

• Editorial par R. Longeon

• Les botnets
par F. Ducrot, M. Danho,
X. Marronnier• Évolution de la propagation
des malwares
par L. Butti

SÉCURITÉ INFORMATIQUE

numéro 61

Octobre 2007

SÉCURITÉ DES SYSTÈMES D'INFORMATION

éditorial

« Ils ne mouraient pas tous, mais tous étaient frappés... »

Quel est donc ce nouveau fléau dont il est tant question dans les salons spécialisés? Des ectoplasmes, venus tout droit des Carpates, chasseraient sur le net les PC mal administrés. Des pièces jointes explosives, au « pair à pair » manipulé, en passant par des liens piégés, tout ne serait qu'astuces pour attirer les badauds « au club des zombies ». Une fois mordue par « la bête », une machine se transformerait en esclave du « botherder ». Pis, elle rentrerait elle-même dans « la bête »... Elle deviendrait « la bête », cherchant à mordre à son tour tout PC à sa portée! Un tiers des ordinateurs familiaux connectés à l'ADSL seraient frappés, lit-on dans la presse.

Cette histoire, racontée ainsi, est évidemment romancée, mais elle est vraie dans le fond sinon dans sa forme. Cette nouvelle malveillance, apparue en 2002 avec Agobot, se nomme botnet. Elle marque une évolution majeure de la délinquance informatique. Hier, les virus, les vers, les chevaux de Troie étaient plutôt... bêtement démonstratifs (tous ceux qui en ont été victimes en témoignent). Aujourd'hui, au contraire, les botnets sont discrets et même sournois; ils enrôlent les machines furtivement pour lancer des « spams », pour capter des mots de passe frappés au clavier, pour lancer des attaques en « déni de service distribué », pour constituer des grilles de calcul en vue du passage de messages chiffrés, et même pour louer sur Internet leurs services de « tueur de serveurs à gages ».

Quelle est l'importance de cette malveillance dans le secteur d'activité « enseignement/recherche »? François Ducrot, Michelle Danho et Xavier Marronnier du Cert-Renater, de par leur fonction, sont les mieux placés pour répondre à cette question. C'est ce qu'ils font dans ce numéro, après avoir expliqué le fonctionnement et l'exploitation des botnets et donné quelques bons conseils pour s'en protéger. Laurent Butti, expert senior en sécurité des réseaux à France Télécom R&D, complète la présentation par un article donnant une vision stratégique de l'évolution de ce type de menace.

Que nous disent-ils en essence? Que ce phénomène n'en est qu'à ses débuts et que le pire est peut-être devant nous...

Robert LongeonChargé de mission à la sécurité
des systèmes d'information du CNRS

Les botnets

François Ducrot, Michelle Danho,
Xavier Marronnier

Cert-Renater

Le terme de botnet est revenu souvent dans l'actualité de la sécurité informatique depuis quelques années. Dans cet article, nous allons exposer ce qu'il recouvre. Nous commencerons par raconter l'origine et le développement des botnets puis, en passant du point de vue de l'administrateur d'un réseau, nous expliquerons ce que signifie héberger une partie d'un botnet.

L'origine des botnets

Le terme botnet est la contraction de l'expression « roBOT NETwork », soit littéralement réseau de robots. Un robot étant un programme localisé sur une machine distante effectuant des actions automatiques sur un serveur.

Les premiers robots ont vu le jour dans le monde des opérateurs IRC. Ils servaient à assurer la permanence de la gestion d'un canal lorsque l'administrateur devait s'absenter. La dérive fut d'utiliser ces outils d'administration afin de prendre l'avantage lors d'affrontements pour le contrôle d'un canal IRC. Le plus connu de ces outils est Eggdrop, apparu en 1993 et retrouvé dans de nombreuses compromissions de systèmes Linux autour des années 2000.

En 1999, le premier ver utilisant IRC comme moyen de contrôle fit son apparition. Il s'agissait de W32, PrettyPark. Ce ver ne déclencha pas d'effet de mode immédiat. À la fin de l'année 2000, le « bot » GTBot, un détournement du client IRC Windows mIRC, fit son apparition. Ces robots de première génération n'apparurent pas comme une menace majeure et sont aujourd'hui pratiquement oubliés. Ce fut à partir de 2002 que la menace commença à prendre sa forme actuelle. Les programmes Agobot, SDBot puis, l'année suivante, SpyBot sont les briques de base sur lesquelles se sont appuyés par la suite les créateurs de botnets. Ces programmes sont construits de façon à faciliter l'émergence de nouvelles variantes en multipliant les moyens d'intrusion, les fonctionnalités offensives et les moyens de protection.

