SAC 025
Avis du SSAC sur l'hébergement Fast Flux et les DNS

Un avis de l'ICANN
Sécurité et stabilité
Comité consultatif
(SSAC)
Janvier 2008

Introduction

"Fast flux" est une technique d'évasion que les cybercriminels et les mécréants de l'Internet utilisent pour échapper à l'identification et pour faire échouer les efforts des services de répression et de lutte contre la criminalité visant à localiser et à fermer les sites Web utilisés à des fins illégales. L'hébergement fast-flux favorise une grande variété d'activités cybercriminelles (fraude, usurpation d'identité, escroqueries en ligne) et est considéré comme l'une des menaces les plus graves pour les activités en ligne aujourd'hui. Une variante de l'hébergement fast-flux, "double flux", exploite les services d'enregistrement et de résolution des noms de domaine.

Cet avis décrit les aspects techniques de l'hébergement fast-flux et des réseaux de services fast-flux. Il explique comment le DNS est exploité pour favoriser les activités criminelles qui utilisent l'hébergement fast-flux, identifie les impacts de l'hébergement fast-flux et attire l'attention sur la manière dont ces attaques prolongent la durée de vie malveillante ou profitable des activités illégales menées à l'aide de ces techniques fast-flux. Il décrit les méthodes actuelles et possibles d'atténuation de l'hébergement fast-flux en divers points de l'Internet. L'avis examine les avantages et les inconvénients de ces méthodes d'atténuation, identifie les méthodes que le SSAC considère comme pratiques et judicieuses, et recommande que les organismes appropriés envisagent des politiques qui rendraient les méthodes d'atténuation pratiques universellement disponibles pour les titulaires de noms de domaine, les ISP, les bureaux d'enregistrement et les registres (le cas échéant pour chacun).

Contexte

Les professionnels de la sécurité, la communauté anti-cybercriminalité et les services de police étudient l'hébergement fast-flux depuis un certain temps. L'hébergement fast-flux fonctionne à partir d'un vaste réseau distribué de systèmes compromis qui peut très bien s'étendre sur toute la planète. Un commerce clandestin florissant loue des dizaines, voire des milliers, de systèmes compromis à des délinquants de l'Internet sous la forme de réseaux de services fast-flux1. Les opérateurs de ces réseaux de services utilisent des canaux de communication secrets (cryptés) hiérarchisés et des techniques de proxy. Ils gèrent ces réseaux avec une certaine diligence en interrogeant régulièrement l'état des systèmes compromis et en effectuant des ajouts et des suppressions sur les réseaux en fonction de la présence ou de l'absence de réponse. La communauté des noms de domaine est particulièrement préoccupée par la façon dont ces opérateurs automatisent les mises à jour des services de noms de domaine pour masquer l'emplacement des sites Web où sont menées des activités illégales - piratage IP (musique, vidéos, jeux), hébergement de pornographie enfantine, hébergement de systèmes de phishing, vente de produits pharmaceutiques illégaux et exécution d'usurpation d'identité et de fraude.

Une variante de l'hébergement fast-flux utilise des mises à jour rapides des informations DNS pour dissimuler l'emplacement d'hébergement des sites web et autres services Internet qui hébergent des activités illégales. Dans une deuxième variante, appelée "double flux", les cybercriminels complètent le réseau de services qui héberge les sites web par un deuxième réseau de services qui héberge les serveurs DNS. Le fonctionnement de ces réseaux de services est décrit en détail dans les sections suivantes du présent avis.

1. Les organismes de sécurité utilisent une variété de termes pour décrire l'hébergement de flux rapides dans leur littérature et leurs publications. Dans cet avis, nous appliquons la terminologie d'un rapport du projet Honeynets, *Know Your Enemy : Fast Flux Service Networks*, voir http://www.honeynet.org/papers/ff/

Terminologie

Pour décrire, dans la mesure du possible, cette technique complexe et multiforme de fast-flux, le SSAC commence par identifier certains des termes que la communauté de la sécurité Internet associe à l'hébergement fast-flux :

botnet. Un botnet est un réseau d'ordinateurs tiers compromis sur lesquels fonctionnent des (ro)bots logiciels. Ces robots peuvent être contrôlés à distance - dans un premier temps par l'attaquant lui-même, puis par une partie qui paie l'attaquant pour l'utilisation du réseau de robots - afin de réaliser un certain nombre d'activités non autorisées ou illégales. L'attaquant est généralement associé à un élément criminel organisé. Il installe le "logiciel bot" sans préavis ni autorisation sur un PC par le biais d'un téléchargement de logiciel espion ou d'un virus joint à un message électronique et, plus souvent, par le biais d'un navigateur ou d'autres exploits côté client (par exemple, des bannières publicitaires compromises). Une fois que le bot est en mesure de s'exécuter, il établit un canal de retour vers une infrastructure de contrôle mise en place par l'attaquant. Les botnets traditionnels sont conçus selon un modèle centralisé, et tous les canaux de retour sont reliés au centre de commande et de contrôle (C&C) de l'attaquant. Récemment, les opérateurs de botnets ont utilisé des modèles peer-to-peer pour le fonctionnement du canal arrière afin de déjouer la détection du C&C par l'analyse du trafic.

