SAC 025
Rapport consultatif du SSAC sur l'hébergement fast-flux et le DNS

REMARQUE SUR LES TRADUCTIONS

La version originale du présent document est rédigée en anglais. Elle est disponible sur la page Web http://www.icann.org/committees/security/sac025.pdf. En cas de différence d'interprétation entre le présent document et le texte original, ce dernier prévaut.

Rapport consultatif du conseil consultatif sur la sécurité et la stabilité
(SSAC, Security and Stability Advisory Committee)
de l'ICANN
Janvier 2008

Introduction

Le « fast-flux » est une technique de dissimulation utilisée pour les cybercriminels et les pirates de l'Internet pour éviter d'être identifiés et déjouer les mesures de lutte anti-criminalité visant à localiser et à fermer les sites utilisés pour des activités illégales. L'hébergement fast-flux est utilisé pour une grande variété de pratiques cybercriminelles (fraude, usurpation d'identité, scams en ligne) et il est considéré comme l'une des menaces les plus sérieuses pour les activités en ligne aujourd'hui. L'une des variantes de l'hébergement fast-flux, l'architecture « double-flux », exploite les failles des services d'enregistrement de noms de domaine et de résolution de noms.

Ce rapport consultatif décrit les aspects techniques de l'hébergement fast-flux et des réseaux de services fast-flux. Il explique la manière dont le DNS est exploité pour développer des activités illégales qui utilisent l'hébergement fast-flux, identifie les conséquences de l'hébergement fast-flux et souligne la manière dont ces attaques permettent de prolonger ces activité illégales. Il décrit les méthodes actuelles et possibles pour atténuer les risques liés à l'hébergement fast-flux en divers points de l'Internet. Ce rapport consultatif présente les avantages et les inconvénients de ces méthodes, identifie les méthodes que le SSAC considère comme applicables et raisonnables, et recommande que les organismes appropriés envisagent des règles qui rendraient ces méthodes pratiques d'atténuation des risques universellement disponibles pour les registrants, les fournisseurs de services Internet, les bureaux d'enregistrement et les registres (selon ce qui peut être appliqué pour chacun).

Contexte

Les professionnels de la sécurité, la communauté de la lutte contre la cybercriminalité et les organismes chargés de l'application de la loi étudient depuis un certain temps l'hébergement fast-flux. L'hébergement fast-flux fonctionne au haut d'un grand réseau réparti de systèmes compromis tout à fait susceptible de s'étendre au monde entier. Un marché souterrain extrêmement florissant loue des milliers de systèmes compromis à des pirates Internet en tant que réseaux de services fast-flux[1]. Les opérateurs de ces réseaux de services utilisent des canaux de communication hiérarchiques invisibles (chiffrés) et des techniques de proxy. Ils gèrent ces réseaux avec une grande efficacité en interrogeant à intervalles réguliers l'état des systèmes compromis, et ils administrent les ajouts et les suppressions aux réseaux selon la présence ou l'absence de réponse. La communauté des noms de domaine est particulièrement préoccupée par la manière dont ces opérateurs automatisent les modifications des services de noms de domaine pour masquer l'emplacement des sites Web sur lesquels sont effectuées des activités illégales : interception IP (musique, vidéos, jeux), hébergement de sites à contenu pédophile, hébergement de systèmes d'hameçonnage (phishing), vente de produits pharmaceutiques illégaux, vol et usurpation d'identité, etc.

[1] Les organismes de sécurité utilisent divers termes pour décrire l'hébergement fast-flux dans leurs documents et publications. Dans le présent rapport consultatif, nous appliquons la terminologie utilisée dans un rapport Honeynets Project, *Know Your Enemy: Fast Flux Service Networks*, voir http://www.honeynet.org/papers/ff/

L'une des variantes de l'hébergement fast-flux utilise des modifications rapides du DNS pour masquer l'emplacement des sites Web et d'autres services Internet qui hébergent des activités illégales. Dans une seconde variante, appelée « double-flux », les pirates Internet complètent le réseau de services qui héberge des sites Web par un second réseau de services qui héberge des serveurs DNS. Le fonctionnement de ces réseaux de services est décrit plus en détail dans les sections suivantes de ce rapport consultatif.

Terminologie

Pour décrire cette technique complexe et multi-facettes du « fast flux » dans sa réalité actuelle, le SSAC commence par identifier les principaux termes que la communauté de la sécurité sur Internet associe à l'hébergement fast-flux :

botnet : Un botnet (robot net, réseau de robots) est un réseau d'ordinateurs tiers compromis exécutant des programmes robots (« bots » en anglais). Ces robots peuvent être contrôlés à distance (d'abord par l'initiateur réel de l'attaque et ensuite par un tiers qui paie le pirate pour utiliser le botnet) pour réaliser n'importe quelles activités non autorisées ou illégales. Le pirate, généralement lié à une organisation criminelle, installera le programme robot sans avis ni autorisation sur un ordinateur par le biais d'un téléchargement de logiciel espion ou d'un virus attaché à un message électronique, ou encore, plus communément, par l'intermédiaire du navigateur ou d'une autre faille côté client (par exemple, publicité de bannière compromise). Une fois que le programme robot peut s'exécuter, il établit une voie de retour pour permettre la configuration d'une infrastructure de contrôle par le pirate. La conception classique du botnet utilisait un modèle centralisé et toutes les voies de retour étaient connectées au centre de commande et de contrôle (C&C) d'un pirate. Récemment, les opérateurs de botnets ont commencé à employer des modèles poste-à-poste pour les voies de retour afin de déjouer la détection du centre de commande et de contrôle (C&C) par le biais de l'analyse de trafic.

