notification dans le navigateur, un outil d'autodécouverte en ligne ou un message SMS.

11. Prévention

La prévention consiste à renforcer un système ou un service afin qu'il soit moins vulnérable à la compromission et à l'exploitation. Par exemple, sur de nombreux systèmes, la prévention peut impliquer :

- Mise à jour du système d'exploitation et de toutes les applications avec les correctifs de sécurité disponibles.
- Installation ou activation d'un pare-feu
- Utilisation d'un logiciel anti-virus
- S'assurer que le système est régulièrement sauvegardé
- Utiliser des mots de passe forts
- Désactiver tous les services réseau inutiles
- Encourager les utilisateurs à utiliser les services Internet en toute sécurité (par exemple, le courrier électronique, la navigation sur Internet, etc.)

12. Assainissement

La remédiation est le processus que suit l'utilisateur final pour nettoyer un ordinateur infecté afin qu'il ne le soit plus. Dans les cas simples, il s'agit d'installer et d'exécuter un produit anti-virus. Dans les cas plus difficiles, la remédiation peut impliquer une intervention plus substantielle allant jusqu'à "atomiser et paver" le système - le formater et le réinstaller à partir de zéro, ou au moins à partir de la dernière sauvegarde propre connue. Une fois que le système est propre ou qu'il a été réinstallé, il est normalement renforcé pour le protéger contre la réinfection.

13. Spam

Courriel non désiré et non demandé, souvent de nature commerciale, envoyé normalement à un grand nombre de destinataires sous une forme sensiblement identique. Le spam est souvent envoyé par des "affiliés" qui sont payés par la personne qui gère le programme d'affiliation lorsque les destinataires achètent le produit annoncé par le spam.

Annexe 2 - Références

1. Recommandations sur la manière de gérer les effets des ordinateurs infectés par des bots malveillants : "Recommandations pour la remédiation des bots dans les réseaux des ISP".

http://tools.ietf.org/rfc/rfc6561.txt

2. Groupe de travail 8 du CSRIC II - Meilleures pratiques en matière de protection des réseaux des ISP

http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PRO TECTION_20101213.pdf

3. icode - Code de pratique de l'industrie australienne de l'Internet concernant la cybersécurité

http://iia.net.au/images/resources/pdf/icode-v1.pdf

4. Japan Cyber Clean Center - Projet Anti-Botnet

https://www.ccc.go.jp/en_index.html

5. Centre consultatif anti-botnet allemand - Projet anti-botnet

https://www.botfrei.de/en/

6. Équipe japonaise d'intervention en cas d'urgence informatique

(CERT) http://www.jpcert.or.jp/english/

7. US CERT - Comprendre les menaces cachées : Rootkits et Botnets

http://www.us-cert.gov/cas/tips/ST06-001.html

8. Alliance for Telecommunications Industry Solutions (ATIS)

http://www.atis.org/

9. Département de la sécurité intérieure

http://www.dhs.gov/files/programs/gc_1158611596104.shtm

10. Département de la sécurité intérieure - Équipe de préparation aux situations d'urgence informatique des États-Unis

http://www.us-cert.gov/

11. Union internationale des télécommunications Botnet Mitigation Toolkit

http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

12. Institut national des normes et de la technologie (NIST) du département du commerce des États-Unis.

http://www.nist.gov/index.html

13. Demande d'information du ministère du Commerce et du ministère de la Sécurité intérieure - Modèles visant à promouvoir la notification volontaire des entreprises aux consommateurs concernant l'utilisation illicite de matériel informatique par des botnets et des logiciels malveillants connexes

http://www.gpo.gov/fdsys/pkg/FR-2011-09-21/pdf/2011-24180.pdf

14. Commentaires reçus en réponse à la demande d'information du ministère du Commerce et du ministère de la Sécurité intérieure - Modèles visant à promouvoir la notification volontaire des entreprises aux consommateurs concernant l'utilisation illicite d'équipements informatiques par des botnets et des logiciels malveillants connexes

http://www.nist.gov/itl/botnetcomments.cfm

15. Messaging Anti-Abuse Working Group (MAAWG.org) - Code de conduite

http://www.maawg.org/sites/maawg/files/news/CodeofConduct.pdf

16. Collection de bonnes pratiques du M3AAWG pour les ISP et les opérateurs de

réseau http://www.maawg.org/published-documents

17. Base de données nationale sur les vulnérabilités - National Institute of Standards and

Technology http://nvd.nist.gov/

18. Internet Storm Center

http://isc.sans.edu/index.html

19. Fondation Shadowserver

http://shadowserver.org

20. Liste de blocage de la

politique de Spamhaus

http://www.spamhaus.org/pbl/

21. Liste de blocage

composite

http://cbl.abuseat.org

22. OnGuard Online

http://www.onguardonline.gov/default.aspx

23. IETF BCP38 Filtrage de l'entrée du réseau

http://tools.ietf.org/html/bcp38