bot-herder. L'architecte et l'auteur de l'attaque distribuée qui est utilisée pour créer, maintenir et exploiter un botnet pour un gain financier ou autre (politique). Une fois le botnet établi, le bot-herder loue l'utilisation de son botnet à un **opérateur de services Fast Flux.**

Fast flux. Cette expression est utilisée pour représenter la capacité à déplacer rapidement l'emplacement d'un service web, de messagerie, DNS ou généralement tout service Internet ou distribué d'un ou plusieurs ordinateurs connectés à Internet vers un autre ensemble d'ordinateurs afin de retarder ou d'échapper à la détection.

Installations de Fast Flux. Dans cet article, le terme "*installation" fait référence* à un agent logiciel qui a été installé sans consentement sur un grand nombre d'ordinateurs à travers l'Internet.

Réseau de services Fast Flux. Dans ce document, un réseau de services fait référence à un sous-ensemble de bots que le bot-herder assigne à un opérateur de services Fast Flux donné qui, à son tour, fournit à son client des installations pour l'hébergement de fast-flux ou le service de noms. Notez que ce réseau de services est souvent géré 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 variations sont probables, et les attaquants peuvent modifier l'hébergement fast-flux futur pour échapper aux méthodes de détection de l'hébergement fast-flux tel qu'il est décrit ici, ou ajouter des couches supplémentaires de hiérarchie ou d'abstraction.

Bien qu'une attention considérable soit accordée aux aspects techniques du fast-flux, il existe un ensemble associé d'activités "commerciales" qui mérite également d'être décrit. Nous considérons le cas où un mécréant veut mener une attaque de phishing.

Les aspects commerciaux de l'hébergement de flux rapides commencent avec les auteurs de logiciels malveillants. Certains auteurs de logiciels malveillants développent des kits d'hameçonnage, des logiciels qui peuvent être personnalisés pour envoyer des courriers électroniques d'hameçonnage à une liste de destinataires et héberger le site web illégal associé où le courrier électronique d'hameçonnage envoie les victimes. D'autres collectent des adresses électroniques et vendent des listes pour le spam. D'autres encore développent des logiciels zombies. Le logiciel bot est un agent flexible et contrôlable à distance qui peut être chargé d'exécuter des fonctions arbitraires pour le compte d'un logiciel de **centre de commande et de contrôle** (C&C) correspondant : une fois installé secrètement sur un système compromis, le logiciel bot facilite les téléchargements ultérieurs et l'exécution à distance de logiciels supplémentaires spécifiques à l'attaque. Les organisateurs de bots utilisent souvent des vers transmis par courrier électronique pour infecter et compromettre des milliers de systèmes, bien que les compromissions côté client, telles que les exploits basés sur les navigateurs, soient les plus importantes aujourd'hui.

Les auteurs de logiciels malveillants et les bot-herders sont des *fournisseurs de biens* dans la communauté cybercriminelle. Les fournisseurs de biens utilisent des canaux Internet Relay Chat (iRC) cryptés et privés/sécurisés ou des lieux de rencontre souterrains similaires pour faire de la publicité et trouver des acheteurs pour leurs biens criminels2 . Les biens criminels d'un bot-herder sont essentiellement les installations qu'il peut mettre à disposition contre paiement ou location. L'éleveur loue le commandement et le contrôle d'un nombre négocié de systèmes compromis à un client, qui peut les utiliser directement ou les gérer pour le compte d'un autre mécréant ; dans ce dernier cas, le client de l'éleveur de robots sert de fournisseur de services d'hébergement de flux rapides. Dans cette économie complexe et secrète, une partie désireuse de mener des activités criminelles peut négocier avec plusieurs parties pour obtenir une liste de spam (phish), déployer un système de phishing ou un autre kit d'attaque, ainsi qu'un botnet et mener elle-même l'attaque, ou bien elle peut négocier avec une seule partie, un opérateur de réseau de services fast-flux, pour diriger l'attaque de phishing en son nom.

Dans l'hébergement de flux rapide, les réseaux de service de flux rapide sont utilisés à deux fins :

- **Pour héberger des sites web de référence**. Les bots de ce réseau de services n'hébergent généralement pas le contenu du client fast-flux mais redirigent le trafic web vers le serveur web où 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 appliqué.
- **Pour héberger des serveurs de noms**. Les bots de ce réseau de services exécutent des serveurs de noms de référence pour le client fast-flux. Ces serveurs de noms transmettent les demandes DNS à des serveurs de noms cachés qui hébergent des zones contenant des enregistrements de ressources DNS A pour un ensemble de sites Web de référence. Les serveurs de noms cachés ne retransmettent pas les réponses par le biais du serveur de noms référent, mais répondent directement à l'hôte demandeur. Lorsque ce deuxième réseau est exploité en conjonction avec (1) pour renforcer la tromperie, on parle de *double flux*.