bot-herder : Architecte et contrôleur de l'attaque distribuée qui est utilisée pour créer, gérer et exploiter un botnet pour un gain financier ou autre (politique). Une fois qu'un botnet est établi, le bot-herder le loue à un **opérateur de services fast-flux**

Fast-flux : Ce terme est utilisé pour décrire la possibilité de modifier rapidement l'emplacement d'un site Web, d'une messagerie, d'un DNS ou de tout service Internet ou distribué d'un ensemble d'ordinateurs à un autre sur Internet pour retarder ou empêcher toute détection.

Dispositifs fast-flux : Dans le présent document, le terme *dispositif* désigne un agent logiciel qui a été installé sans autorisation sur un grand nombre d'ordinateurs connectés à Internet.

Réseau de services fast-flux : Dans le présent document, un réseau de services désigne le sous-ensemble de programmes robots que le bot-herder assigne à un opérateur de services fast-flux donné qui, à son tour, fournit à un client des machines pour l'hébergement fast-flux ou un service de noms fast-flux. Il convient de noter que ce réseau de services est souvent contrôlé par un « intermédiaire » et non par le client lui-même.

Anatomie de l'hébergement fast-flux

La description qui suit est représentative de l'hébergement fast-flux. D'autres manifestations et variantes sont possibles, et les pirates sont susceptibles de faire évoluer la technique fast-flux pour déjouer les méthodes de détection de l'hébergement fast-flux tel qu'il est décrit ici. Ils peuvent également ajouter des couches supplémentaires de hiérarchie ou d'abstraction.

Alors que les aspects techniques du fast-flux suscitent une attention considérable, il convient également de décrire les activités frauduleuses qui s'y rattachent. Nous étudierons le cas où un pirate cherche à conduire une attaque d'hameçonnage (phishing).

Les aspects commerciaux de l'hébergement fast-flux commencent par les auteurs de logiciels malveillants. Certains auteurs de logiciels malveillants développent des kits d'hameçonnage. Il s'agit de progiciels qui peuvent être personnalisés pour fournir des courriels hameçons à une liste de destinataires et héberger le site Web illégal associé vers lequel le courriel hameçon dirige les victimes. D'autres exploitent des adresses e-mail et vendent des listes pour le spam. D'autres encore développent des logiciels robots. Un logiciel robot est un agent souple, contrôlable à distance qui peut être dirigé pour exécuter des fonctions arbitraires pour le compte d'un logiciel de **centre de commande et de contrôle** (C&C) correspondant : une fois installé frauduleusement sur un système compromis, le logiciel robot facilite les téléchargements suivants et l'exécution à distance d'un logiciel supplémentaire spécifique à une attaque. Les bot-herders utilisent souvent les vers répandus par des courriels pour infecter et compromettre des milliers de systèmes, bien que les compromissions côté client, telles que les failles basées sur les navigateurs, soient les points d'attaque les plus courants aujourd'hui.

Les auteurs de logiciels malveillants et les bot-herders sont les *fournisseurs de marchandises* de la communauté des cybercriminels.[2] Ces fournisseurs de marchandises utilisent des canaux IRC (Internet Relay Chat) chiffrés et privés/sécurisés ou des lieux de rencontre souterrains similaires pour faire leur publicité et trouver des acheteurs pour leurs marchandises délictueuses. Les marchandises délictueuses d'un bot-herder sont essentiellement les installations qu'il peut mettre à disposition par le biais d'un accord de location ou d'abonnement. Le bot-herder loue le contrôle d'un nombre négocié de systèmes compromis à un client qui peut les utiliser directement ou les gérer pour le compte d'une autre pirate ; dans ce dernier cas, le client du bot-herder joue le rôle de fournisseur de services d'hébergement fast-flux. Dans cette économie complexe et souterraine, un tiers qui veut conduire des activités frauduleuses peut négocier avec plusieurs tiers pour obtenir une liste de spam (hameçons), déployer un système d'hameçonnage et un autre kit d'attaques, et un botnet ou conduire l'attaque lui-même, ou il peut négocier avec un autre tiers, un opérateur de réseau de service fast-flux, pour diriger l'attaque d'hameçonnage pour son compte.

Dans l'hébergement fast-flux, les réseaux de services fast-flux sont utilisés pour deux fonctions :

1) **Héberger des sites Web directifs :** Les programmes robots de ce réseau de services n'hébergent généralement pas le contenu du client de fast-flux, mais il redirige le trafic Web vers le serveur Web sur lequel le client fast-flux héberge des activités non autorisées ou illégales. Lorsqu'il s'agit du seul réseau exploité pour l'hébergement fast-flux, le terme *single-flux* est employé.

2) **Héberger des serveurs de noms :** Les programmes robots de ce réseau de service exécutent des référents de serveurs de noms pour le client fast-flux. Ces serveurs de noms transmettent les requêtes DNS à des serveurs de noms masqués qui hébergent des enregistrements de ressource A DNS pour un ensemble de sites Web directifs. Les serveurs de noms masqués ne retransmettent pas les réponses via le serveur de noms de renvoi mais répondent directement à l'hôte demandeur. Lorsque ce second réseau est exploité conjointement avec (1) pour renforcer la dissimulation, le terme *double-flux* est utilisé.