Architecture d'un botnet

Un botnet est donc un ensemble de machines esclaves, organisées en réseau et contrôlées à distance par une ou plusieurs personnes, *a priori* malveillantes.

Du point de vue de l'organisation, un botnet a pour objectif de permettre à un individu, le « botherder », le [suite page 2](#) ➔

créateur du botnet, de contrôler simultanément l'ensemble des machines esclaves (ou zombies) faisant partie de son réseau. Le botnet est un réseau fortement hiérarchisé comprenant un opérateur et des utilisateurs, des serveurs maîtres et des machines esclaves. L'opérateur est la personne qui a créé le botnet et qui en contrôle l'emploi. Les utilisateurs sont les personnes ayant payé l'opérateur pour utiliser les ressources du botnet.

L'architecture traditionnelle

Dans ce modèle, un ou plusieurs serveurs IRC sont utilisés comme canal de commande et contrôle (C&C). Après infection, les machines clientes du botnet, les bots ou zombies, se connectent au serveur maître sur un canal IRC privé afin de signaler leur existence, d'obtenir des mises à jour ou des instructions. Le «botherder» pourra les contrôler en se connectant sur un des serveurs maîtres pour envoyer ses ordres. Le point faible de ce modèle d'organisation est sa sensibilité à la détection. En effet, une fois les maîtres identifiés, il suffit de surveiller et de filtrer ceux-ci pour démanteler le botnet ou le rendre inopérant sur un segment de réseau.

Le modèle «Peer-to-Peer»

Ici, le réseau est fortement décentralisé de façon à éviter sa destruction par un simple filtrage. Il n'y a plus de serveur C&C central. Chaque machine infectée dispose d'une liste initiale d'adresses IP de points d'entrée dans le botnet. Une fois le «bot» intégré au réseau, cette liste est mise à jour de façon dynamique. On se sert des zombies pour relayer les ordres à travers l'ensemble du réseau. Les ordres mettent plus de temps à se propager dans ce contexte, mais le réseau est plus robuste : la perte d'un nœud ne met pas à mal l'existence du réseau tout entier.

Variation sur ces modèles

De nouvelles méthodes de communication apparaissent. Il s'agit de conserver les concepts essentiels de ces deux modèles, mais en changeant le canal C&C.

On peut, par exemple, utiliser un serveur web en lieu et place du serveur IRC comme maître. L'avantage pour le pirate provient du fait que le trafic web sortant d'un site n'est pratiquement jamais interdit, car trop abondant pour pouvoir être surveillé sans informations complémentaires. On peut trouver également l'emploi des

messageries instantanées qui offrent les mêmes avantages que le web pour éviter les filtrages et le chiffrement des communications pour aveugler les sondes de détection d'intrusion positionnées par les gestionnaires de réseaux pour détecter les problèmes.

Taille

La taille des botnets est très variable, de quelques centaines de machines zombies à plusieurs dizaines de milliers. La moyenne est de l'ordre du millier d'éléments.

Un communiqué de presse du FBI en date du 13 juin 2007 peut illustrer les aspects économiques de ces outils [9]. Si l'une des personnes arrêtées est le créateur du botnet, les autres en sont les utilisateurs. Le nombre de machines faisant partie du botnet est de l'ordre du million. Le premier des utilisateurs a utilisé le botnet pour lancer des attaques de déni de service distribué. Le deuxième a envoyé un nombre considérable de messages publicitaires pour les services offerts sur son site web depuis les machines du botnet.

Selon une déclaration de Vinton Cerf, un des fondateurs de l'Internet, à Davos, en janvier 2007, pratiquement une machine connectée à Internet sur quatre ferait partie d'un botnet [10].

Cycle de vie d'un botnet

Pour constituer un botnet, un pirate doit répandre ses outils sur un grand nombre de machines, tout en évitant d'attirer l'attention des utilisateurs. Pour plus d'efficacité, il va faire en sorte d'infecter des machines qui vont ensuite être chargées de recruter d'autres victimes, accroissant ainsi considérablement la vitesse de constitution de son réseau. Il peut employer les méthodes généralement utilisées par les créateurs de virus pour diffuser à grande échelle leurs codes malveillants et les faire installer à l'insu des utilisateurs :

- Code malveillant envoyé en pièce jointe dans un courrier électronique. Lorsque l'utilisateur télécharge et exécute le fichier, il se retrouve contaminé. Cette méthode est indépendante des logiciels de l'utilisateur (hormis le système d'exploitation, bien sûr) et permet de contourner les précautions prises au niveau des serveurs de messagerie.
- Fichier d'apparence anodine contenant un cheval de Troie (jeux, faux correctifs, économiseurs d'écran, etc.).

