Internet Engineering Task Force (IETF)
Request for Comments : 6561
Catégorie : Information
ISSN: 2070-1721
Traduction Claude Brière de L'Isle

J. Livingood
N. Mody
M. O'Reirdan
Comcast

mars 2012

Recommandations pour remédier aux zombis dans les réseaux de FAI

Résumé
Le présent document contient des recommandations sur la façon dont les fournisseurs d'accès Internet peuvent utiliser divers remèdes techniques pour gérer les effets de la contamination de zombis malveillants sur les ordinateurs utilisés par leurs abonnés. Les utilisateurs de l'Internet dont les ordinateurs sont infectés sont exposés à des risques tels que la perte de leurs données personnelles et une susceptibilité accrue à des fraudes en ligne. De tels ordinateurs peuvent aussi devenir les participants involontaires ou les composants d'un réseau criminel en ligne, d'un réseau de pourriels, et/ou d'un réseau de fraude aussi bien qu'être utilisés dans une attaque répartie de déni de service. Atténuer les effets et remédier à l'installations de zombis malveillants rendra plus difficile le fonctionnement du réseaux de zombies et pourrait réduire le niveau du crime en ligne sur l'Internet en général et/ou sur le réseau d'un fournisseur d'accès Internet particulier.

Statut de ce mémoire
Le présent document n'est pas une spécification de l'Internet en cours de normalisation ; il est publié dans un but d'information.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir la Section 2 de la RFC5741.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc6561

Table des Matières

1. Introduction

Le présent document contient des recommandations sur la façon dont les fournisseurs d'accès Internet peuvent utiliser diverses techniques pour gérer les effets d'infections de robots malveillants sur les ordinateurs utilisés par leurs abonnés. Les usagers Internet qui ont des ordinateurs infectés sont exposés aux risques tels que la perte de leurs données personnelles et une susceptibilité accrue à subir des fraudes en ligne. De tels ordinateurs peuvent aussi devenir les participants involontaires ou les composants d'un réseau criminel en ligne, d'un réseau de pourriels, et ou d'un réseau d'usurpation d'identité, ou être utilisés au titre d'une attaque répartie de déni de service. Atténuer les effets et remédier à l'installation de robots malveillants rendra plus difficile le fonctionnement des réseaux de robots et pourrait réduire le niveau de crime en ligne sur l'Internet en général et/ou sur le réseau particulier d'un fournisseur de services Internet.

1.1 Terminologie

La présente section définit les termes clés utilisés dans le présent document.

1.1.1 Automates malveillants

Un automate malveillant ou potentiellement malveillant (dérivé du mot "robot", que les anglophones abrègent simplement en "bot") se réfère à un programme qui est installé sur un système afin de permettre que ce système effectue automatiquement (ou semi-automatiquement) une tâche ou ensemble de tâches normalement sur la commande et le contrôle d'un administrateur distant, notre "maître du robot". Les robots sont aussi appelés "zombies". De tels zombis peuvent avoir été installés subrepticement, sans que l'utilisateur comprenne bien ce que l'automate va faire une fois installé, comme partie ignorée d'une autre installation de logiciel, sous de faux prétextes, et/ou de diverses autres façons possibles.

Il est important de noter qu'il y a de "bons" automates. On trouve souvent de tels bons automates qui interagissent avec une ressource de calcul dans des environnements comme celui des jeux et de la causette (IRC, *Internet Relay Chat*) [RFC1459], où une présence continuelle, interactive peut être une exigence pour participer aux jeux. Comme ces bons robots accomplissent des fonctions utiles, légales, et non perturbatrices, il n'y a pas de raison pour qu'un fournisseur de services surveille leur présence et/ou alerte les usagers de leur présence.

Bien qu'il puisse y avoir de bons robots sans danger, pour les besoins du présent document, toutes les mentions de robots devront supposer que les automates impliqués sont malveillants ou potentiellement malveillants par nature. De tels automates malveillants devront généralement être supposés avoir été déployés sans la permission ou la compréhension consciente de l'usager particulier de l'Internet. Donc, à l'insu de l'usager, les robots peuvent transformer l'ordinateur de l'usager en une plateforme à partir de laquelle des activités malveillantes peuvent être conduites. De plus, explicitement inclus dans cette catégorie sont les robots potentiellement malveillants, qui peuvent initialement apparaître comme neutres mais peuvent simplement être en attente d'instructions distantes pour se transformer et/ou autrement commencer à s'engager dans un comportement malveillant. En général, l'installation d'un automate malveillant à l'insu de l'usager et sans son consentement est considéré dans la plupart des régions du monde comme illégale, et les activités de robots malveillants impliquent généralement des activités illégales ou autrement malveillantes.

1.1.2 Réseaux de zombies, ou botnets

Un réseau de zombies *(bot network, ou "botnet")* est défini comme un réseau concerté d'automates capables d'agir sur des instructions générées à distance. Les activités malveillantes sont soit concentrées sur les informations de la machine locale, soit agissent pour fournir des services aux machines distantes. Les robots sont très personnalisables de sorte qu'ils peuvent être programmés pour faire de nombreuses choses. Les activités malveillantes majeures incluent, mais sans s'y limiter, le vol d'identité, l'envoi de pourriels, des spim (pourriels sur la messagerie instantanée (IM)), des spit (pourriels sur la téléphonie Internet), la collecte d'adresses de messagerie, des attaques de déni de service réparties (DDoS), des enregistrements de clés, des clonages frauduleux de serveur DNS (redirection), l'hébergement de services de mandataires, l'hébergement de flux rapide (voir au paragraphe 1.1.5) l'hébergement de contenus illégaux, l'utilisation dans des attaques par interposition, et des clics frauduleux.

Les vecteurs d'infection (chemins d'infection) incluent les systèmes d'exploitation non réparés, les faiblesses logicielles (qui incluent ce qu'on appelle les vulnérabilités du jour zéro pour lesquelles il n'existe toujours pas de remède) les mots de passe faibles/non existants, les sites de la Toile malveillants, les navigateurs non corrigés, les logiciels malveillants, les applications d'aide vulnérables, les protocoles non sûrs par nature, les protocoles mis en œuvre sans que les dispositifs de sécurité soient activés, et les techniques d'ingénierie sociale pour obtenir l'accès à l'ordinateur de l'usager. La détection et la destruction des robots est un problème actuel et aussi une bataille constante entre la communauté de la sécurité de l'Internet et les ingénieurs de sécurité des réseaux d'un côté et les développeurs de robots de l'autre.

Au début, certains robots utilisaient IRC pour communiquer mais étaient facile à contrer si le serveur de commande et de contrôle était identifié et désactivé. De nouvelles commandes et méthodes de contrôle ont évolué, car celles actuellement employées par les maîtres de robots les rendent beaucoup plus résistants à la désactivation. Avec l'introduction d'architectures d'homologue à homologue (P2P, *peer-to-peer*) et des protocoles associés, l'utilisation de HTTP et autres protocoles résilients de communication, et la large adoption du chiffrement, les robots sont considérablement plus difficiles à identifier et isoler de l'usage normal du réseau. Par suite, une confiance accrue est mise dans la détection des anomalies et l'analyse du comportement, à la fois en local et à distance, pour identifier les robots.

1.1.3 Hôte

Utilisé dans le contexte du présent document, l'hôte ou ordinateur d'un utilisateur final est destiné à se référer à un appareil informatique qui se connecte à l'Internet. Cela englobe les appareils utilisés par les utilisateurs de l'Internet comme des ordinateurs personnels (incluant les appareils de bureau, les ordinateurs portables et les tablettes) les téléphones mobiles, les téléphones intelligents, les passerelles domestiques, et autres appareils informatiques d'utilisateur qui sont connectés ou peuvent être connectés à l'Internet public et/ou aux réseaux privés IP.

De plus en plus, d'autres systèmes et appareils domestiques contiennent des hôtes incorporés qui sont connectés ou peuvent être connectés à l'Internet public et/ou à des réseaux IP privés. Cependant, ces appareils peuvent n'être pas sous le contrôle interactif de l'usager Internet, comme ce peut être le cas avec divers appareils de domotique et de connectique.

1.1.4 Logiciels malveillants

Malgiciel *(malware)* est l'abrégé de "logiciel malveillant". Dans ce cas, les robots malveillants sont considérés comme un sous ensemble de malgiciels. D'autres formes de malgiciels pourraient inclure les virus et autres types similaires de logiciel. Les utilisateurs de l'Internet peuvent parfois causer l'infection de leurs hôtes par des malgiciels, qui peuvent inclure un robot ou causer l'installation du robot lui-même, via un accès imprudent à un site spécifique de la Toile, en téléchargeant un fichier, ou d'autres activités.