[2] An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants, voir http://www.cs.cmu.edu/~jfrankli/acmccs07/ccs07_franklin_eCrime.pdf

La figure 1 illustre ces mécanismes.

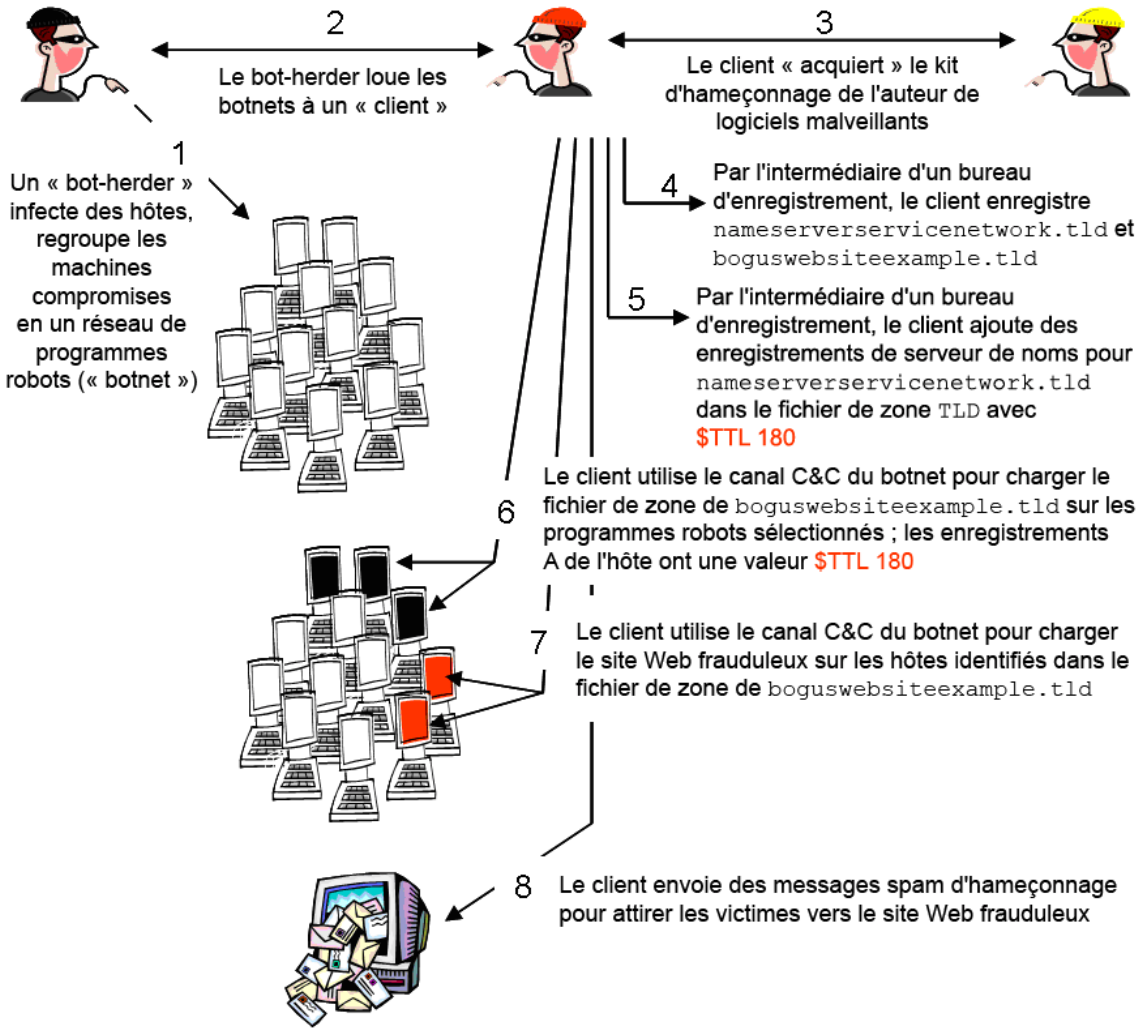

Figure 1. Éléments d'une attaque avec hébergement « double-flux »

Exploitation du service de noms : hébergement « double-flux »

Les clients fast-flux enregistrent souvent des noms de domaines pour leurs activités illégales auprès d'un bureau d'enregistrement ou d'un revendeur accrédité. Dans une forme particulière d'attaque, le client fast-flux enregistre un nom de domaine (pour un réseau de services de flux) pour héberger des sites Web illégaux `(boguswebsitesexample.tld)` et un second (ou plusieurs) nom(s) de domaine pour un réseau de services de flux fournissant un service de résolution de noms `(nameserverservicenetwork.tld)`. Le client fast-flux identifie ces domaines auprès de son opérateur de réseau de services fast-flux. Celui-ci utilise des techniques automatisées pour changer rapidement les informations de serveur de noms dans les enregistrements conservés par le bureau d'enregistrement pour ces domaines ;
en particulier, l'opérateur de réseau de services fast-flux

- modifie les adresses IP du serveur de noms de domaine afin qu'elles pointent vers des hôtes différents dans le domaine `nameserverservicenetwork.tld` et ;
- définit les durées de vie (TTL, time-to-live) dans les enregistrements d'adresse pour ces serveurs de noms sur une valeur très petite (souvent 1 à 3 minutes).