Voir "Activité de marché" telle que décrite dans *Une enquête sur la nature et les causes de la richesse des mécréants de l'Internet, voir* http://www.cs.cmu.edu/~jfrankli/acmccs07/ccs07_franklin_eCrime.pdf.

La figure 1 illustre ces relations.

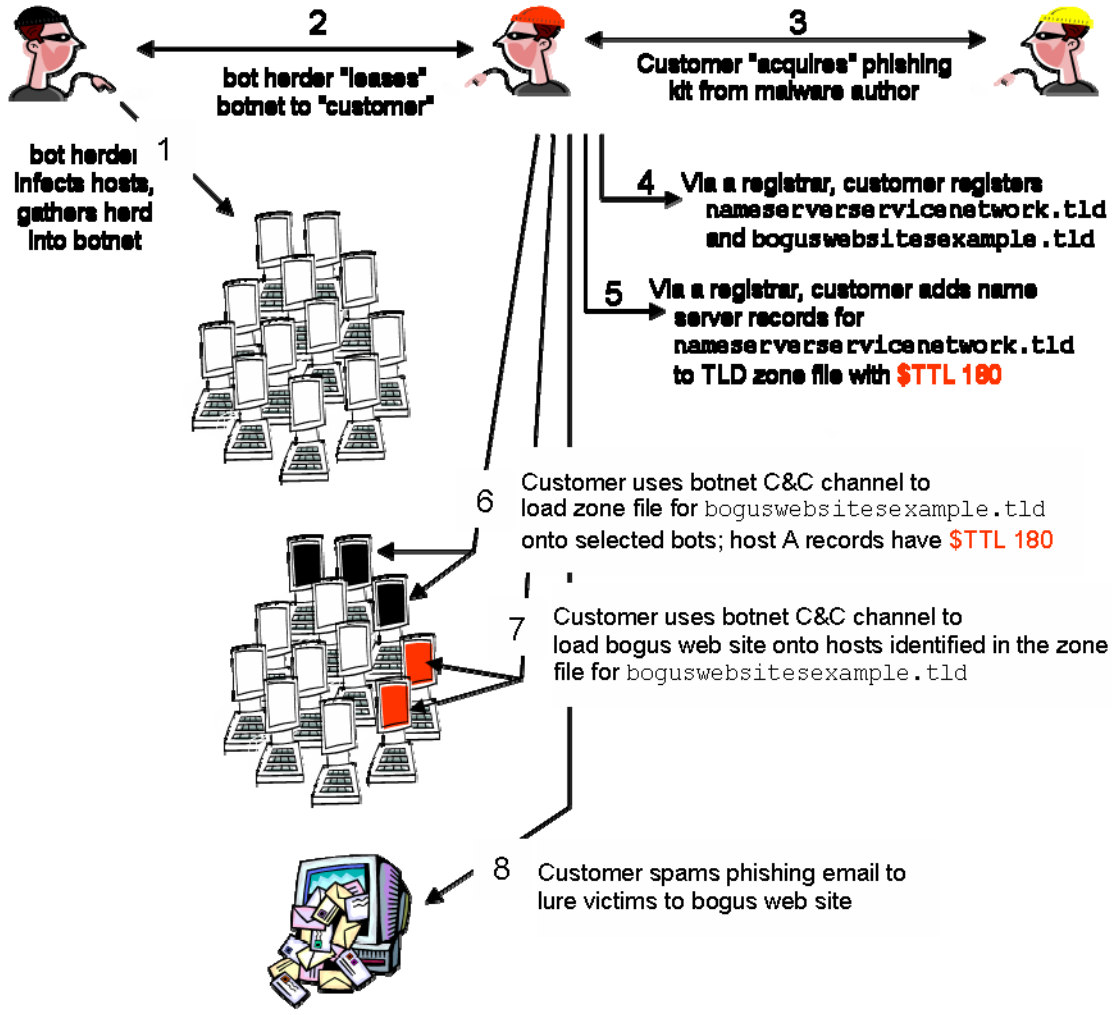

Figure 1. Éléments d'une attaque par hébergement "double flux

Exploitation du service de nom : Hébergement Double Flux

Les clients de Fast Flux enregistrent souvent des noms de domaine pour leurs activités illégales à un prix élevé. un registraire ou un revendeur accrédité. Dans une forme d'attaque, le client à flux rapide enregistre une nom de domaine (pour un réseau de service de flux) pour héberger des sites web illégaux (`boguswebsitesexample.tld`) et un (deuxième ou plusieurs) nom(s) de domaine pour un flux pour fournir 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.
L'opérateur du réseau de services de flux rapide utilise des techniques automatisées pour changer rapidement de nom.

les informations relatives au serveur dans les registres d'enregistrement tenus par le registraire de ces domaines ; en particulier, l'opérateur du réseau de services de flux rapide

- modifie les adresses IP des serveurs de noms du domaine pour qu'elles pointent vers différents hôtes du domaine `nameserverservicenetwork.tld` et
- fixe les temps de vie (TTL) dans les enregistrements d'adresses pour ces serveurs de noms à une valeur très faible (1-3 minutes est courant).