Dans d'autres cas, les hôtes connectés à l'Internet peuvent être infectés par un malgiciel à travers des activités malveillantes initiées de l'extérieur comme l'exploitation de vulnérabilités ou la recherche en force brute d'accréditifs d'accès.

1.1.5 Flux rapides

Un flux rapide du système des noms de domaine (DNS, *Domain Name System*) survient lorsque un domaine est entré dans le DNS en utilisant des enregistrements A pour plusieurs adresses IP, dont chacune est associée a une valeur de durée de vie (TTL, *Time-to-Live*) très courte. Cela signifie que le domaine se résout en diverses adresses IP sur une très courte période.

Le flux rapide DNS est normalement utilisé en conjonction avec des mandataires qui fonctionnent normalement sur des hôtes d'utilisateurs compromis. Ces mandataires acheminent les demandes de la Toile à l'hôte réel, qui dessert les données recherchées. L'effet de cela est de rendre la détection de l'hôte réel beaucoup plus difficile et d'assurer que l'extrémité arrière ou le site caché restent actifs aussi longtemps que possible.

2. Position du problème

Les hôtes des utilisateurs de l'Internet, qui dans ce cas sont les clients d'un fournisseur d'accès Internet (FAI), peuvent être infectés par un malgiciel qui peut contenir et/ou installer un ou plusieurs robots sur un hôte. Ils peuvent poser un problème majeur pour un FAI pour un certain nombre de raisons (sans mentionner, bien sûr, les problèmes créés pour les usagers). D'abord, ces robots peuvent être utilisés pour envoyer des pourriels, dans certains cas, de très gros volumes de pourriels [Spamalytics]. Ces pourriels peuvent résulter en des coûts supplémentaires pour les FAI en termes de gaspillage du réseau, de serveurs, et/ou de ressources en personnel, entre autres nombreux autres coûts potentiels et effets collatéraux. De tels pourriels peuvent aussi avoir un effet négatif sur la réputation du FAI, de ses clients, et la réputation de l'espace d'adresses IP utilisé par

le FAI (à quoi on se réfère souvent simplement comme la "réputation IP"). Une autre complication potentielle est que l'espace IP compromis par la mauvaise réputation peut continuer de subir cette mauvaise réputation même lorsque utilisé pour des objets parfaitement innocents à la suite de la réallocation de cet espace IP.

De plus, ces robots peuvent agir comme plateformes pour diriger, participer, ou autrement conduire des attaques sur des infrastructures critiques de l'Internet [Threat-Report]. Les robots sont fréquemment utilisés au titre d'attaques coordonnées de DDoS pour des motivations criminelles, politiques, ou autres [Gh0st], [Dragon], [DDoS]. Par exemple, des robots ont été utilisés pour attaquer des ressources et infrastructures de l'Internet allant des sites de la Toile aux serveurs de messagerie et du DNS, ainsi que les infrastructures critiques de l'Internet de pays entiers [Estonia], [Combat-Zone]. Les motifs de telles attaques coordonnées de DDoS peuvent aller de la tentative d'extorsion criminelle à la protestation en ligne et à la ferveur nationaliste [Whiz-Kid]. Les attaques de DDoS peuvent aussi être motivées par de simples vendettas personnelles ou par des gens qui cherchent simplement à s'amuser un peu aux dépens des autres.

Il y a de nombreux indices qui laissent penser que des robots sont utilisés dans le monde de l'entreprise à des fins d'espionnage industriel incluant l'exfiltration de données financières et de secrets d'affaires. Cela s'étend aussi à la possibilité que des robots soient utilisés pour des besoins d'État tels que l'espionnage.

Bien que tout ordinateur puisse être infecté par des robots, la majorité des infections de robot affectent les ordinateurs personnels utilisés par les usagers finaux de l'Internet. Par suite du rôle des FAI dans la fourniture de la connexité IP, parmi beaucoup d'autres services, aux utilisateurs de l'Internet, ces FAI sont dans une position unique pour avoir la capacité de tenter de détecter et observer les réseaux de zombis qui fonctionnent sur leurs réseaux. De plus, les FAI peuvent aussi être dans une position unique pour pouvoir notifier à leurs clients les infections actuelles, potentielles, ou probables par des robots ou autres.

Du point de vue de l'utilisateur final, recevoir un avertissement qu'il peut y avoir un ordinateur infecté sur son réseau est une information importante. Une fois qu'on le sait, on peut prendre des mesures pour retirer les robots, résoudre les problèmes qui peuvent découler de l'infection de robots, et se protéger contre de futures menaces. Il est important de notifier aux usagers qu'ils peuvent être infectés par un robot parce que les robots peuvent consommer de grandes quantités de ressources de calcul local et de réseau, permettre des vols d'informations personnelles (y compris des informations personnelles financières) permettre d'utiliser l'hôte pour des activités criminelles (qui peuvent résulter en l'incrimination de l'utilisateur de l'Internet) et détruire l'hôte ou le laisser dans un état irrécupérable via des technologies de robot "tueur".

Par suite, l'intention du présent document est de donner des lignes directrices aux FAI et autres organisations pour remédier aux hôtes infectés par des robots, afin de réduire la taille des réseaux de zombis et minimiser les dommages potentiels que les robots peuvent infliger à l'infrastructure de l'Internet en général ainsi qu'aux utilisateurs individuels de l'Internet. Les efforts des FAI et des autres organisations peuvent, à la longue, réduire le réservoir d'hôtes infectés par des robots sur l'Internet, ce qui à son tour pourrait résulter en plus petits réseaux de zombis avec moins de capacités de perturbation.

L'atténuation potentielle des maux causés par les robots est réalisée par un processus de détection, de notification aux utilisateurs de l'Internet, et l'application de remèdes aux infections de robots par divers outils, comme on le décrit dans la suite du présent document.

3. Notice importante de limitation et de portée

Les techniques décrites dans le présent document ne garantissent en aucune façon la guérison de tous les robots. La suppression de robot est potentiellement une tâche qui exige des connaissances spécialisées, de l'habileté et des outils ; cela peut être au delà des capacités de l'utilisateur moyen. Les tentatives de suppression de robot peuvent fréquemment être vouées à l'échec ou ne réussir que partiellement, laissant le système de l'usager dans un état instable et insatisfaisant ou même dans un état où l'infection subsiste. Les tentatives de suppression de robot peuvent avoir des effets collatéraux allant de la perte de données à la perte complète de l'usage du système.

En général, la seule façon dont un utilisateur peut être sûr qu'il a supprimé certains des malgiciels les plus sophistiqués d'aujourd'hui est de "remettre à zéro" le système : de reformater le pilote, de réinstaller le système d'exploitation et les applications (incluant toutes les corrections) à partir de zéro, et ensuite de restaurer les fichiers d'utilisateur à partir d'une sauvegarde sûre connue. Cependant, l'introduction d'un malgiciel persistant enraciné dans la mémoire peut signifier que, dans certains cas, cela peut n'être pas suffisant et se révéler être plus que ce qu'on peut raisonnablement attendre qu'un utilisateur final puisse résoudre [BIOS]. Les usagers expérimentés auront à reflasher ou reimager les sections de la mémoire persistante ou les composants de leurs hôtes afin de supprimer le malgiciel tapi dans la mémoire persistante. Cependant, dans certains cas, même la remise à zéro du système ne va pas résoudre le problème, ce qui plaide en faveur du remplacement du disque dur et/ou le remplacement complet de l'hôte.

Les appareils qui ont des systèmes d'exploitation incorporé, comme les consoles de jeux vidéo et les applications de

domotique, vont vraisemblablement être au delà des capacités de réparation d'un utilisateur seul et pourraient donc exiger l'aide d'un conseil, de mises à jour et d'outils spécifiques du fabricant. Cependant, dans certains cas, de tels appareils vont avoir une fonction ou un bouton pour permettre à l'utilisateur de réinitialiser à une configuration d'usine par défaut, qui peut parfois permettre à l'usager de remédier à l'infection. On devrait faire attention quand on communique aux utilisateurs de l'Internet des conseils sur des remèdes à cause de la croissante diversité des appareils informatiques qui peuvent, ou pourraient être infectés par robots à l'avenir.

Le présent document n'est pas destiné à régler les problèmes relatifs à la prévention des robots sur un appareil d'utilisateur final. Ceci sort du domaine d'application du présent document.