Les enregistrements de ressources associés à un domaine de serveur de noms utilisé dans l'hébergement fast-flux peuvent apparaître dans un fichier de zone TLD :

```
$TTL 180
boguswebsitesexample.tld.     NS
NS1.nameserverservicenetwork.tld
boguswebsitesexample.tld.     NS
NS2.nameserverservicenetwork.tld
…
NS1.nameserverservicenetwork.tld.   A  10.0.0.1
NS2.nameserverservicenetwork.tld.   A  10.0.0.2
```

Notez que la durée de vie (TTL, time-to-live) des enregistrements de ressource est définie sur une valeur très basse (dans cet exemple, 180 secondes). À l'expiration de la durée de vie, l'automatisation de l'opérateur du réseau de services fast-flux garantit qu'un nouvel ensemble d'enregistrements A pour les serveurs de noms remplace l'ensemble existant :

```
$TTL 180
boguswebsitesexample.tld.     NS
NS1.nameserverservicenetwork.tld
boguswebsitesexample.tld.     NS
NS2.nameserverservicenetwork.tld
…
NS1.nameserverservicenetwork.tld.   A  192.168.0.123
NS2.nameserverservicenetwork.tld.   A  10.10.10.233
```

La fenêtre d'opportunité pour l'identification et la fermeture des serveurs de noms qui desservent cette attaque fast-flux est par conséquent très réduite.

Les enregistrements de ressources dans `nameserverservicenetwork.tld` pointent vers des proxy ou des hôtes de renvoi, et non vers les programmes robots qui fournissent la résolution de noms pour `boguswebsitesexample.tld`. Les hôtes de renvoi écoutent le port 53 et transmettent les requêtes DNS à un programme robot « DNS » qui héberge un fichier de zone pour `boguswebsitesexample.tld`. Le programme robot « DNS » résout le nom de domaine du site Web frauduleux en adresse IP d'un hôte dans le réseau de services de flux Web et retourne le message de réponse directement au résolveur à l'origine de la demande. À ce stade, l'adresse IP du programme robot DNS est connue uniquement par un ensemble potentiellement étendu d'hôtes de renvoi et les adresses IP des référents changent toutes les 180 secondes.

Hébergement fast-flux avec serveurs Web référents

Dans la section précédente, nous décrivons la manière dont l'hébergement « double-flux » ajoute un niveau de dissimulation par l'utilisation de programmes robots dans le réseau `nameserverservicenetwork.tld` et par une modification rapide des enregistrements A dans les hôtes de serveurs Web référents dans le réseau `boguswebsitesexample.tld`. Les enregistrements de ressource A des serveurs Web référents sont également configurés avec une valeur TTL (time-to-live, durée de vie) faible. À l'expiration des durées de vie (TTL) des hôtes de serveurs Web, l'automatisation de l'opérateur du réseau de services fast-flux garantit une nouvelle fois qu'un nouvel ensemble d'enregistrements pour les serveurs Web remplace l'ensemble existant. Par conséquent, la fenêtre d'opportunité pour l'identification et la fermeture des serveurs Web référents qui desservent cette attaque fast-flux est très réduite.

Les enregistrements associés au site Web illégal peuvent apparaître dans un fichier de zone hébergé sur un robot DNS dans le réseau `nameserverservicenetwork.tld` sous la forme suivante :

```
boguswebsitesexample.tld.     180  IN   A    192.168.0.1
boguswebsitesexample.tld.     180  IN   A    172.16.0.99
boguswebsitesexample.tld.     180  IN   A    10.0.10.200
boguswebsitesexample.tld.     180  IN   A    192.168.140.11
```

Notez encore que la durée de vie (TTL, time-to-live) de chaque enregistrement de ressource A est définie sur une valeur très basse (dans cet exemple, 180 secondes). À l'expiration de la valeur TTL, les enregistrements de ressource seront automatiquement modifiés pour pointer vers d'autres robots qui hébergent ce site Web illégal. Quelques minutes seulement plus tard, le fichier de zone peut apparaître comme suit :

```
boguswebsitesexample.tld.     180  IN   A    192.168.168.14
boguswebsitesexample.tld.     180  IN   A    172.17.0.199
boguswebsitesexample.tld.     180  IN   A    10.10.10.2
boguswebsitesexample.tld.     180  IN   A    192.168.0.111
```

Les effets combinés de la modification rapide des enregistrements A dans la zone `boguswebsitesexample.tld` et des enregistrements A de serveur de noms dans la zone TLD fournissent malheureusement un moyen très efficace permettant aux sites illégaux de continuer à fonctionner plus longtemps que les sites qui n'utilisent pas le fast-flux.

Hébergement fast-flux : quel lien avec l'essai de noms de domaine ?