- L'exploitation d'une faille d'un navigateur web : il est possible d'utiliser des sites web piégés afin d'infecter les utilisateurs consultant ces sites. Typiquement, il s'agit de sites de téléchargement de fichiers protégés par le droit d'auteur (warez) ou de sites de «charme». L'autre cas est celui de sites web légitimes piratés afin d'exécuter un programme à distance sur la machine d'une victime visitant le site web.

- L'exploitation d'une faille d'un logiciel très utilisé.

- Le «Peer-to-Peer» : le code malveillant se fait passer pour un fichier «alléchant» que l'utilisateur est invité à télécharger et à exécuter. L'exécution semblera échouer à cause d'une erreur dans le fichier alors que, en réalité, un nouveau zombie est né, etc. Pour inciter l'utilisateur à exécuter l'action qui va déclencher la procédure d'infection de son poste, les pirates utilisent des techniques d'ingénierie sociale plus ou moins subtiles. Qu'ils jouent sur la peur, la curiosité ou la séduction, force est de constater que leurs techniques sont très efficaces. L'internaute, mal sensibilisé aux problèmes de sécurité contribue très largement au succès de ces réseaux.

Les machines ainsi infectées peuvent ensuite mettre en œuvre d'autres techniques plus agressives pour faire croire le réseau.

- Campagnes d'envois de messages contenant un programme malicieux en pièce jointe ou encore des messages contenant des liens vers des pages web contenant du code malveillant.

- «Scans» réseau permettant de détecter et d'attaquer :

- des machines présentant des failles de sécurité sur des services accessibles par le réseau ;

- des portes dérobées (backdoors) déjà mises en place par d'autres codes malveillants ;

- des machines présentant des services protégés par des mots de passe faibles. La propagation par les partages réseau permet de se répandre à l'intérieur d'un sous-réseau de façon particulièrement efficace.

Une fois la machine infectée, le nouveau «bot» va se connecter au botnet et signaler sa présence. Ensuite, depuis la généralisation de la conception modulaire du mécanisme d'infection, la nouvelle recrue va télécharger et exécuter d'autres modules (mises à jour, nouvelles fonctionnalités). Pour assurer sa sécu- — suite page 3 —>

rité, le « bot » va alors effectuer quelques tâches dans le but de neutraliser les logiciels constituant la protection du poste infecté (antivirus, pare-feu personnels...). Quelques-uns de ces codes malveillants installent aussi des « rootkits » et autres programmes chargés de les rendre invisibles aux yeux des utilisateurs des systèmes ou des personnes chargées de les administrer. Il peut aussi appliquer des correctifs et nettoyer la machine afin d'éviter qu'un autre pirate n'y accède.

On voit bien ici l'intérêt de la construction modulaire des « bots ». À la différence d'un ver classique, dont l'efficacité diminue avec le comblement de la faille exploitée, un « bot » du type Agobot peut être modifié pour exploiter une nouvelle faille de sécurité afin de se propager encore plus longtemps sur davantage de systèmes. De plus, la modularité des vers engendre une altération de la signature virale lors des modifications du code qui, combinée avec l'utilisation de techniques de camouflage du code source rend les antivirus aveugles... Une fois bien installé sur la machine, le « bot » se met en attente des commandes de son maître.

Mais à quoi servent-ils ?

Au vu de l'organisation des botnets, on peut s'interroger sur l'intérêt pour un pirate de constituer un tel réseau. Les composants d'un botnet ne sont pas ciblés, donc il ne s'agit pas d'une attaque contre un site précis. Le nombre de machines attaquées n'est pas représentatif de l'habileté du pirate et la nature discrète du botnet contredit l'idée de s'autoproclamer auteur du ver le plus répandu.

En fait, les botnets sont l'illustration de la transformation du pirate informatique. Le défi technique a fait place à une économie souterraine dans laquelle le piratage n'est qu'un outil qu'il faut rentabiliser. Le changement d'orientation dans les motivations des pirates, de la curiosité et de la recherche de notoriété vers la recherche de profits financiers, a été marqué par l'apparition de « bots » de plus en plus sophistiqués et intégrant des fonctionnalités permettant de mener diverses actions frauduleuses depuis les postes infectés. Le « botherder » en loue l'utilisation pour une somme variable. D'après certaines informations, le prix le plus courant serait de 0,10 \$ par machine de botnet louée [5].

On peut se demander quels types d'acti-

tivité justifient la location des services d'un botnet. La réponse est : toutes celles qui pourraient avoir pour conséquence d'ostraciser leur auteur de la plupart des réseaux, voire le conduire à répondre de délits devant un tribunal.