4. Détection des robots

Un FAI doit d'abord identifier qu'un usager de l'Internet est infecté ou a probablement été infecté par un robot (un usager est supposé être le client d'un FAI ou être par ailleurs connecté au réseau du FAI). Le FAI devrait tenter de détecter la présence de robots en utilisant des méthodes, processus, et outils qui préservent la confidentialité des informations personnelles identifiables (PII, *personally identifiable information*) de leurs clients. Le FAI ne devrait pas bloquer le trafic légitime pendant la détection de robot et devrait plutôt employer des méthodes de détection, outils, et processus qui cherchent à ne pas interrompre et soient transparents pour les utilisateurs de l'Internet et les applications des utilisateurs finaux.

Les méthodes de détection, outils, et processus peuvent inclure l'analyse de flux de trafic spécifique de réseaux et/ou d'applications (comme le trafic pour un serveur de messagerie électronique), l'analyses de données de trafic agrégé du réseau et/ou d'application, des flux de données reçus d'autres FAI et organisations (comme des listes des adresses IP du FAI qui ont été rapportées comme ayant envoyé des pourriels) des retours des clients du FAI ou d'autres utilisateurs de l'Internet, ainsi qu'une grande variété d'autres possibilités. En pratique, il s'est révélé efficace de confirmer une infection de robot par l'utilisation d'une combinaison de multiples points de détection de données de robot. Cela aide à corroborer des informations de bien fondé de consistance diverses, ainsi que d'éviter ou minimiser la possibilité de fausse identification positive des hôtes. La détection devrait aussi, lorsque possible et faisable, tenter de classer le type spécifique d'infection de robot afin de confirmer qu'il est malveillant par nature, estimer la variété et la sévérité des menaces qu'elle fait peser (comme un robot d'envoi de pourriels, un robot de collecte de clés, un robot de distribution de fichiers, etc.) et déterminer les méthodes potentielles pour un remède éventuel. Cependant, étant donnée la nature dynamique de la gestion de réseau de zombis et les incitations criminelles à rechercher des récompenses financières rapides, les réseaux de zombis mettent fréquemment à jour ou changent le cœur de leurs capacités. Par conséquent, les réseaux de zombis qui sont initialement détectés et classés par le FAI comme constitutifs d'un type particulier de robot doivent être continuellement surveillés et retracés afin d'identifier correctement la menace que fait peser le réseau de zombis à un instant particulier.

La détection est aussi sensible au temps. Si une analyse complexe est requise et que de multiples confirmations sont nécessaires pour vérifier qu'un robot est bien présent, il est alors possible que le robot puisse causer des dommages (soit à l'hôte infecté, soit à un système ciblé à distance) avant qu'il puisse être stoppé. Cela signifie qu'un FAI doit mettre en balance le désir ou le besoin de classer définitivement et/ou de confirmer la présence d'un robot, ce qui peut prendre un certain temps, avec la capacité de prédire la probabilité d'un robot dans un très court délai. Une telle détermination doit avoir un taux de faux positifs relativement faible afin de conserver la confiance des usagers. Ce défi "définitif contre probable" est difficile et, quand on est dans le doute, les FAI devraient pencher plutôt du côté de la prudence en communiquant qu'une infection de robots a lieu. Cela signifie aussi que les utilisateurs de l'Internet peuvent bénéficier de l'installation de logiciels de sécurité fondés sur le client sur leur hôte. Cela peut activer une détection d'activité de robot fondée sur une heuristique rapide, comme la détection d'un robot lorsque il commence à communiquer avec d'autres réseaux de zombis et exécuter des commandes. Tout système de détection de robot devrait aussi être capable de s'adapter, soit via une intervention manuelle, soit automatiquement, afin de faire face à une menace en évolution rapide.

Comme noté ci-dessus, les méthodes de détection, outils, et processus devraient assurer la conservation de la confidentialité des informations personnelles identifiables (PII) du client. Cette protection accordée aux PII devrait aussi s'étendre aux tiers qui traitent les données au nom des FAI. Bien que les méthodes, outils et processus de détection de robot soient similaires aux défenses contre les pourriels et les virus déployées par le FAI pour le bénéfice de ses clients (et peuvent être directement en rapport avec ces défenses) les tentatives de détection de robots devraient prendre en compte le besoin qu'a un FAI de s'assurer que toutes les PII collectées ou détectées incidemment sont proprement protégées. Ceci est important parce que tout comme les défenses contre les pourriels peuvent impliquer d'examiner le contenu des messages électroniques, qui peuvent contenir des PII, les défenses contre les robots peuvent elles aussi venir en contact accidentel avec des PII. La définition des PII varie d'une juridiction à l'autre de sorte qu'un soin particulier devrait être pris de s'assurer que toutes les actions entreprises sont conformes avec la législation et les bonnes pratiques de la juridiction dans laquelle les PII sont rassemblées. Finalement, selon la région dans laquelle fonctionne le FAI, certaines méthodes relatives à la détection de robot peuvent devoir être incluses dans les documents de clauses de service pertinents ou les autres documents à la disposition du consommateur d'un FAI particulier.

Il y a plusieurs méthodes, outils, et processus de détection de robot que peut choisir d'utiliser un FAI, comme noté dans la liste qui suit. Il est important de noter que les solutions techniques disponibles sont relativement immatures et vont probablement changer au fil du temps, évoluant rapidement dans les années à venir. Bien que ces éléments soient décrits en relation avec les FAI, ils peuvent aussi être applicables aux organisations qui gèrent d'autres réseaux, comme des réseaux de campus et d'entreprise.

a. Lorsque ce n'est pas interdit par la loi et que c'est une pratique acceptée de l'industrie dans une région particulière, un FAI peut d'une certaine manière "examiner" son espace IP afin de détecter les hôtes non réparés ou par ailleurs vulnérables, ou détecter les signes d'infection. Cela peut fournir au FAI l'opportunité d'identifier facilement les utilisateurs de l'Internet qui apparaissent comme déjà infectés ou qui courent un grand risque d'être infectés par un robot. Les FAI devraient noter que certains types d'examen d'accès peuvent laisser les services réseau en état de connexion ou les rendre inutilisables du fait de fragilités courantes et que de nombreux pare-feu modernes et mises en œuvre de détection d'intrusion fondées sur l'hôte peuvent alerter l'utilisateur de l'Internet de l'examen. Par suite, l'examen peut être interprété comme une attaque malveillante contre l'hôte. L'examen des vulnérabilités a une forte probabilité de laisser accessibles les services et applications du réseau dans un état endommagé et va souvent résulter en une plus forte probabilité de détection par l'utilisateur de l'Internet et interprété ensuite comme une attaque ciblée. Selon la vulnérabilité pour laquelle un FAI peut faire son examen, certaines méthodes automatisées de vérification des vulnérabilités peuvent résulter en l'altération des données ou qu'elles soient créées à nouveau sur l'hôte de l'utilisateur de l'Internet, ce qui peut être un problème dans de nombreux environnements juridiques. On devrait aussi noter que du fait de la prévalence des appareils de traduction d'adresse réseau, des appareils de traduction d'adresse d'accès, et/ou de pare-feu dans les réseaux d'utilisateurs, l'examen des faiblesses fondé sur le réseau peut être d'une valeur limitée. Donc, bien qu'on note que c'est une technique qui peut être utilisée, il est peu probable qu'elle soit particulièrement efficace et elle a des effets secondaires problématiques, qui conduisent les auteurs à se prononcer contre l'utilisation de cette méthode particulière.

b. Un FAI peut aussi communiquer et partager des données choisies, via des boucles de retour ou d'autres mécanismes, avec diverses tierces parties. Les boucles de retour sont des alimentations de rapports en temps réel (ou presque en temps réel) de formatage cohérent, des actes de piratage offerts par les officines de traitement des données menaçantes, des organisations d'alerte sur la sécurité, des autres FAI, et d'autres organisations. Les formats des boucles de retour incluent ceux définis aussi bien dans le format de rapport d'abus (ARF, *Abuse Reporting Format*) [RFC5965] et le format d'échange de description d'objet d'incident (IODEF, *Incident Object Description Exchange Format*) [RFC5070]. Les données peuvent inclure, sans s'y limiter, des adresses IP d'hôtes qui paraissent être infectées ou probablement infectées, des adresses IP, des noms de domaines ou des noms de domaine pleinement qualifiés (FQDN) connus pour héberger un malgiciel et/ou être impliqués dans la commande et le contrôle de réseaux de zombis, des techniques récemment essayées ou découvertes pour détecter, ou remédier à, des infections de robots, de nouveaux vecteurs de menace, et autres informations pertinentes. Quelques bons exemples de partage de données sont notés à l'Appendice A.