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 sous la forme suivante :

```
TTL 180
boguswebsitesexample.tld.      NSNS1    .nameserverservicenetwork.tld
boguswebsitesexample.tld.      NSNS2    .nameserverservicenetwork.tld
…
NS1.nameserverservicenetwork.tld.   A10.0.0.1
NS2.nameserverservicenetwork.tld.   A10.0.0.2
```

Notez que la durée de vie (TTL) des enregistrements de ressources est fixée à un niveau très bas (dans l'exemple, 180 secondes). Lorsque le TTL expire, l'automatisation de l'opérateur du réseau de services de flux rapide garantit qu'un nouvel ensemble d'enregistrements A pour les serveurs de noms remplace l'ensemble existant :

```
TTL 180
boguswebsitesexample.tld.      NSNS1    .nameserverservicenetwork.tld
boguswebsitesexample.tld.      NSNS2    .nameserverservicenetwork.tld
…
NS1.nameserverservicenetwork.tld. A 192.168.0.123
NS2.nameserverservicenetwork.tld. A 10.10.10.233
```

La fenêtre d'opportunité pour identifier et arrêter les serveurs de noms qui supportent cette attaque à flux rapide est donc très réduite.

Les enregistrements de ressources dans `nameserverservicenetwork.tld` pointent vers des hôtes proxy ou référents plutôt que vers les robots qui assurent la résolution de noms pour `boguswebsitesexample.tld`. Les hôtes référents écoutent le port 53 et transmettent les requêtes DNS à un robot "DNS" qui héberge un fichier de zone pour `boguswebsitesexample.tld`. Le robot "DNS" résout le nom de domaine du site Web frauduleux en l'adresse IP d'un hôte du réseau de services de flux Web et renvoie le message de réponse directement au résolveur demandeur. À ce stade, l'adresse IP du bot DNS n'est connue que d'un groupe potentiellement important d'hôtes référents, et les adresses IP des référents changent toutes les 180 secondes.

Référencement Web Flux Hébergement

Dans la section précédente, nous avons décrit comment l'hébergement double flux ajoute un niveau d'évasion en employant des bots dans le réseau `nameservicenetwork.tld` et en changeant rapidement les enregistrements A des serveurs web de référence dans le réseau `boguswebsitesexample.tld`. Les enregistrements de ressources A des serveurs web de référence sont également configurés avec des TTL courts. Lorsque les TTL des serveurs web hôtes expirent, l'automatisation de l'opérateur du réseau de services de fast-flux garantit à nouveau qu'un nouvel ensemble d'enregistrements A pour les serveurs web

remplace l'ensemble existant. Ainsi, la fenêtre d'opportunité pour identifier et fermer les serveurs web de référence qui supportent cette attaque à flux rapide est très réduite.

Les enregistrements associés au site web illégal pourraient apparaître dans un fichier de zone hébergé sur un bot DNS du réseau `nameservicenetwork.tld` comme :

```
                              DAN
boguswebsitesexample.tld.     180  S      A      192.168.0.1
                              DAN
boguswebsitesexample.tld.     180  S      A      172.16.0.99
                              DAN
boguswebsitesexample.tld.     180  S      A      10.0.10.200
                              DAN
boguswebsitesexample.tld.     180  S      A      192.168.140.11
```

Notez à nouveau que la durée de vie (TTL) de chaque enregistrement de ressource A est très faible (dans l'exemple, 180 secondes). Lorsque le TTL expire, les enregistrements de ressources sont automatiquement modifiés pour pointer vers d'autres bots qui hébergent ce site Web illégal. Quelques minutes plus tard, le fichier de zone pourrait être le suivant :

```
                              DAN
boguswebsitesexample.tld.     180  S      A      192.168.168.14
                              DAN
boguswebsitesexample.tld.     180  S      A      172.17.0.199
                              DAN
boguswebsitesexample.tld.     180  S      A      10.10.10.2
                              DAN
boguswebsitesexample.tld.     180  S      A      192.168.0.111
```

Hébergement Fast Flux : Lié à la dégustation de noms de domaine ?