Pour certains, l'essai de noms de domaine et l'hameçonnage (phishing) sont des activités liées[3]. L'APWG (Anti-Phishing Working Group, groupe de travail contre l'hameçonnage) a un publié un rapport sur les liens entre l'essai de noms de domaine et les attaques d'hameçonnage. Ce rapport résume les conclusions de deux études qui ont cherché à déterminer si les noms de domaine essayés sont également utilisés pour faciliter des attaques d'hameçonnage. Un membre de l'APWG a commencé par étudier un ensemble de noms de domaine qui a avaient été utilisés dans des attaques d'hameçonnage et il a tenté de déterminer si ces noms avaient été annulés durant la période de rédemption (Add Grace Period). Un second membre de l'APWG a comparé les noms de domaine utilisés dans des attaques d'hameçonnage avec une liste d'environ trois millions de noms de domaine essayés sur une période d'une semaine. Le résultat des deux études indique qu'« il y a très peu de cas d'essais de noms de domaine effectués par des auteurs d'attaques d'hameçonnage et que les cas qui existent ont des explications possibles qui ne sont pas liées à l'essai de noms de domaine »[4].

Les attaques d'hameçonnage utilisent de plus en plus l'hébergement fast-flux (en particulier, les attaques contre de grandes institutions financières), c'est pourquoi le SSAC conclut qu'il n'y a pas de relation significative entre l'essai de noms de domaine et l'hébergement fast-flux. Le SSAC observe également que les buts de l'hébergement fast-flux et de l'essai de noms de domaine ne sont pas les mêmes. L'un des principaux objectifs de l'hébergement fast-flux est de prolonger la durée de vie d'un site qui héberge des activités illégales historiquement établies comme lucratives, parmi lesquelles le vol d'informations financières et de cartes de crédit. Les cartes de crédit volées sont utilisées pour payer les frais d'enregistrement du nom de domaine des sites hameçonnés, il n'y a donc aucun intérêt à enregistrer un nom puis à l'abandonner. En revanche, l'unique objectif des internautes qui essaient les noms de domaine est de payer des frais d'enregistrement pour des noms de domaine qui seront rentables uniquement dans une période d'essai de quelques jours.

[3] Voir CADNA Background, http://www.cadna.org/en/index.html
[4] APWG: The Relationship of Phishing and Domain Name Tasting, http:// www.antiphishing.org/reports/DNSPWG_ReportDomainTastingandPhishing.pdf

Solutions actuelles et possibles pour limiter les risques d'attaque

Plusieurs solutions d'atténuation des risques peuvent être mises en œuvre pour réduire les menaces liées à l'hébergement fast-flux.

Fermeture des robots qui hébergent des services fast-flux

Les bot-herders piratent des ordinateurs reliés à des réseaux d'entreprise ou domestiques. Toutefois, un bot-herder exploite généralement les failles d'ordinateurs peu sécurisés qui sont connectés à des circuits d'accès haut débit résidentiels (modem câble et DSL), car la possibilité de trouver un hôte exploitable est plus grande dans cette configuration que dans les réseaux gérés par des administrateurs expérimentés. Les hôtes de réseaux d'organisme d'enseignement, d'état ou d'entreprise sont vulnérables à la compromission des systèmes, mais ils sont généralement moins susceptibles d'en être victimes et les tentatives d'exploitation de failles ont plus de chance d'être détectées par les administrateurs réseau.

Il existe plusieurs méthodes de prévention qui peuvent être largement mises en œuvres pour réduire le nombre d'ordinateurs susceptibles d'être exploités et utilisés pour héberger des programmes robots. Ces méthodes incluent notamment, de manière évidemment non limitative :

a) Amélioration des mesures de sécurité de bureau (pare-feu personnel, logiciel antivirus, logiciels de détection de logiciel espion et de détection d'intrusion d'hôte) sur les hôtes dans les réseaux privés et publics (services d'accès haut débit résidentiel).
b) Déploiement de passerelles de protection contre les logiciels malveillants par les fournisseurs d'accès Internet pour les clients avec accès haut débit résidentiel, par les fournisseurs de services de sécurité gérés ou les administrateurs de la sécurité internes pour les réseaux d'entreprise et développement de l'adoption de passerelles de protection contre les logiciels malveillants par les administrateurs de la sécurité des réseaux privés.
c) Information, sensibilisation et formation, mettant particulièrement l'accent sur la compréhension et l'application de règles de trafic de sortie très strictes.

D'autres méthodes de prévention sont également disponibles, notamment :

d) Création d'une « liste blanche » de processus et d'exécutables.
e) Contrôle des accès/admissions au réseau.
f) Analyse des comportements de botnets connus, développement de la technique de détection (par exemple, signature) qui peut être utilisée pour bloquer l'activité à une passerelle de sécurité de « gestion des menaces ». Ceci est une extension logique de (b), ci-dessus.

Bien qu'apparemment les plus pratiques à mettre en œuvre, les méthodes (a) et (b) ne se sont pas avérées efficaces pour la prévention des menaces d'attaques de logiciels malveillants.[5] Le logiciel Storm[6] ainsi que d'autres logiciels malveillants de conception similaire peuvent être modifiés et distribués de manière périodique par ses créateurs en utilisant des programmes robots[7] encore non détectés, et les mesures de protection contre les logiciels malveillants basés sur la signature n'ont pas permis d'éradiquer des logiciels malveillants tels que le virus de type cheval de Troie, Storm[8]. Les ordinateurs infectés par ce logiciel malveillant propagent la compromission plus rapidement que la communauté ne peut identifier et désinfecter les ordinateurs compromis. L'information et la sensibilisation (c) sont un processus terriblement lent. L'enquête du FBI, CSI/FBI Computer Crime and Security Survey, indique que 97 % des ordinateurs sont équipés de logiciels antivirus, 79 % de logiciels de protection contre les logiciels malveillants, mais que les infections par robots atteignent un niveau alarmant : en juin 2007, le FBI américain a annoncé que sa campagne en cours contre la cybercriminalité avait permis d'identifier plus d'un million d'ordinateurs compromis par des logiciels robots, uniquement dans la juridiction des États-Unis du FBI. Ces chiffres concernent les réseaux d'entreprise. Parmi les utilisateurs employant un accès haut débit résidentiel, l'utilisation de programmes anti-virus ou de protection contre les logiciels malveillants n'est pas aussi élevée, les configurations de réseau sont plus susceptibles d'être négligées et les abonnements aux mises à jour des logiciels de protection sont souvent mal suivis.