c. Un FAI peut utiliser Netflow [RFC3954] ou d'autres moyens similaires de surveillance passive de réseau pour identifier les anomalies de réseau qui peuvent indiquer une attaque de réseau de zombis ou des communications de robots. Par exemple, un FAI peut être capable d'identifier des hôtes compromis en identifiant du trafic destiné aux adresses IP associées à la commande et au contrôle de réseaux de zombis ou destiné à la combinaison d'une adresse IP et d'un accès de contrôle associé à un réseau de commande et contrôle (parfois le trafic de commande et de contrôle vient d'un hôte qui a un trafic légitime). De plus, les robots peuvent être identifiés lorsque un hôte distant est soumis à une attaque de DDoS, parce que les hôtes qui participent à l'attaque sont probablement infectés par un robot. Cela peut souvent être observé aux bordures du réseau bien que les FAI devraient être avertis des techniques d'usurpation d'adresse IP de source qui peuvent être employées pour éviter ou déjouer la détection.

d. Un FAI peut utiliser des techniques fondées sur le DNS pour effectuer la détection. Par exemple, un certain robot répertorié peut être connu pour interroger une liste spécifique de noms de domaines à des moments ou dates spécifiques (dans l'exemple du robot appelé "Conficker" (voir [Conficker]) souvent en faisant correspondre des interrogations du DNS à des listes bien connues de domaines associés à des malgiciels. Dans de nombreux cas, de telles listes sont distribuées ou partagées en utilisant des tiers, comme les officines de nettoyage des données menaçantes.

e. Parce que les hôtes infectés par des robots sont fréquemment utilisés pour envoyer des pourriels ou participer à des attaques de DDoS, le FAI qui dessert ces hôtes va normalement recevoir des plaintes sur le trafic réseau malveillant. Ces plaintes peuvent être envoyées aux comptes spécifiés dans la [RFC2142], comme à abuse@, ou à d'autres adresses pertinentes pour les abus ou la sécurité spécifiées par le site au titre de ses données de contact WHOIS (ou autres).

f. Les FAI peuvent aussi découvrir des hôtes probablement infectés par des robots situés dans d'autres réseaux. Donc, lorsque la loi le permet dans une certaine région, il peut valoir la peine que les FAI partagent les informations relatives aux hôtes compromis avec l'opérateur de réseau distant pertinent, les chercheurs en sécurité et les gestionnaires de listes de blocs.

g. Les FAI peuvent faire fonctionner ou s'abonner à des services qui fournissent des capacités de "sinkholing" *(le trou dans*

l'évier) ou de "honeynet" *(réseau appât)*. Cela peut permettre au FAI d'obtenir des listes presque en temps réel d'hôtes infectés par des robots lorsque ils tentent de se joindre à un plus grand réseau de zombis ou de se propager à d'autres hôtes sur un réseau.

h. Les associations professionnelles de FAI devraient examiner la possibilité de colliger des statistiques provenant des FAI membres afin d'avoir de bonnes statistiques sur les infections par des robots sur la base des données réelles des FAI.

i. Un système de détection d'intrusion (IDS, *Intrusion Detection System*) peut être un outil utile pour aider réellement à identifier le malgiciel. Un IDS tel que Snort (plate-forme IDS à source ouverte ; voir [Snort]) peut être placé dans un système clos et utilisé pour analyser le trafic d'un utilisateur final pour confirmer le type de malgiciel. Cela va aider à trouver un remède pour l'appareil infecté.

5. Notification aux utilisateurs de l'Internet

Une fois qu'un FAI a détecté un robot, ou la forte probabilité d'un robot, des mesures devraient être prises pour informer l'utilisateur de l'Internet qu'il peut avoir un problème de robot. Un FAI devrait décider de la ou des méthodes les plus appropriées pour fournir la notification à un ou plusieurs de ses clients ou utilisateurs de l'Internet, selon une gamme de facteurs qui incluent les capacités techniques du FAI, les attributs techniques de son réseau, les considérations financières, les ressources de serveur disponibles, les ressources organisationnelles disponibles, le nombre probable d'hôtes infectés détecté à un moment donné, et la sévérité de toutes les menaces possibles. De telles méthodes de notification peuvent inclure une ou plusieurs des méthodes décrites dans les paragraphes qui suivent, ainsi que d'autres méthodes possibles non décrites ici.

Il est important de noter qu'aucune de ces méthodes ne garantit de réussir à cent pour cent et que chacune a son propre ensemble de limitations. De plus, dans certains cas, un FAI peut déterminer qu'une combinaison de deux méthodes ou plus est plus appropriée et efficace et réduit les chances qu'un malgiciel puisse bloquer une notification. À ce titre, les auteurs recommandent l'utilisation de plusieurs méthodes de notification. Finalement, la notification est aussi considérée comme sensible au délai ; si l'usager ne reçoit pas ou ne voit pas la notification à temps, un certain robot pourrait lancer une attaque, exploiter l'usage, ou causer d'autres dommages. Si possible, un FAI devrait établir un moyen préféré de communication lorsque l'abonné souscrit au service. Au titre du processus de notification, les FAI devraient garder un enregistrement de l'allocation des adresses IP aux abonnés pendant un délai assez long pour permettre que toutes technologies de détection de robot couramment utilisées soient capables de relier précisément une adresse IP infectée à un abonné. Cet enregistrement devrait être conservé pendant la période nécessaire pour prendre en charge la détection de robot, mais pas plus, afin de protéger la vie privée de l'abonné individuel.

Un facteur important à se rappeler est que la notification aux utilisateurs finaux doit être résistante aux usurpations potentielles. Ceci devrait être fait pour protéger, aussi raisonnablement que possible, contre la possibilité que des notifications légitimes soient usurpées et/ou utilisées par des tiers qui ont l'intention d'effectuer des attaques malveillantes supplémentaires contre les victimes de malgiciels ou même de délivrer un malgiciel supplémentaire.

Il devrait être possible à l'utilisateur final d'indiquer le moyen préféré de notification sur la base d'un choix d'options pour la méthode de notification. Il est recommandé que l'utilisateur final n'ait pas entièrement le choix des méthodes de notification.

Lorsque l'usager a la notification, un FAI devrait s'engager à lui donner autant d'informations que possible concernant la méthode de détection de robot employée chez le FAI, tout en ne fournissant pas ces informations à ceux qui créent ou déploient les robots ce qui pourrait leur permettre d'éviter la détection.

5.1 Notification par message électronique

C'est une forme courante de notification par les FAI. Un inconvénient de l'utilisation de la messagerie électronique est qu'il n'est pas garantit que le message soit vu dans un délai raisonnable, s'il l'est. L'usager peut utiliser une adresse de messagerie principale différente de celle fournie au FAI. De plus, certains FAI ne fournissent pas du tout de compte de messagerie au titre d'un bouquet de services Internet et/ou n'ont pas besoin de méthode pour demander ou conserver les adresses principales de messagerie électronique des utilisateurs de l'Internet de leurs réseaux. Une autre possibilité est que l'usager, son client de messagerie, et/ou son serveur de messagerie puisse déterminer ou classer une telle notification comme pourriel, ce qui pourrait supprimer le message ou autrement le classer dans un fichier de messagerie que l'usager ne va pas vérifier de façon régulière ou à temps. Les maîtres de zombis sont aussi connus pour se faire passer pour le FAI ou des envoyeurs de confiance et envoyer des messages frauduleux aux usagers. Cette technique d'ingénierie sociale conduit souvent à de nouvelles infestations de robots. Finalement, si les accréditifs de messagerie de l'usager sont compromis, un pirate et/ou un robot pourront simplement accéder au compte de messagerie de l'usager et supprimer le message avant qu'il soit lu par l'usager.

5.2 Notification par appel téléphonique

Un appel téléphonique peut être un moyen efficace de communication dans des situations de risque particulièrement élevé. Cependant, les appels téléphoniques ne sont pas toujours faisables à cause du coût que représente la réalisation d'un grand nombre d'appels, mesuré en temps, en argent, en ressources organisationnelles, en ressources de serveur, ou autres moyens. De plus, il n'est pas garanti que l'usager va répondre au téléphone. Dans la mesure où le numéro de téléphone appelé par le FAI peut être pris par l'ordinateur infecté, le robot sur cet hôte peut être capable de déconnecter, renvoyer, ou autrement interférer avec un appel entrant. Les usagers peuvent aussi interpréter une telle notification téléphonique comme un appel de télémarketing et donc ne pas lui faire bon accueil ou ne pas accepter du tout l'appel. Finalement, même si un représentant du FAI est capable de se connecter et de parler à un usager, celui-ci va probablement manquer de l'expertise technique nécessaire pour comprendre la menace ou être capable de la traiter effectivement.