Pour certains, la dégustation de noms de domaine et le phishing sont des activités liées3. Le groupe de travail anti-hameçonnage (APWG) a publié un rapport sur la relation entre les noms de domaine goûtés et les attaques de phishing. Le rapport résume les résultats de deux études qui ont cherché à déterminer si les parties qui goûtent aux noms de domaine utilisent également ces noms pour faciliter les attaques de phishing. Un membre de l'APWG a commencé avec un ensemble de noms de domaine qui avaient été utilisés dans des attaques de phishing et a essayé de déterminer si ces noms avaient été annulés pendant la période de grâce d'ajout. Un deuxième membre de l'APWG a comparé les noms de domaine utilisés dans les attaques de phishing à une liste d'environ trois millions de noms de domaine qui ont été goûtés pendant une période d'une semaine. Les résultats de ces deux études indiquent qu'"il y a très peu de cas de dégustation de noms de domaine par des hameçonneurs et que les cas qui existent ont des explications possibles qui ne sont pas liées à la dégustation "[4].

Les attaques de phishing utilisent de plus en plus l'hébergement fast-flux (en particulier les attaques contre les grandes institutions financières) ; le SSAC conclut donc qu'il n'y a pas de relation significative entre la dégustation de noms de domaine et l'hébergement fast-flux. Le SSAC observe également que les objectifs de l'hébergement fast-flux et de la dégustation de noms de domaine ne sont pas identiques. 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 dont la rentabilité est historiquement prouvée, notamment le vol d'informations financières et de cartes de crédit. Les cartes de crédit volées sont utilisées pour payer les frais d'enregistrement des noms de domaine des sites d'hameçonnage

1. Voir CADNA Background, http://www.cadna.org/en/index.html
2. APWG : La relation entre le phishing et les noms de domaine, http:// www.antiphishing.org/reports/DNSPWG_ReportDomainTastingandPhishing.pdf

il n'y a aucune incitation à enregistrer un nom et à s'en défaire. En comparaison, les goûteurs de domaines ne sont intéressés que par le paiement de frais d'enregistrement pour des noms de domaine qui s'avéreront rentables dans une fenêtre d'essai de quelques jours.

Solutions d'atténuation actuelles et possibles

Plusieurs solutions d'atténuation peuvent être mises en œuvre pour réduire la menace que représente l'hébergement de flux rapides.

Fermez les bots qui hébergent les installations de fast-flux.

Les bot-herders compromettent les ordinateurs des réseaux professionnels et résidentiels. Cependant, un bot-herder exploite généralement des ordinateurs mal sécurisés connectés à des circuits d'accès à large bande résidentiels (modem câble et DSL), car la probabilité de trouver un hôte exploitable y est plus grande que sur les réseaux gérés par un personnel informatique expérimenté. Les hôtes des établissements d'enseignement, des administrations ou des entreprises sont vulnérables à la compromission des systèmes, mais ils sont, en moyenne, moins susceptibles d'être compromis et les tentatives d'exploitation risquent davantage d'être détectées par les administrateurs réseau.

Les méthodes d'atténuation disponibles aujourd'hui et pouvant être largement mises en œuvre pour réduire le nombre de PC susceptibles d'être exploités et utilisés pour héberger des logiciels zombies incluent (mais ne sont certainement pas limitées à) :

5 Amélioration des mesures de sécurité des postes de travail (antivirus, antispyware, logiciel pare-feu personnel, logiciel de détection des intrusions sur l'hôte) sur les hôtes des réseaux privés et publics (c'est-à-dire le service d'accès résidentiel à large bande).

6 Déploiement de passerelles anti-malware par les FAI pour les clients résidentiels d'accès à large bande ; par les fournisseurs de services de sécurité gérés ou les administrateurs de sécurité interne pour les réseaux d'entreprise et adoption accrue de passerelles anti-malware par les administrateurs de sécurité des réseaux privés.

7 L'éducation, la sensibilisation et la formation, avec un accent particulier sur la compréhension et l'application de politiques rigoureuses en matière de trafic de sortie.

Les autres méthodes d'atténuation à envisager sont les suivantes :

- Liste blanche des processus et des exécutables.
- Contrôles d'accès/admission au réseau.
- Analyse des comportements connus des botnets, développement d'une technique de détection (par exemple, une signature) qui peut être utilisée pour bloquer l'activité au niveau d'une passerelle de sécurité de "gestion des menaces". Il s'agit d'une extension logique du point b) ci-dessus).

Bien qu'elles semblent les plus pratiques, les méthodes (a) et (b) ne se sont pas avérées efficaces pour atténuer la menace des logiciels malveillants. Storm5 et les logiciels malveillants de conception similaire peuvent être modifiés et distribués périodiquement par leurs créateurs à l'aide de robots6 non encore détectés et de systèmes de signatures.