La création d'une liste blanche de processus et d'exécutables est une technique de protection contre les logiciels malveillants qui impose des règles sur les exécutables ; seul un ensemble approuvé d'applications et de processus liés est autorisé à s'exécuter sur un ordinateur. La création des listes blanches d'exécutables n'est pas largement répandue, en particulier parmi les internautes du grand public. La diversité des applications, le rythme d'apparition de nouvelles applications, le manque de solutions commerciales conviviales et de services qui pourraient faire office d'autorités reconnues pour les listes blanches (si ce modèle est même applicable) constituent des obstacles à l'adoption de cette technique.

Aujourd'hui, les solutions de contrôle d'admission/d'accès au réseau qui sont développées visent à interdire à des postes non sécurisés de se connecter à des réseaux locaux ou étendus. Une évaluation de sécurité est effectuée sur un ordinateur pour déterminer s'il est exempt d'exécutables malveillants avant d'autoriser cet ordinateur à se connecter à Internet. Si l'ordinateur est compromis, il est mis en quarantaine et ne peut pas être reconnecté tant que la violation de sécurité est corrigée pour l'accès haut débit résidentiel. La méthode (e) n'est pas largement répandue et nécessiterait le développement de normes et de logiciels supplémentaires. Les fournisseurs d'accès Internet et les fournisseurs d'accès haut débit résidentiel indiquent qu'ils refusent de supporter les coûts de mise en œuvre et de gestion du filtrage des accès réseau et du trafic entrant.

[5] Storm Worm DDoS Attack, http://www.secureworks.com/research/threats/view.html?threat=storm-worm
[6] *Imperfect Storm aids spammers,* http://www.securityfocus.com/news/11442
[7] Common Malware Enumeration CME-711trojan downloader. http://cme.mitre.org/data/list.html
[8] *Over 1 Million Potential Victims of Botnet Cyber Crime,* http://www.fbi.gov/page2/june07/botnet061307.htm

Mise hors service des hôtes fast-flux

Un nombre très important d'hôtes compromis utilisés dans ces attaques sont des ordinateurs connectés à des services d'accès haut débit résidentiel. Ces ordinateurs hébergent généralement le logiciel robot de serveur de noms et de serveur Web référent.

La détection, l'identification et la résolution des incidents sont les procédures d'atténuation des risques les plus couramment utilisées aujourd'hui. Tout d'abord, un système est identifié ou signalé comme hébergeant des activités illégales. Dans le scénario de l'hébergement fast-flux, il peut s'agir d'un serveur de noms ou d'un serveur Web référent, ou du système qui héberge le site Web illégal, les personnes chargées de dénoncer les irrégularités dans le cadre de la lutte contre la cybercriminalité recueillent des informations sur le site : l'emplacement et la juridiction du système hébergeur, le propriétaire du domaine, l'administrateur du site et le fournisseur de services Internet, et le type d'activité illégale. Ces personnes utilisent les services WHOIS et d'autres moyens pour identifier et contacter plusieurs parties tierces (en parallèle et de manière répétée) jusqu'à ce qu'elles reçoivent une assistance pour mettre fin à l'activité illégale[9]:

- Dans les cas où des activités illégales s'avèrent hébergées sur un système compromis (par exemple, sur un serveur Web utilisé pour des activités commerciales légales dont l'administrateur ne sait pas qu'il héberge également un site illégal) le propriétaire du domaine est contacté pour participer à la mise hors service.
- Le fournisseur de services Internet ou le fournisseur d'hébergement est contacté pour mettre fin au service fourni à cet hôte.
- Dans les cas où les personnes chargées de dénoncer les irrégularités nécessitent une assistance locale (interprétation du langage, confirmation qu'elles sont de bonne foi, ou assistance dans l'obtention d'informations supplémentaires), la communauté locale des CERT/CIRT (Computer Emergency or Incident Response Teams) est contactée. (Dans certains pays, les CERT encouragent ces personnes à les contacter au stade le plus précoce possible).
- Dans les cas où des programmes robots résidant sur des ordinateurs hébergent des serveurs de noms d'hôte, les bureaux d'enregistrement ou les registres sont contactés pour supprimer les enregistrements NS des fichiers de zone TLD ou pour suspendre des domaines.

[9] Ce scénario, tel qu'il apparaît par le biais de la correspondance personnelle avec les dénonciateurs, est représentatif des méthodes employées pour répondre aux attaques d'hameçonnage dans lesquelles l'hébergement fast-flux est utilisé de façon intensive.