5.3 Notification par message postal

Cette forme de notification est probablement le moyen le moins populaire et efficace de communication, dû au temps de préparation, au délai de livraison, ou coût d'impression et de papier, et du coût d'affranchissement.

5.4 Notification d'un jardin clos

Placer un usager dans un jardin clos est une autre approche que les FAI peuvent utiliser pour notifier leurs abonnés. Un "jardin clos" se réfère à un environnement qui contrôle les informations et services qu'il est permis à un abonné d'utiliser et les permissions d'accès réseau qui lui sont accordées. La mise en œuvre d'un jardin clos peut aller de strict à lâche. Dans un environnement de jardin clos strict, l'accès à la plupart des ressources Internet est normalement limité par le FAI. À l'opposé, un environnement de jardin clos lâche permet l'accès à toutes les ressources Internet, sauf celles réputées malveillantes, et assure l'accès à celles qui peuvent être utilisées pour notifier les infections aux utilisateurs.

Les jardins clos sont efficaces parce que il est possible de notifier à l'usager et simultanément bloquer toutes les communications entre le robot et le canal de commande et contrôle. Bien que dans de nombreux cas, il soit presque garanti à l'usager de voir le message de notification et de prendre toutes les actions de remède appropriées, cette approche peut poser d'autres problèmes. Par exemple, ce n'est pas dans tous les cas qu'un utilisateur se sert activement d'un hôte qui met en œuvre un navigateur de la Toile, qu'il a un navigateur qui fonctionne activement dessus, ou qu'il fait fonctionner une autre application qui utilise les accès qui sont redirigés sur le jardin clos. Dans un exemple, un usager pourrait être en train de jouer en ligne, via l'utilisation d'une console de jeux dédiée, connectée à l'Internet. Dans un autre exemple, l'usager peut n'être pas en train d'utiliser un hôte avec un navigateur de la Toile lorsque il est placé dans le jardin clos et peut être plutôt engagé dans une conversation téléphonique ou peut attendre de recevoir un appel utilisant un appareil de voix sur IP (VoIP) d'un certain type. Par suite, le FAI peut ressentir le besoin de tenir une liste potentiellement longue de domaines qui ne sont pas normalement sujets aux restrictions d'un jardin clos, ce qui pourrait bien se révéler une tâche onéreuse d'un point de vue opérationnel.

Pour ces raisons, la mise en œuvre d'un jardin clos lâche a plus de sens, mais il a un ensemble d'inconvénients différent. Le FAI doit supposer que l'usager va finalement utiliser un navigateur de la Toile pour accuser réception de la notification ; autrement, l'usager va rester dans le jardin clos et ne pas le savoir. Si l'intention du jardin clos lâche est seulement de notifier à l'usager l'infection de robot, ce n'est pas idéal parce que la notification est sensible au délai, et l'usager peut ne pas recevoir la notification avant qu'il invoque une demande pour un service et/ou ressource ciblés. Cela signifie que le robot peut éventuellement commettre plus de dommages. De plus, le FAI doit identifier quels services et/ou ressources interdire pour les besoins de la notification. Cela n'a pas à être spécifique d'une ressource et peut être temporaire et/ou fondé sur une politique. Un exemple de la façon de faire la notification sur la base du délai pourrait impliquer une notification pour toutes les demandes HTTP toutes les 10 minutes, ou montrer la notification toutes les cinq demandes HTTP.

Le FAI a plusieurs options pour déterminer quand laisser sortir l'usager du jardin clos. Une approche peut être de laisser l'usager déterminer quand il sort. Cette option est suggérée quand l'objectif principal du jardin clos est seulement de notifier les usagers et de fournir des informations sur les remèdes, en particulier lorsque la notification n'est pas une garantie de réussite du remède. Ce pourrait aussi être le cas que, pour une raison quelconque, l'usager estime qu'il ne peut pas prendre le temps de remédier au problème de l'hôte et que d'autres activités en ligne qu'il voudrait reprendre sont plus importantes. La sortie du jardin clos peut aussi impliquer un processus de vérification que c'est bien l'utilisateur qui demande la sortie du jardin clos et non le robot.

Une fois que l'usager a accusé réception de la notification, il peut décider de remédier au problème et sortir du jardin clos ou de sortir du jardin clos sans remédier au problème. Une autre approche peut être d'appliquer une politique plus stricte et d'exiger que l'usager nettoie l'hôte avant qu'on lui permette de sortir du jardin clos, bien que ceci ne soit pas toujours techniquement faisable en fonction du type de robot, des techniques de camouflage employées par le robot, et/ou d'une gamme d'autres facteurs. Donc, le FAI peut aussi avoir besoin de prendre en charge des outils pour examiner l'hôte infecté (dans le style d'un examen de virus, plutôt que de l'examen d'un accès) et déterminer si il est encore infecté ou s'il peut s'appuyer sur le jugement de l'usager que le robot a été désactivé ou supprimé. Un défi de cette approche est que l'usager peut avoir

plusieurs hôtes qui partagent une seule adresse IP, comme via un appareil de passerelle domestique commune qui effectue la traduction d'adresse réseau (NAT, *Network Address Translation*). Dans un tel cas, le FAI peut avoir besoin de déterminer à partir d'un retour de l'usager, ou d'autres moyens, que tous les hôtes affectés ont été nettoyés, ce qui peut être ou non techniquement faisable.

Finalement, lorsque on utilise un jardin clos, une liste d'adresses bien connues devrait être créée aussi bien pour les fabricants de système d'exploitation que les marchands de sécurité, et inscrite dans une liste blanche qui permette d'accéder à ces sites. Ceci peut être important pour permettre l'accès à partir du jardin clos pour les utilisateurs finaux à la recherche de réparations de système d'exploitation et d'application. Il est recommandé que les jardins clos soient considérés avec sérieux car une méthode de notification comme celle qu'ils offrent est facile à mettre en œuvre et s'est révélée un moyen efficace pour attirer l'attention de l'utilisateur final.

5.5 Notification par message instantané

Le message instantané (IM) donne au FAI un moyen simple de communiquer avec l'utilisateur. Il y a plusieurs avantages à utiliser l'IM qui le rendent une option attractive. Si le FAI fournit des services d'IM et si l'usager y souscrit, il peut alors être facilement notifié. La notification fondée sur l'IM peut être un moyen qui vaut la peine pour communiquer automatiquement avec les utilisateurs à partir d'un système d'alerte par IM ou par un processus manuel, impliquant le personnel de soutien du FAI. Idéalement, le FAI devrait permettre à l'usager d'enregistrer son identité d'IM dans un système de gestion des comptes du FAI et d'accorder la permission d'être contacté via ce moyen. Si le fournisseur de service d'IM prend en charge la messagerie hors ligne, l'usager peut alors être notifié sans considération de sa connexion actuelle dans le système d'IM.

Il y a plusieurs inconvénients à cette méthode de communications. Il est très probable qu'un abonné puisse interpréter la communication comme un pourriel et donc l'ignorer. Aussi, ce ne sont pas tous les usagers qui utilisent l'IM et/ou l'usager peut ne pas fournir son identité d'IM au FAI et il faut donc utiliser quelque autre moyen de remplacement. Même dans les cas où un usager a bien une adresse d'IM, il peut n'être pas enregistré dans le système d'IM lorsque la notification est tentée. Cela peut être un problème de confidentialité de la part des usagers lorsque une telle notification par IM doit être transmise sur un réseau tiers et/ou le service d'IM. À ce titre, si cette méthode devait être utilisée, la notification devrait être discrète et ne pas inclure de PII dans la notification elle-même.

5.6 Notification par service de message court (SMS)

Le SMS permet au FAI d'envoyer une brève description du problème à notifier à l'usager, normalement à un appareil mobile comme un téléphone. Idéalement, le FAI devrait permettre à l'usager d'enregistrer son numéro de mobile et/ou son adresse de SMS dans le système de gestion des comptes du FAI et accorder la permission d'être contacté par ce moyen. Le principal avantage du SMS est que les usagers sont familiarisés à la réception de messages de texte et vont vraisemblablement les lire. Cependant, les usagers peuvent ne pas agir immédiatement sur la notification si ils ne sont pas devant leur hôte au moment de la notification par SMS.