▪ Attaque DDoS de Storm Worm, http://www.secureworks.com/research/threats/view.html?threat=storm-worm

▪ *Imperfect Storm aide les spammeurs,* http://www.securityfocus.com/news/11442

Les mesures de lutte contre les logiciels malveillants basées sur les technologies de l'information n'ont pas été efficaces pour éradiquer les logiciels malveillants tels que le programme trojan Storm7. Les PC que ces logiciels malveillants infectent agrandissent le troupeau plus rapidement que la communauté ne peut identifier et désinfecter les PC compromis. L'éducation et la sensibilisation (c) est un processus douloureusement lent. Selon l'enquête CSI/FBI sur la criminalité et la sécurité informatiques, 97 % des PC sont équipés d'un logiciel antivirus et 79 % d'un logiciel antispyware, mais le nombre d'infections par des robots est alarmant : en juin 2007, le FBI a annoncé que son initiative de lutte contre la cybercriminalité visant à combattre les réseaux de robots avait permis d'identifier plus d'un million de PC compromis par des logiciels de robots, rien que dans la juridiction américaine du FBI8. Ces chiffres s'appliquent aux réseaux d'entreprises/de commerces. Chez les utilisateurs résidentiels de la large bande, l'utilisation de logiciels antivirus et antispyware n'est pas aussi répandue, les configurations de sécurité et de réseau sont plus souvent négligées et les abonnements aux mises à jour des définitions de logiciels malveillants sont souvent laissés en suspens.

La liste blanche des processus et des exécutables est une technique de prévention des logiciels malveillants qui applique une politique en matière d'exécutables ; plus précisément, l'exécution de toutes les applications et des processus connexes, à l'exception d'un ensemble de confiance, sera empêchée sur un PC. La mise en œuvre de la liste blanche des exécutables n'est pas très répandue, en particulier parmi les utilisateurs de l'internet grand public/résidentiel.

Aujourd'hui, des solutions de contrôle d'accès/admission au réseau sont développées dans le but d'empêcher les points d'extrémité non sécurisés de se connecter aux LAN et WLANS. Une évaluation de la sécurité est effectuée sur un ordinateur afin de déterminer s'il est exempt d'exécutables malveillants avant de l'autoriser à se connecter à Internet. Si l'ordinateur est compromis, il est mis en quarantaine et ne peut pas se reconnecter tant que la violation de la sécurité n'est pas corrigée pour le haut débit résidentiel (e) n'est pas largement mis en œuvre et nécessiterait des normes et un développement logiciel supplémentaires. Les FAI et les fournisseurs d'accès à large bande résidentiels indiquent qu'ils ne peuvent pas supporter le coût de la mise en œuvre et de la gestion de l'accès au réseau et du filtrage du trafic entrant.

Fermez les hôtes à flux rapide

Un nombre considérable d'hôtes compromis utilisés dans ces attaques sont des PC connectés à des services résidentiels à large bande. Ces PC hébergent généralement des logiciels de référencement web et de serveur de noms.

La détection, l'isolement et la réponse aux incidents sont les procédures d'atténuation les plus courantes pratiquées aujourd'hui. Tout d'abord, un système est identifié ou signalé comme hébergeant des activités illégales. Dans le scénario d'hébergement de fast-flux, il peut s'agir d'un serveur web ou de nom de référence ou du système qui héberge le site web illégal. Les intervenants en matière de lutte contre la criminalité recueillent des informations sur le site : emplacement et juridiction du système d'hébergement, propriétaire du domaine, administrateur du site et fournisseur de services Internet, et type d'activité illégale. Les intervenants utilisent les services WHOIS et d'autres moyens pour

[7] Common Malware Enumeration CME-711trojan downloader. http://cme.mitre.org/data/list.html

[8] *Plus d'un million de victimes potentielles de la cybercriminalité par botnet,* http://www.fbi.gov/page2/june07/botnet061307.htm

identifier et contacter plusieurs parties - en parallèle et à plusieurs reprises - jusqu'à ce qu'elles reçoivent de l'aide pour mettre fin à l'activité illégale9 :

- Dans les cas où des activités illégales semblent être hébergées sur un système compromis (par exemple, sur un serveur web qui mène des activités légitimes et dont l'administrateur ne sait pas que le serveur héberge également un site illégal), le propriétaire du domaine est contacté pour aider à la fermeture.
- Le fournisseur d'accès Internet ou le fournisseur d'hébergement est contacté pour demander l'interruption du service à l'hôte.
- Dans les cas où les intervenants ont besoin d'une assistance locale (interprétation linguistique, confirmation que les intervenants sont de bonne foi, ou aide pour obtenir des informations supplémentaires), les équipes locales d'intervention en cas d'urgence ou d'incident informatique (CERT/CIRT) sont contactées. (Dans certains pays, les CERT encouragent les intervenants à les contacter le plus tôt possible dans le processus).
- Dans les cas où des bots sur des PC hébergent des serveurs de noms, les bureaux d'enregistrement ou les registres sont contactés pour supprimer les enregistrements NS des fichiers de zone TLD ou suspendre les domaines.