[10] L'hébergement « à l'épreuve des balles » désignent les fournisseurs d'hébergement de messagerie Web et en masse qui imposent peu ou pas de conditions d'utilisation sur le contenu et les activités hébergées sur leurs serveurs. Le terme « à l'épreuve des balles » est utilisé pour souligner que les services hébergés par ce type de fournisseurs ne seront pas suspendus. Un grand nombre de fournisseurs à l'épreuve des balles ne se conduisent pas en toute bonne foi avec les organismes chargés de l'application de la loi ou de la lutte contre la criminalité, et ils opèrent dans des juridictions où les autorités locales ou les lois de l'Internet leur offrent une protection relativement sûre pour leurs activités illégales.

Les sites illégaux eux-mêmes peuvent opérer à partir de serveurs compromis dans des domaines légaux, des fournisseurs de sites Web d'hébergement mutualisé, ou des installations d'hébergement Web « à l'épreuve des balles » (quasi-)légaux. Dans les cas où cette coopération n'est pas évidente, lorsque les opérateurs ou les autorités locales ne reconnaissent pas les dénonciateurs ou ne leur font pas confiance, ou ne souhaitent pas s'appuyer sur les informations fournies par ces personnes ou les CERT, les dénonciateurs peuvent demander l'aide des organismes chargés de l'application de la loi ou chercher à obtenir une injonction de tribunal pour contraindre l'opérateur à fermer le site. Il s'agit généralement d'actions de dernier recours dans la mesure où les délais requis pour identifier les organismes chargés de l'application de la loi, entreprendre avec eux une action coordonnée et obtenir une injonction de tribunal dans la juridiction appropriée se mesurent généralement en jours et en semaines, alors que les dénonciateurs cherchent à fermer les sites illégaux dans un délai de quelques heures.

La modification rapide des enregistrements de ressource A qui renvoient aux serveurs Web référents compromis constitue un obstacle majeur à la détection et à la mise en place de mesures pour fermer les sites d'hébergement fast-flux. Dans de nombreux cas, la durée de vie d'un site illégal hébergé sur un réseau fast-flux dépasse largement la durée de vie moyenne estimée à environ 4 jours[11].

Les améliorations apportées à cette forme d'atténuation des risques incluent :

1) l'adoption de procédures qui accélèrent la suspension d'un nom de domaine pour éliminer le problème des sites illégaux qui sont fermés mais rapidement ré-hébergés sur un serveur différent, avec un autre fournisseur d'accès Internet ;
2) une meilleure coordination et un meilleur partage des informations parmi les dénonciateurs, les organismes chargés de l'application de la loi et les CERT ; l'inclusion d'une base de données contenant des points de contact (interface multilingue), des informations sur les exigences spécifiques à la juridiction, des conventions, et d'autres informations utiles dans les opérations de suspension classiques.

Mise hors service des domaines utilisés dans l'hébergement fast-flux

Dans certains scénarios de mise hors service, les personnes chargées de dénoncer les irrégularités dans le cadre de la cybercriminalité déterminent qu'un nom de domaine est utilisé pour des attaques de type fast-flux, s'adressent au bureau d'enregistrement ou au registre dans lequel est enregistré ce nom de domaine, expliquent la nature du problème et convainquent le bureau d'enregistrement de suspendre le nom de domaine.

[11] Les statistiques mensuelles de l'APWG en décembre 2006 et août 2007 indiquent que les sites d'hameçonnage ont une durée de vie moyenne en ligne comprise entre 3,3 et 4,5 jours, voir http://www.apwg.org/phishReportsArchive.html ; toutefois cette moyenne est calculée sans faire de distinction entre les sites d'hameçonnage hébergés de manière conventionnelle et ceux qui utilisent le fast-flux. Comme les adresses IP des hôtes fast-flux changent rapidement, l'hébergement fast flux contribue à *abaisser* les chiffres.

Les registres et les bureaux d'enregistrement ne sont statutairement pas contraints de répondre d'une manière particulière aux réclamations relatives à l'hébergement, et la technique de l'hébergement fast-flux n'est pas en tant que telle une activité illégale tant qu'elle n'est pas clairement associée à une activité illégale (détournement d'ordinateurs, usurpation d'identité). Les bureaux d'enregistrement et les registres définissent leurs propres règles en matière d'utilisation illégale et mettent en œuvre de manière indépendante des procédures de réaction. Toutefois, il existe certaines pratiques communes. Les registres ont besoin de suffisamment d'informations pour établir clairement qu'un nom de domaine est utilisé illégalement ou encourage un comportement criminel, et ils conduisent en général leurs propres enquêtes. Si la propre enquête du registre corrobore les données présentées par le dénonciateur ou le plaignant, le registre peut fournir cette preuve au bureau d'enregistrement de cet enregistrement qui prendra en général rapidement les mesures appropriées pour résoudre le problème signalé. Les statuts propres du bureau d'enregistrement et les accord d'accréditation du bureau d'enregistrement (RAA, Registrar Accreditation Agreement) de l'ICANN (si ceux-ci s'appliquent pour le TLD dans lequel est enregistré le nom de domaine) déterminent la réaction du bureau d'enregistrement, qui peut être de suspendre le domaine (c'est-à-dire d'utiliser l'état HOLD pour empêcher le DNS de résoudre le nom de domaine), de suspendre le nom de domaine et de modifier l'enregistrement pour refléter que ce nom de domaine fait l'objet d'un litige ou que les règles d'enregistrement ont été enfreintes, ou de suspendre le nom de domaine et de le supprimer de la zone. Les registres réagissent en général avec une grande célérité aux demandes d'application de la loi, aux citations à comparaître et aux injonctions de tribunal. De nombreux bureaux d'enregistrement et registres comportent des services juridiques, et proposent des listes de questions/réponses et des formulaires de contact accessibles par navigateur. Les bureaux d'enregistrement et les registres peuvent fournir des listes de questions/réponses et des formulaires similaires pour faciliter et accélérer les communications avec les organismes chargés de l'application de loi et les dénonciateurs.