Un désavantage est que les FAI peuvent devoir continuer avec un autre moyen de notification si toutes les informations nécessaires ne peuvent pas être convoyées en un message, étant données les contraintes sur le nombre de caractères dans un message individuel (normalement 140 caractères). Un autre inconvénient du SMS est le coût associé. Le FAI doit soit construire sa propre passerelle SMS pour faire l'interface avec les divers fournisseurs de service de réseau sans fil, soit utiliser un relais de SMS tiers pour notifier les utilisateurs. Dans les deux cas, un FAI peut subir des redevances relatives aux notifications par SMS, selon la méthode utilisée pour envoyer les notifications. Un inconvénient supplémentaire est que les messages SMS envoyés à un usager peuvent résulter en une charge pour l'usager par son fournisseur mobile, selon le plan auquel il a souscrit et le pays dans lequel il réside. Un autre désavantage mineur est qu'il est possible de notifier le mauvais usager si celui prévu a changé de numéro de mobile en oubliant de le mettre à jour chez le FAI.

Cette méthode de communications présente plusieurs autres inconvénients. Il y a une forte probabilité que l'abonné puisse interpréter la communication comme un pourriel et donc l'ignorer. Aussi, ce ne sont pas tous les usagers qui utilisent des SMS, et/ou l'usager peut ne pas fournir son adresse de SMS ou son numéro de mobile au FAI. Même dans les cas où un usager a une adresse de SMS et un numéro de mobile, son appareil n'est pas forcément branché ou par ailleurs disponible sur un réseau mobile lorsque la notification est tentée. Il peut aussi y avoir un souci de confidentialité de la part des usagers lorsque une telle notification par SMS doit être transmise sur un réseau tiers et/ou un relais de SMS. À ce titre si cette méthode devait être utilisée, la notification devrait être discrète et ne pas inclure de PII dans la notification elle-même.

5.7 Notification par le navigateur de la Toile

La notification presque en temps réel au navigateur de l'usager est une autre technique qui peut être utilisée [RFC6108], bien que la façon dont un tel système peut fonctionner sorte du domaine d'application du présent document. Une telle notification pourrait avoir un avantage comparée à une notification dans un jardin clos, en ce qu'elle ne restreint pas, par définition, le

trafic à une liste spécifiée de destinations de la même façon que le ferait un jardin clos. Cependant, comme avec la notification dans le jardin clos, il n'est pas garanti que l'usager va se servir de son navigateur à un moment donné, bien qu'un tel système puisse certainement fournir une notification quand ce navigateur va finir par être utilisé. Comparé au jardin clos, une notification par le navigateur de la Toile est probablement préférée du point de vue des utilisateurs de l'Internet, car il n'y a pas de risque de perturber des sessions qui ne sont pas avec la Toile, comme des jeux en ligne, des appels VoIP, etc. (comme noté au paragraphe 5.4).

Il y a d'autres méthodes de notification par le navigateur qui sont offertes commercialement par un certain nombre de fabricants. Beaucoup des techniques utilisées sont brevetées, et il n'est pas dans le domaine d'application du présent document de décrire comment elles sont mises en œuvre. Ces techniques ont été mises en œuvre avec succès par plusieurs FAI.

On devrait noter que la notification par le navigateur est seulement destinée à notifier les appareils qui fonctionnent avec un navigateur.

5.8 Considérations sur les notifications aux localisations de réseau public

La livraison d'une notification à une localisation qui fournit un réseau public partagé, comme une station de chemin de fer, un jardin public, une cafétéria, ou une localisation similaire peut être de peu de valeur dans la mesure où les usagers qui se connectent à de tels réseaux sont normalement très transitoires et généralement pas connus des administrateurs de site ou de réseau. Par exemple, un système peut détecter qu'un hôte sur un tel réseau a un robot, mais le temps qu'une notification soit générée, cet usager sera parti du réseau et se sera déplacé ailleurs.

5.9 Considérations sur les notifications aux localisations de réseau avec une adresse IP partagée

La livraison d'une notification à une localisation qui accède à l'Internet acheminée par une ou plusieurs adresses IP publiques partagées peut être de faible valeur car il peut être assez difficile de différencier les usagers lorsque on fournit une notification. Par exemple, sur un réseau d'affaires de 500 usagers, partageant tous une adresse IP publique, il serait sous optimal de fournir une notification à tous les 500 usagers si on a seulement besoin qu'un usager spécifique soit notifié et fasse quelque chose. Il en résulte que de tels réseaux peuvent avoir intérêt à établir une détection de robot et un système de notification localisés, juste comme ils vont probablement établir aussi d'autres systèmes localisés pour la sécurité, le partage de fichiers, la messagerie et ainsi de suite.

Cependant, si un FAI devait mettre en œuvre une forme de notification à de tels réseaux, il serait mieux de simplement envoyer des notifications à un administrateur du réseau désigné sur le site. Dans un tel cas, l'administrateur du réseau local pourrait aimer recevoir des informations supplémentaires dans une telle notification, comme une date et un horodatage, l'accès de source du système infecté, et les sites et accès malveillants qui peuvent avoir été visités.

5.10 Notification et expertise de l'utilisateur final

L'efficacité ultime de toutes les formes de notification susmentionnées dépend fortement de l'expertise de l'utilisateur final et de la formulation d'une telle notification. Par exemple, lorsque un usager reçoit et accuse réception d'une notification, cet usager peut manquer de la nécessaire expertise technique pour comprendre ou être capable de traiter effectivement la menace. Par suite, il est important que de telles notifications utilisent un langage clair et facile à comprendre, afin que la majorité des usagers (qui ne sont pas des techniciens) puisse comprendre la notification. De plus, une notification devrait fournir des lignes directrices faciles à comprendre sur la façon de remédier à une menace comme décrit à la Section 6, potentiellement avec un chemin pour que les usagers avec des connaissances techniques, et un autres pour ceux qui n'en ont pas.

6. Remèdes pour les hôtes infectés par un robot

Cette section couvre les différentes options disponibles pour porter remède à un hôte, ce qui signifie de retirer, désactiver, ou autrement rendre un robot inoffensif. Avant cette étape, un FAI a détecté le robot, notifié à l'usager qu'un de ses hôtes est infecté avec un robot, et peut maintenant fournir des moyens recommandés pour nettoyer l'hôte. L'approche généralement recommandée est de fournir les outils et les instructions nécessaires à l'usager afin qu'il puisse effectuer lui-même la suppression du robot, étant donnés les risques et difficultés particulières inhérentes aux tentatives de suppression d'un robot.

Par exemple, cela peut inclure la création d'un site spécial de la Toile au contenu tourné vers la sécurité qui serait dédié à cet effet. Ceci devrait être un site de sécurité de la Toile faisant l'objet d'une bonne publicité auquel un usager confronté à une infection par un robot peut être dirigé pour trouver les remèdes. Ce site de sécurité de la Toile devrait expliquer clairement pourquoi l'usager a reçu une notification et pourrait inclure une explication de ce que sont les robots et les menaces qu'ils font peser. Il devrait y avoir une claire explication des étapes que l'usager devrait suivre afin de tenter de nettoyer son hôte et des

informations sur la façon dont les usagers peuvent garder leur hôte à l'abri de futures infections. Le site de sécurité de la Toile devrait aussi avoir un processus de guidage qui emmène les usagers non techniciens à travers le processus de réparation, étape par étape et faciles à comprendre.

En termes de texte utilisé pour expliquer ce que sont les robots et les menaces qu'ils font peser, quelque chose de simple comme ce qui suit peut suffire :

Qu'est ce qu'un robot ? Un robot est un morceau de logiciel, généralement installé à votre insu sur votre machine qui envoie des messages non désirés ou essaye de voler vos informations personnelles. Il peut être très difficile à détecter, bien que vous ayez pu remarquer que votre ordinateur fonctionne beaucoup plus lentement que d'habitude ou que vous ayez pu remarquer une activité régulière du disque même quand vous ne faites rien. Ignorer ce problème présente des risques pour vous et vos informations personnelles .Donc, les robots doivent être retirés pour protéger vos données et vos informations personnelles.

De nombreux robots sont conçus pour fonctionner de façon très furtive, et à ce titre, il peut être nécessaire de vous assurer que l'utilisateur de l'Internet comprend l'ampleur de la menace qu'il a en face de lui en dépit de la nature furtive du robot.

Il est aussi important de noter qu'il peut n'être pas immédiatement apparent à l'utilisateur de l'Internet quels appareils ont précisément été infectés par un robot particulier. Cela peut être dû à la configuration du réseau de rattachement de l'usager, qui peut englober plusieurs hôtes, où a été utilisée une passerelle de rattachement qui effectue la traduction d'adresse réseau (NAT, *Network Address Translation*) pour partager une seule adresse IP publique. Donc, l'un de ces appareils peut être infecté par un robot. La conséquence de cela pour un FAI est qu'un conseil de remède peut en fin de compte n'être pas immédiatement opérable par l'utilisateur de l'Internet, car cet usager peut avoir besoin d'effectuer des investigations supplémentaires au sein de son propre réseau de rattachement.