Les sites illégaux eux-mêmes peuvent fonctionner à partir de serveurs compromis dans des domaines légitimes, de fournisseurs de sites Web d'hébergement partagé ou d'installations d'hébergement Web "à l'épreuve des balles" (quasi) légitimes10. En cas d'absence de coopération - lorsque les opérateurs et les autorités locales ne reconnaissent pas les intervenants, ne leur font pas confiance ou ne sont pas disposés à agir sur la base des informations fournies par les intervenants et les CERT - les intervenants peuvent demander l'aide d'agents chargés de l'application de la loi (LEA) ou demander une ordonnance du tribunal pour contraindre l'opérateur à retirer le site. Il s'agit généralement d'actions de dernier recours, car les délais nécessaires pour identifier et coordonner les LEA et obtenir une action en justice dans la juridiction appropriée sont souvent de plusieurs jours ou semaines, et les intervenants cherchent à démanteler les sites illégaux en quelques heures.

La modification rapide des enregistrements de ressources A qui mènent aux serveurs web de référence ayant fait l'objet d'un flux déjoue la détection et entrave les mesures visant à fermer les sites d'hébergement fast-flux. Dans de nombreux cas, la durée de vie d'un site illégal hébergé en fast-flux se prolonge bien au-delà de la moyenne d'environ 4 jours11.

Les améliorations apportées à cette forme d'atténuation sont les suivantes :

[9] Ce scénario, relaté par une correspondance personnelle avec des intervenants, est représentatif des méthodes utilisées pour répondre aux attaques de phishing où l'hébergement de flux rapides est utilisé de manière agressive.

[10] L'hébergement à l'épreuve des balles fait référence aux fournisseurs d'hébergement de sites Web et de courriers électroniques groupés qui imposent peu ou pas de conditions de service régissant le contenu et les activités hébergés sur leurs serveurs. Le terme "bulletproof" est utilisé pour souligner que les services hébergés chez ces fournisseurs ne seront pas supprimés. De nombreux fournisseurs d'hébergement "bulletproof" n'agissent pas en parfaite bonne foi avec les organismes chargés de l'application de la loi et de la lutte contre la criminalité, et ils opèrent dans des juridictions où les autorités locales et les lois sur l'Internet offrent un refuge relativement sûr pour les activités illégales.

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

1) Adopter des procédures qui accélèrent la suspension d'un nom de domaine, afin d'éliminer le problème des sites illégaux qui sont fermés mais qui sont rapidement ré-hébergés sur un autre serveur, chez un autre fournisseur d'accès.
2) Une meilleure coordination et un meilleur partage des informations entre les intervenants, les LEA et les CERT. Inclure une (des) base(s) de données contenant les points de contact (langues parlées), des informations sur les exigences juridictionnelles, les conventions et d'autres informations utiles dans les activités typiques de suspension.

Retirer du service les domaines utilisés dans l'hébergement fast-flux

Dans certains scénarios de mise hors service, les intervenants de la lutte contre la criminalité déterminent qu'un nom de domaine est utilisé pour des attaques de type "fast-flux", se rendent au bureau d'enregistrement ou au registre où le nom de domaine est enregistré, expliquent la nature du problème et convainquent le bureau d'enregistrement de mettre le nom de domaine hors service.

Les registres et les bureaux d'enregistrement ne sont pas tenus par une politique de répondre d'une manière particulière aux plaintes concernant l'hébergement fast-flux et la technique d'hébergement fast-flux en soi ne constitue pas une activité illégale tant qu'elle n'est pas clairement associée à une activité illégale (abus et fraude informatiques, vol d'identité). Les registres et bureaux d'enregistrement définissent leurs propres politiques en matière d'abus et mettent en œuvre des procédures de réponse de manière indépendante. Cependant, certaines pratiques communes existent. Les registres exigeront des informations suffisantes pour démontrer clairement que le nom de domaine fait l'objet d'un abus ou qu'il encourage un comportement criminel et mèneront généralement leurs propres enquêtes. Si la propre enquête du registre corrobore les données présentées par le répondant ou le plaignant, le registre peut transmettre ces preuves au bureau d'enregistrement qui agira généralement rapidement pour résoudre le problème signalé. La politique du bureau d'enregistrement et le RAA de l'ICANN (s'il est applicable au TLD dans lequel le nom de domaine est enregistré) influent sur la réponse du bureau d'enregistrement, qui peut être de suspendre le domaine (c'est-à-dire d'utiliser le statut HOLD pour empêcher le DNS de résoudre le nom) ; de suspendre le nom de domaine et de modifier l'enregistrement pour indiquer que le nom de domaine est un litige ou que la politique d'enregistrement a été abusée ; ou de suspendre le nom de domaine et de le supprimer de la zone. Les registres répondent généralement aux demandes des forces de l'ordre, aux citations à comparaître et aux ordonnances des tribunaux dans les plus brefs délais. De nombreux registres et bureaux d'enregistrement disposent de départements généraux chargés des abus, et les FAQ et les formulaires de contact sont souvent accessibles par navigateur. Les registres et les bureaux d'enregistrement pourraient fournir des FAQ et des formulaires similaires pour faciliter et accélérer la communication avec la LEA et les intervenants de la lutte contre la criminalité.

