This translation is a joint initiative of MAAWG (www.maawg.org) and ITU (www.itu.int/ITU-D/cyb/cybersecurity).

MEILLEURES PRATIQUES DU MAAWG CONCERNANT L'UTILISATION D'UN JARDIN FERMÉ

Critères de sortie et d'entrée, apport de solutions et sensibilisation des abonnés

Introduction

Compte tenu de l'augmentation des utilisations abusives du réseau par les abonnés, les fournisseurs de services Internet (ISP) sont obligés d'appliquer des mesures plus proactives afin de protéger leurs réseaux et le trafic qui en sort. Les spammeurs et les pirates recourent de plus en plus à des "réseaux de machines zombies" ("botnets") pour utiliser abusivement le réseau en propageant des spams, des virus et d'autres formes de maliciels. Ces maliciels sont installés subrepticement sur les ordinateurs personnels des abonnés, à leur insu, qui sont alors très nombreux à être pris pour cibles pour être des complices dans ces réseaux malveillants, sans s'en rendre compte.

Afin de renforcer la mission du MAAWG qui consiste à préserver la messagerie électronique contre les utilisations abusives et les exploits en ligne, le sous-comité du MAAWG chargé des réseaux de machines zombies recommande de suivre les meilleures pratiques ci-après concernant la mise en œuvre d'un jardin fermé. Un jardin fermé désigne un environnement qui contrôle les informations et les services qu'un abonné est autorisé à utiliser et les autorisations d'accès au réseau qui sont accordées. Ces pratiques visent essentiellement à aider les utilisateurs finals à repérer et à supprimer les programmes non souhaités ou les maliciels qui résident dans leurs ordinateurs personnels et à mettre fin aux utilisations abusives du réseau. Sauf indication contraire, il appartient aux ISP de mettre en œuvre toutes les recommandations.

Les utilisations et les définitions des mots clés tels que DOIT/OBLIGATION, DEVRAIT/RECOMMANDATION et PEUT/POSSIBILITÉ employés dans l'ensemble du présent document sont à interpréter comme indiqué dans le Document RFC 2119.

I. Les critères de sortie et d'entrée applicables à un jardin fermé doivent être concis

Afin de sensibiliser les utilisateurs aux risques et aux problèmes associés à un ordinateur personnel infecté par un maliciel, les ISP PEUVENT mettre en œuvre un jardin fermé pour les nouveaux comptes d'utilisateur ou pour tout compte qu'ils jugent dangereux ou générateur de trafic suspect. Les critères d'entrée et de sortie applicables à un jardin fermé doivent être clairs et concis de manière à être compris par l'utilisateur final.

Résumé des recommandations:

a) OBLIGATION de notifier clairement le problème suspecté; par exemple utilisation du réseau non conforme à la politique d'utilisation acceptable (AUP). OBLIGATION

aussi d'expliquer la notification et de donner les grandes lignes de la procédure recommandée pour remédier au problème ou pour effacer le maliciel de l'ordinateur.

b) **POSSIBILITÉ de rediriger le trafic HTTP [80] vers l'adresse ou le site web de quarantaine.**

c) **POSSIBILITÉ de rediriger le trafic de commande et de contrôle des réseaux de machines zombies vers un réseau leurre pour analyse.**

d) **RECOMMANDATION de gérer l'ensemble du trafic SMTP [25] sortant vers une zone de quarantaine ou un agent de transfert de messages (MTA) leurre.**

e) **RECOMMANDATION de permettre un échappement immédiat basé sur la confiance. La confiance peut être confirmée par une action témoignant d'un ordinateur personnel propre ou par une demande d'utilisation du réseau "tel qu'il est" pendant une période configurable.**

f) **POSSIBILITÉ de permettre la sortie si certains logiciels de nettoyage ou de sécurité approuvés par l'ISP sont téléchargés et installés.**

g) **L'ISP PEUT utiliser des paramètres internes de réputation de l'abonné (déterminés au moyen de techniques de détection telles que des filtres de contenu, une inspection approfondie des paquets et des diagrammes d'utilisation/comportement) pour déclencher des événements d'entrée dans le jardin fermé ou de sortie de ce jardin.**

h) **L'ISP PEUT utiliser des technologies permettant de déterminer automatiquement la posture de sécurité de l'abonné telle qu'annoncée par le logiciel client installé et sécurisé de l'abonné.**

II. Les solutions apportées doivent être pratiques pour l'utilisateur final

A mesure que les ISP continuent de veiller à protéger leurs réseaux et leurs abonnés contre les utilisations abusives, il est important que leur façon de procéder ne soit pas trop compliquée pour l'utilisateur final. Pour couvrir ses investissements, l'ISP PEUT aussi choisir d'offrir des solutions à l'utilisateur final moyennant paiement. Ces solutions DOIVENT être fournies via un support compatible avec l'environnement d'assistance type de l'ISP. De plus, le jardin fermé DOIT permettre d'accéder aux sites web de sorte que l'utilisateur final puisse télécharger les mises à jour et les corrections logicielles applicables critiques, soit par accès direct soit par accès indirect via un proxy. (Ceci offre la possibilité pour le fournisseur ou l'ASP sous contrat de fournir des solutions via un seul portail, comme c'est le cas de Microsoft avec Windows Update et les nombreux téléchargements de nouveaux programmes de commande qu'il lance pour votre compte.)