La modification rapide des enregistrements de ressource A qui renvoient aux serveurs de noms référents compromis par la technique fast-flux est un obstacle majeur à la détection et à la mise en place de mesures pour fermer les sites d'hébergement fast-flux.

Les méthodes d'atténuation des risques pratiquées aujourd'hui, bien que manière non uniforme, incluent :

- l’authentification des contacts avant d’autoriser toute modification des configurations de serveur de noms ;
- la mise en œuvre de mesures pour empêcher toute modification automatique (par script) des configurations de serveurs de noms ;
- la définition d'une durée de vie (TTL) minimale autorisée (par exemple, 30 minutes) suffisamment longue pour contrecarrer l'élément « double flux » de l'hébergement fast-flux ;
- la mise en œuvre ou l'expansion de systèmes de surveillance des infractions signalant les modifications de configuration DNS excessives ;

- la publication ou la mise en application d'une convention universelle d'accès aux services qui interdit à des services de domaines enregistrés ou d'hébergement (DNS, Web, messagerie) d'encourager des activités illégales ou répréhensibles (énumérées dans la convention).

Des méthodes supplémentaires de détection et d'atténuation ont été proposées, notamment :

- **Mise en quarantaine (et « honeypot ») des noms de domaine :** Selon un ensemble de critères à déterminer, obtenir du bureau d'enregistrement qu'il suspende les mises à jour de serveur de noms pour les noms de domaine suspectés d'être associés à une attaque de type fast-flux. Durant la période de suspension, observer et consigner l'intégralité de l'activité des comptes du registrant et les tentatives de modification des enregistrements. Ceci étend la fenêtre d'analyse des incidents et offre aux enquêteurs une opportunité pour remonter à l'origine des modifications et identifier les programmes robots.

- **Limitation du rythme (ou limitation en nombre par heure/jour/semaine) des mises à jour des serveurs de noms associées à un nom de domaine enregistré :** les registres et les bureaux d'enregistrement appliquent déjà des techniques de limitation de rythme sur les services WHOIS basé sur les requêtes pour éviter les utilisations illégales. Déterminer un rythme de modification (a) qui est adapté aux applications légales de durée de vie courte pour les enregistrement NS dans les fichiers de zone TLD, (b) qui fournit aux enquêteurs une fenêtre d'opportunité pour remonter à l'origine des modifications et identifier les programmes robots, et (c) qui rend les durées de vie (TTL) courtes moins utilisables par les instigateurs d'attaques de type fast-flux.

- **Séparation des modifications de durée de vie (TTL) courte du processus normal de modification des enregistrements :** Traiter les requêtes pour définir des valeurs TTL au-dessous d'une certaine limite comme des requêtes spéciales nécessitant une vérification.

- **Utilisation des domaines suspendus pour éduquer les internautes :** Ne pas renvoyer immédiatement les domaines identifiés comme utilisés à des fins illégales, mais rediriger plutôt les visiteurs vers une page de redirection expliquant que ce domaine a été suspendu parce qu'il était utilisé pour des activités illégales ou répréhensibles, et informant les internautes sur les différentes manières de détecter et d'éviter les attaques de types hameçonnage et autres.

Conclusions

Le SSAC soumet les conclusions suivantes à la discussion au sein de la communauté :

1) L'hébergement fast-flux offre une infrastructure pour le lancement d'attaques hautement sophistiquées qui exploitent de plus en plus le services de résolution et d'enregistrement des noms de domaine pour abriter des activités illégales et répréhensibles.

2) Les méthodes actuelles pour contrecarrer l'hébergement fast-flux par la détection et le démantèlement des programmes robots ne sont pas efficaces.

3) La méthode du « double flux » rend encore plus difficile la détection et entravent les mesures prises pour fermer les sites Web d'hébergement fast-flux.
4) Les modifications fréquentes des enregistrements de noms de serveur par un registrant de nom de domaine et les durées de vie (TTL) courtes dans les enregistrements A de nom de serveur dans les fichiers de zone TLD sont des signes qui peuvent être surveillés pour identifier l'utilisation potentiellement abusive de services de noms.

5) Les mesures interdisant les modifications automatiques des informations DNS et imposant des durées de vie (valeurs TTL) minimales pour les enregistrements A de serveur de noms dans les fichiers de zone TLD s'avèrent efficaces, mais ne sont pas appliquées de manière uniforme.

6) Des mesures supplémentaires ont été proposées pour combattre l'hébergement fast flux et méritent d'être étudiées plus en détail.

Recommandations

L'hébergement fast-flux est un problème grave et de plus en plus présent qui peut affecter les services de noms dans tous les TLD. Le SSAC encourage l'ICANN, les registres et les bureaux d'enregistrement à étudier les pratiques décrites dans le présent rapport consultatif, pour établir les meilleures pratiques à mettre en œuvre pour atténuer les risques de l'hébergement fast-flux, et à envisager la prise en compte de ces pratiques dans les futures conventions.