Les méthodes d'atténuation qui sont pratiquées aujourd'hui, mais pas de manière uniforme, comprennent :

- Authentifier les contacts avant d'autoriser les modifications des configurations des serveurs de noms.
- Mettre en place des mesures pour empêcher les changements automatisés (scriptés) des configurations des serveurs de noms.
- Fixez un TTL minimum autorisé (par exemple, 30 minutes) suffisamment long pour contrecarrer l'élément de double flux de l'hébergement à flux rapide.

- Mettre en œuvre ou étendre les systèmes de surveillance des abus pour signaler les modifications excessives de la configuration du DNS.
- Publier et faire respecter un accord universel sur les conditions de service qui interdit l'utilisation d'un domaine enregistré et des services d'hébergement (DNS, web, courrier) pour favoriser des activités illégales ou répréhensibles (telles qu'énumérées dans l'accord).

D'autres moyens de détection et d'atténuation ont été suggérés. Il s'agit notamment de :

- **Mettez les noms de domaine en quarantaine (et en pots de miel).** Sur la base d'un ensemble de critères à déterminer, demandez au bureau d'enregistrement de suspendre les mises à jour du serveur de noms pour les noms de domaine suspectés d'être liés à une attaque à flux rapide. Pendant la période de suspension, observez et enregistrez toute l'activité du compte du titulaire et les tentatives de mise à jour. Cela élargit la fenêtre d'analyse de l'incident et donne aux enquêteurs la possibilité de retrouver l'origine des mises à jour et d'identifier les bots.

- **Limiter le taux ou (limiter par nombre par heure/jour/semaine) les changements de serveurs de noms associés à un nom de domaine enregistré**. Les registres et les bureaux d'enregistrement appliquent déjà des techniques de limitation du taux sur les services WHOIS basés sur les requêtes afin de décourager les abus. Déterminer un taux de changement qui (a) tient compte des applications légitimes de TTL courts pour les enregistrements NS dans les fichiers de zone TLD, (b) offre aux enquêteurs une fenêtre d'opportunité pour retracer l'origine des mises à jour et identifier les bots, et (c) permet d'éviter les abus.
  (c) rend les TTL courts moins utiles aux attaquants à flux rapide.

- **Séparer les "mises à jour des TTL courts" du traitement normal des changements d'enregistrement.** Traitez les demandes visant à fixer des TTL inférieurs à une certaine limite comme des demandes spéciales nécessitant une certaine forme de vérification.

- **Utilisez les domaines suspendus pour éduquer les consommateurs.** Ne renvoyez pas immédiatement les domaines dont il est prouvé qu'ils sont utilisés à des fins illégales ; établissez plutôt et redirigez les visiteurs vers une page de renvoi expliquant que ce domaine a été suspendu parce qu'il était utilisé pour des activités illégales ou répréhensibles, et informez les utilisateurs sur les moyens de détecter et d'éviter d'être victimes de phishing et d'autres activités criminelles.

Constatations

Le SSAC soumet les conclusions suivantes à l'attention de la communauté :

1) L'hébergement fast-flux permet la mise en place d'une infrastructure de lancement d'attaques très sophistiquée qui exploite de plus en plus les services de résolution et d'enregistrement des noms de domaine pour favoriser des activités illégales et répréhensibles.

2) Les méthodes actuelles visant à contrecarrer l'hébergement de flux rapides en détectant et en démantelant les botnets ne sont pas efficaces.

3) Le double flux permet de déjouer la détection et d'entraver les mesures visant à fermer les sites web hébergeant le fast-flux.

4) Les modifications fréquentes des enregistrements du serveur de noms (NS) par le titulaire d'un nom de domaine et les TTL courts dans les enregistrements A du serveur de noms dans les fichiers de zone TLD sont des signatures qui peuvent être surveillées pour identifier les abus potentiels des services de noms.

5) Les mesures qui empêchent les modifications automatisées des informations DNS et qui fixent des TTL minimaux plus longs pour les enregistrements A des serveurs de noms dans les fichiers de zone TLD semblent être efficaces mais ne sont pas appliquées uniformément.

6) Des mesures supplémentaires ont été suggérées pour lutter contre l'hébergement des flux rapides et méritent d'être étudiées plus avant.

Recommandations

L'hébergement fast-flux est un problème sérieux et croissant qui peut affecter les services de noms dans tous les TLD. Le SSAC encourage l'ICANN, les registres et les bureaux d'enregistrement à prendre en considération les pratiques mentionnées dans le présent avis, à établir les meilleures pratiques pour atténuer l'hébergement fast-flux et à examiner si de telles pratiques doivent être abordées dans les futurs accords.