Résumé des recommandations:

a) **OBLIGATION de pouvoir fournir des solutions gratuites et/ou payantes (ou des liens vers les outils en ligne existants).**

b) **OBLIGATION de présenter des informations reconnaissables qui légitiment la pratique en tant que procédure de notification et de correction officielle de l'ISP. Ces informations peuvent par exemple être des données comme un numéro de compte ou la réponse secrète à une question.**

c) **OBLIGATION de fournir des détails sur comment contacter le service d'assistance clientèle pour obtenir de l'aide.**

d) **RECOMMANDATION de ne pas nécessiter de réamorçage de l'ordinateur personnel de l'utilisateur final pour que la solution entre en application.**

e) **OBLIGATION de fournir des liens vers des URL et des domaines qui aident à résoudre le problème avec des programmes de correction de système d'exploitation et des mises à jour de sécurité (le cas échéant).**

f) **RECOMMANDATION de permettre, par un clic, de dialoguer avec le service d'assistance clientèle ou avec un tiers offrant une assistance clientèle pour le compte de l'ISP.**

g) **RECOMMANDATION de fournir des informations sur un contact pour obtenir l'aide de l'ISP ou pour signaler une utilisation abusive (par exemple un numéro de téléphone).**

h) **RECOMMANDATION de demander aux clients qui envoient du trafic SMTP [25] malveillant de reconfigurer les agents utilisateur de courrier (MUA) pour envoyer les messages électroniques sortants sur le port 587.**

i) **RECOMMANDATION de présenter des solutions uniques en fonction du problème et des actions passées de l'utilisateur; autrement dit, un utilisateur DEVRAIT obtenir une solution pour son problème exact ou pour le type de maliciel suspecté.**

j) **RECOMMANDATION de fournir un client de sécurité qui soit le moins intrusif possible, se télécharge rapidement, s'installe facilement sans conflit avec les autres logiciels d'application (par exemple un client de sécurité déjà configuré), ne nécessite pas de réamorçage et ne nécessite pas de balayage complet de l'ordinateur pour détecter et supprimer le maliciel.**

k) **OBLIGATION de prévoir des exceptions de réacheminement pour que l'utilisateur soit autorisé à utiliser les services d'urgence en ligne.**

III. La sensibilisation des utilisateurs finals devrait faire partie des priorités

Etant donné que l'utilisateur final est généralement le maillon faible de la chaîne de sécurité, l'ISP DEVRAIT déployer des efforts raisonnables en termes de documentation disponible sur son site web pour que l'utilisateur final puisse s'informer de façon proactive sur les moyens de réduire les risques d'infection par maliciel. A cet égard, une documentation sous la forme de FAQ, de vidéos d'assistance, de didacticiels et d'une base de données de connaissances interrogeable DEVRAIT être mise à la disposition de l'utilisateur final. Si de tels matériels sont fournis, ils DOIVENT être mis à la disposition de l'utilisateur final au moyen d'une méthode cohérente avec l'aspect de l'interface du service d'assistance clientèle de l'ISP. De plus, la documentation disponible DEVRAIT être suffisamment large pour couvrir les applications utilisées avec plusieurs types différents de technologies Internet et avec plusieurs types différents de systèmes d'exploitation informatiques (par exemple Windows, MacOS, Linux).

Résumé des recommandations:

a) **OBLIGATION de présenter des informations reconnaissables qui légitiment la pratique en tant que procédure de notification et de correction officielle de l'ISP. Ces informations peuvent par exemple être des données comme un numéro de compte ou la réponse secrète à une question.**

b) **RECOMMANDATION de sensibiliser intuitivement les utilisateurs au moyen de FAQ et de didacticiels.**

c) **RECOMMANDATION de fournir d'autres outils d'apprentissage (par exemple une présentation vidéo simple et des centres de connaissances interrogeables).**

d) **RECOMMANDATION de fournir des informations de sensibilisation pour plusieurs types d'applications, dont la messagerie électronique (POP3/SMTP) et la navigation (HTTP).**