Une complication supplémentaire est que l'usager peut avoir une infection de robot sur un appareil comme une console vidéo, un système multimédia, un appareil, ou autre système informatique d'usager terminal qui n'a pas une interface typique d'ordinateur. Par suite, il faut que le FAI soit vigilant lorsque possible afin qu'il puisse identifier et communiquer la nature spécifique de l'appareil qui a été infecté par un robot et fournir des avis de remèdes plus appropriés. Si le FAI ne peut pas isoler l'appareil ou identifier son type, il devrait alors préciser à l'usager que tout avis initial est générique et qu'un avis plus motivé pourra être donnés (ou est disponible) une fois que le type de l'appareil infecté sera connu.

Il y a un certain nombre de forums qui existent en ligne pour fournir un soutien en rapport avec la sécurité aux utilisateurs finaux. Ces forums sont animés par des volontaires et sont souvent concentrés sur l'utilisation d'un ensemble d'outils commun pour aider les utilisateurs finaux à soigner les hôtes infectés par des malgiciels. Il peut être avantageux que les FAI entretiennent des relations avec un ou plusieurs forums, peut-être en leur offrant un hébergement gratuit ou d'autres formes de soutien.

Il est aussi important de garder présent à l'esprit que tous les utilisateurs ne seront pas techniquement compétents, comme on l'a noté au paragraphe 5.10. Par suite, il peut être plus efficace de fournir une gamme d'options de suggestions comme remède. Cela peut inclure, par exemple, une approche très détaillée de "à faire vous-mêmes" pour les experts, un processus guidé plus simple pour l'utilisateur moyen, et même une assistance aux soins comme décrit au paragraphe 6.2.

6.1 Processus de remède guidé

Au minimum, le processus de remède guidé devrait inclure les objectifs suivants, avec des options et/ou recommandations pour les réaliser :

1. Sauvegarder les fichiers personnels. Par exemple, avant de commencer, s'assurer de sauvegarder toutes les données importantes. (On devrait faire cela de façon régulière.) On peut sauvegarder ses fichiers manuellement ou en utilisant un utilitaire logiciel de sauvegarde système, qui peut faire partie du système d'exploitation (OS, *Operating System*). On peut sauvegarder les fichiers sur une clé USB, un CD/DVD-ROM réinscriptible, un disque dur externe, un serveur de fichier du réseau, ou un service de sauvegarde sur l'Internet. On peut suggérer qu'il serait sage que la sauvegarde de l'usager soit effectuée sur un appareil ou support de sauvegarde séparé si on suspecte une infection de robot.

2. Télécharger les réparations d'OS et les mises à jour de logiciel anti-virus (A/V). Par exemple, des liens pourraient être fournis avec les mises à jour de Microsoft Windows, d'OS Mac d'Apple, ou autres systèmes d'exploitation majeurs qui sont pertinents pour les usagers et leurs appareils.

3. Configurer l'hôte à installer automatiquement les mises à jour de l'OS, A/V, et autres navigateurs communs de la Toile comme Internet Explorer de Microsoft, Mozilla Firefox, Apple Safari, Opera, et Google Chrome.

4. Obtenir l'assistance d'un professionnel si on est incapable de supprimer les robots soi-même. Si on achète l'assistance d'un

professionnel, on devrait être invité à déterminer à l'avance combien on accepte de payer cette aide. Par exemple, si l'hôte à réparer est vieux et peut facilement être remplacé par un système nouveau, plus rapide, plus grand, et plus fiable pour un certain coût, il n'y aurait pas de sens à dépenser plus que cela pour réparer le vieil hôte. D'un autre côté, si le consommateur a un hôte tout neuf, il peut être parfaitement raisonnable de dépenser cette somme pour tenter de le réparer.

5. Pour continuer, que l'usager ou un assistant technique compétent travaille à la réparation de l'hôte, la première tâche devrait être de déterminer laquelle des plusieurs machines potentiellement infectées peut être celle qui réclame l'attention (dans le cas courant de plusieurs hôtes dans un réseau de rattachement). Parfois, comme dans les cas où il y a seulement un hôte directement rattaché, ou si l'usager a remarqué des problèmes chez un de ses hôtes, ceci peut être facile. D'autres fois, ce peut être plus difficile, en particulier si il n'y a pas d'indices montrant quel hôte est infecté. Si l'usager est derrière une passerelle/routeur de rattachement, la première tâche peut alors être de s'assurer de quelles machines sont infectées. Dans certains cas, l'usager peut devoir vérifier toutes les machines pour identifier celle qui est infectée.

6. Les FAI peuvent aussi offrir un CD/DVD avec des processus et logiciels de réparation pour le cas où un hôte serait si gravement infecté qu'il serait incapable de communiquer sur l'Internet.

7. Des enquêtes pourraient être faites auprès des utilisateurs pour solliciter des retours sur l'efficacité du processus de notification et de réparation et quelles recommandations de changements pourraient améliorer la facilité d'utilisation, la compréhension et l'efficacité du processus de réparation.

8. Si l'usager est intéressé à faire rapport de l'infection par un robot de l'hôte à une autorité d'application des lois, l'hôte devient alors une "scène de crime" cybernétique, et l'infection ne devrait pas être réparée tant que les autorités n'ont pas collecté les preuves nécessaires. Pour des individus dans cette situation, le FAI peut souhaiter fournir des liens avec les autorités locales, régionales, nationales, ou autres compétentes pour la criminalité informatique. (Note : certains incidents "mineurs", même si ils sont très traumatisants pour l'usager, peuvent n'être pas suffisamment sérieux pour que les autorités engagent leurs ressources limitées dans une investigation.) De plus, chaque région peut avoir des organisations dédiées au crime informatique auxquelles ces incidents peuvent être rapportés. Par exemple, aux États-Unis, cette organisation est le "Internet Crime Complaint Center", à http://www.ic3.gov.

9. Les usagers peuvent aussi être intéressés par des liens avec des forums d'experts de sécurité, où d'autres usagers peuvent les aider.

6.2 Processus de remède avec assistance professionnelle

Il faut reconnaître que sur la base de l'état actuel des outils de réparation et des capacités techniques des utilisateurs finaux, de nombreux utilisateurs sont dans l'incapacité de se réparer tout seuls. Par suite, il est recommandé que les usagers aient l'option d'une assistance professionnelle. Cela peut englober une assistance en ligne ou par téléphone pour la réparation, ainsi qu'un travail in situ avec un professionnel qui a l'entraînement et l'expertise de la suppression de malgiciels. Il devrait être clair au moment de l'offre de ce service qu'il est destiné à ceux qui n'ont pas les compétences ou ne se sentent pas assez sûrs d'eux pour tenter la réparation et qu'il n'est pas une vente déguisée du FAI.

7. Échec ou refus de remède

Les systèmes de FAI devraient retracer l'historique de l'infection des hôtes par des robots afin de détecter quand des usagers ont délibérément manqué à réparer ou refusé de prendre des mesures pour réparer. Dans de tels cas, les FAI peuvent devoir envisager de prendre des mesures supplémentaires pour protéger leur réseau, les autres usagers et hôtes sur ce réseau, et les autres réseaux. De telles mesures peuvent inclure une progression d'actions jusque et y inclus la clôture du compte. Le refus de réparer peut être vu comme un problème commercial, et à ce titre, aucune recommandation technique n'est possible.

8. Partage de données entre l'usager et le FAI

On considèrera de plus qu'il pourrait être utile de créer un processus par lequel les usagers pourraient choisir, à leur gré et sur leur consentement exprès, de partager les données concernant leurs infections par des robots avec leur FAI et/ou d'autres tiers autorisés. De tels tiers peuvent inclure des entités gouvernementales qui agrègent ces données, comme le "Internet Crime Complaint Center" mentionné plus tôt dans le présent document, des institutions universitaires, et/ou des chercheurs en sécurité. Bien que dans la plupart des cas les informations partagées avec le FAI ou des tiers désignés ne seront utilisées que pour une analyse statistique agrégée, il est aussi possible que certaines recherches soient mieux satisfaites par des données plus détaillées. Donc, tout partage de données d'utilisateur avec le FAI ou des tiers autorisés peut contenir certains types d'informations personnelles identifiables, volontairement ou non. Par suite, de tels partages de données devraient être activés

de façon facultative, où les usagers revoient et approuvent les données à partager et les tiers avec lesquels elles le seront, sauf si le FAI est déjà obligé de partager de telles données afin de se conformer aux lois et règlements locaux applicables.

9. Considérations de sécurité

Le présent document décrit en détails les nombreux risques pour la sécurité et les problèmes qui se rapportent aux réseaux de zombis. À ce titre, il a été jugé approprié d'inclure des informations spécifiques sur la sécurité dans chacune des sections qui précèdent. Le présent document décrit les risques de sécurité relatifs aux infections de robots malveillants eux-mêmes, comme de permettre le vol d'identité, le vol d'accréditifs d'authentification, et l'utilisation d'un hôte pour participer involontairement à une attaque de DDoS, entre autres risques. Finalement, le document décrit aussi les risques de sécurité qui se rapportent aux méthodes particulières de communication d'une notification aux utilisateurs de l'Internet. Les réseaux de robots et les infections de robots posent des risques extrêmement sérieux de sécurité, de sorte que les lecteurs devraient revoir très attentivement le présent document.

De plus, concernant les notifications comme décrit à la Section 5, on devrait veiller à s'assurer que les notifications ont été fournies aux usagers par un site et/ou partie digne de confiance, afin que la notification soit plus difficile à imiter pour les usurpateurs et/ou parties malveillantes qui utilisent des tactiques d'ingénierie sociale. Autrement on devrait avoir soin de s'assurer que l'usager a un certain niveau de confiance que la notification est valide et/ou que l'usager a des moyens pour vérifier via un autre mécanisme ou étape que la notification est valide.

10. Considérations de confidentialité

Le présent document décrit de façon très générale les activités auxquelles les FAI devraient être sensibles, c'est-à-dire lorsque la collecte ou la communication de PII serait possible. De plus, lorsque on effectue des notifications aux utilisateurs finaux (voir la Section 5) ces notifications ne devraient pas inclure de PII.

Comme on l'a noté à la Section 8, tout partage de données provenant de l'usager au FAI et/ou des tiers autorisés devrait être fait sur la base d'une option. De plus, le FAI et/ou les tiers autorisés devraient clairement déclarer quelles données seront partagées et avec qui elles le seront.

Finalement, comme noté dans les autres sections, il peut y avoir des exigences légales ou jurisprudentielles concernant la durée pendant laquelle les données relatives aux abonnés ou les autres données doivent être conservées. Un FAI fonctionnant dans un tel cadre juridique devrait connaître ces exigences et s'y conformer.

11. Remerciements

Les auteurs souhaitent remercier les individus et groupes suivants qui ont effectué la relecture détaillée de ce document et/ou ont fourni des commentaires et réactions qui ont aidé à l'améliorer et le faire évoluer :

Mark Baugher	Stephen Farrell	David Reed
Richard Bennett	Eliot Gillum	Roger Safian
James Butler	Joel Halpern	Donald Smith
Vint Cerf	Joel Jaeggli	Joe Stewart
Alissa Cooper	Scott Keoseyan	Forrest Swick
Jonathan Curtis	Murray S. Kucherawy	Sean Turner
Jeff Chan	The Messaging Anti-Abuse Working Group (MAAWG)	Robb Topolski
Roland Dobbins	Jose Nazario	Maxim Weinstein
Dave Farber	Gunter Ollmann	Eric Ziegast

12. Références pour information

[BIOS] Sacco, A. et A. Ortega, "Persistent BIOS Infection", mars 2009, <http://www.coresecurity.com/files/attachments/Persistent_BIOS_Infection_CanSecWest09.pdf >.

[Combat-Zone] Alshech, E., "Cyberspace as a Combat Zone: The Phenomenon of Electronic Jihad", février 2007, <http://www.memrijttm.org/content/en/report.htm?report=1822 >.

[Conficker] Porras, P., Saidi, H., et V. Yegneswaran, "An Analysis of Conficker's Logic et Rendezvous Points", mars 2009, <

http://mtc.sri.com/Conficker/ >.

[DDoS] Saafan, A., "Distributed Denial of Service Attacks: Explanation, Classification et Suggested Solutions", mars 2009, < www.exploit-db.com/download_pdf/14738/ >.

[Dragon] Nagaraja, S. et R. Anderson, "The snooping dragon: social-malware surveillance of the Tibetan movement", mars 2009, < http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf >.

[Estonia] Evron, G., "Battling Botnets et Online Mobs: Estonia's Defense Efforts during the Internet War", 2008, <http://journal.georgetown.edu/wp-content/uploads/9.1-Evron.pdf >.

[Gh0st] Vallentin, M., Whiteaker, J., et Y. Ben-David, "The Gh0st in the Shell: Network Security in the Himalayas", février 2010, < http://www.infowar-monitor.net/wp-content/uploads/2010/02/cs294-28-paper.pdf >.

[RFC1459] J. Oikarinen et D. Reed, "Protocole Internet de relais de débats", mai 1993. *(Exp., MàJ par 2810-13)*

[RFC2142] D. Crocker, "Noms de boîtes aux lettres pour les services, rôles et fonctions communs", mai 1997. *(P.S.)*

[RFC3954] B. Claise, éd., "Format d'exportation de données pour la version 9 des services NetFlow de Cisco Systems", octobre 2004. *(Information)*

[RFC5070] R. Danyliw et autres, "Format d'échange de description d'objet Incident", décembre 2007. *(P.S.) (MàJ par la* RFC6685*)*

[RFC5965] Y. Shafranovich, J. Levine, M. Kucherawy, "Format extensible pour les rapports de retour de messagerie", août 2010. *(P.S.)* (*MàJ par la* RFC6650)

[RFC6108] C. Chung, A. Kasyanov, J. Livingood, N. Mody, B. Van Lieu, "Concept du système de notification de la Toile de Comcast", février 2011. *(Information)*

[Snort] Roesch, M., "Snort Home Page", mars 2009, < http://www.snort.org/ >.

[Spamalytics] Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G., Paxson, V., et S. Savage, "Spamalytics: An Empirical Analysis of Spam Marketing Conversion", octobre 2008, <http://www.icir.org/christian/publications/2008-ccs-spamalytics.pdf >.

[Threat-Report] Ahamad, M., Amster, D., Barret, M., Cross, T., Heron, G., Jackson, D., King, J., Lee, W., Naraine, R., Ollman, G., Ramsey, J., Schmidt, H., et P. Traynor, "Emerging Cyber Threats Report for 2009: Data, Mobility et Questions of Responsibility will Drive Cyber Threats in 2009 et Beyond", octobre 2008, <http://smartech.gatech.edu/bitstream/1853/26301/1/CyberThreatsReport2009.pdf >.

[Whiz-Kid] Berinato, S., "Case Study: How a Bookmaker et a Whiz Kid Took On a DDOS-based Online Extortion Attack", mai 2005, <http://www.csoonline.com/article/220336/How_a_Bookmaker_et_a_Whiz_Kid_Took_On_a_DDOS_based_Online_Extortion_Attack >.

Appendice A. Exemples de listes de tiers de logiciels malvaillants

Comme noté à la Section 4, de nombreux tiers potentiels peuvent vouloir partager des listes d'hôtes infectés. Cette liste n'est donnée qu'à titre d'exemple, et n'est destinée à être ni exclusive ni exhaustive, et elle va changer au fil du temps.

- Arbor - Atlas, voir à http://atlas.arbor.net/
- Internet Systems Consortium - Secure Information Exchange (SIE), voir à https://sie.isc.org/
- Microsoft - Smart Network Data Services (SNDS), voir à https://postmaster.live.com/snds/
- SANS Institute / Internet Storm Center - DShield Distributed Intrusion Detection System, voir à http://www.dshield.org/about.html
- ShadowServer Foundation, voir à http://www.shadowserver.org/
- Spamhaus - Policy Block List (PBL), voir à http://www.spamhaus.org/pbl/
- Spamhaus - Exploits Block List (XBL), voir à http://www.spamhaus.org/xbl/
- Team Cymru - Community Services, voir à http://www.team-cymru.org/

Adresse des auteurs

Jason Livingood
Comcast Cable Communications
One Comcast Center
1701 John F. Kennedy Boulevard
Philadelphia, PA 19103
USA
mél : jason_livingood@cable.comcast.com
URI : http://www.comcast.com

Nirmal Mody
Comcast Cable Communications
One Comcast Center
1701 John F. Kennedy Boulevard
Philadelphia, PA 19103
USA
mél : nirmal_mody@cable.comcast.com
URI : http://www.comcast.com

Mike O'Reirdan
Comcast Cable Communications
One Comcast Center
1701 John F. Kennedy Boulevard
Philadelphia, PA 19103
USA
mél : michael_oreirdan@cable.comcast.com
URI : http://www.comcast.com