Attaques en déni de service

Il est possible de louer les services d'un botnet pour monter une attaque de déni de service distribué. Ainsi, sur l'ordre du serveur maître, la machine esclave peut lancer des attaques en présentant pour origine le site piraté. Par exemple, l'envoi sur le canal IRC d'une commande déclenche une attaque en déni de service. En utilisant plusieurs milliers de machines émettant des requêtes simultanément, il est possible, par exemple, d'interdire l'accès à un site web. Les pertes subies par un site commercial paralysé pendant plusieurs heures sont sans commune mesure avec le coût de location d'un botnet. En 2004, un Américain a recouru aux services d'un botnet pour attaquer des entreprises avec lesquelles il était en conflit. Sur le plan financier, l'attaque a coûté 1 000 \$ à son organisateur et a entraîné des pertes de l'ordre de 2 millions de dollars à ses victimes [6].

Une variation de cette attaque est l'extorsion par chantage au déni de service. La principale différence est que le paiement

provient de la victime. Le premier cas connu s'est produit en 2004, lorsqu'un site américain a déclaré avoir subi une semaine d'attaques en déni de service après avoir refusé de payer 10 000 \$ à un maître chanteur [7].

Diffusion de spams

On peut également utiliser des « bots » pour émettre massivement des spams. Cette technique offre l'avantage à son commanditaire de camoufler son origine, permettant ainsi de contourner les filtrages par liste noire et les retours de bâton liés à l'envoi massif de spams (comme les vagues de retours d'erreurs massives pouvant survenir après les envois) ou encore le filtrage de son accès par son fournisseur d'accès. L'affaire médiatisée du « Spam King », révélée en mai 2007 est une bonne illustration du niveau que peut atteindre ce type d'activité. Ce professionnel récidiviste des campagnes d'envoi de spams, déjà condamné deux fois à des amendes de plusieurs millions de dollars, exerçait son activité en offrant à des clients potentiels l'envoi de 15 millions de courriers électroniques pour 295 \$ [8].

Attaques des internautes

Il est possible d'utiliser les zombies pour recueillir des informations personnelles sur les utilisateurs, informations qui seront utilisées dans le cadre de vols d'identité ou de fraude à la carte bancaire.

Une autre attaque dirigée par les machines zombies est la diffusion de logiciels publicitaires sur celles-ci. Contre rémunération, le « botherder » installera un logiciel publicitaire sur un certain nombre de machines auxquelles il a accès. On cite une somme de 0,20 \$ par installation.

Manipulation de sites web

D'autres attaques peuvent se fonder sur la manipulation d'outils de statistiques de fréquentation de sites web. Il s'agit soit de manipulations de sondages ou de jeux en ligne par l'utilisation coordonnée de nombreuses machines, suivant la méthode utilisée pour le tiercé dans le film *Le Gentleman d'Epsom*, soit d'une fraude aux clics en augmentant artificiellement le nombre d'utilisateurs suivant les publicités depuis un site complice.

Une autre possibilité est d'utiliser le botnet comme espace de stockage soit pour du contenu illégal, soit pour des sites d'escroqueries de type phishing. — suite page 5 —

Références

- [1] Guillaume Arcas & Xavier Mell, *Misc* n° 27 Botnets : la « menace fantôme » ou pas ?
- [2] John Canavan, *The Evolution of Malicious IRC Bots* : http://www.symantec.com/avcenter/reference/the_evolution_of_malicious_irc_bots.pdf
- [3] XMCO Partners *L'actu Sécu 15* : http://www.xmcopartners.com/actu-secu/actu_secu_juin2007.pdf
- [4] Kim-Kwang Raymond Choo : "Zombies and botnets" <http://www.aic.gov.au/publications/tandi2/tandi333t.html>
- [5] http://www.theregister.co.uk/2004/05/12/phatbot_zombie_trade/
- [6] <http://www.securityfocus.com/news/9411>
- [7] <http://www.greensheet.com/PriorIssues/041201-7.htm>
- [8] http://fr.wikipedia.org/wiki/Robert_Soloway
- [9] <http://www.fbi.gov/pressrel/pressrel07/botnet061307.htm>
- [10] <http://news.bbc.co.uk/1/hi/business/6298641.stm>
- [11] <http://www.pcinpact.com/actu/news/26624-Accuse-du-crash-reseau-dun-hopital-avec-son-.htm>

Évolution de la propagation des malwares

La propagation des logiciels malveillants n'est plus à démontrer. Quand des études récentes [1] estiment qu'environ un quart des ordinateurs connectés à Internet font partie d'un botnet, il est légitime de s'inquiéter et même d'affirmer que les mécanismes de sécurité aujourd'hui déployés ne sont pas suffisants. Ces botnets n'ont pour but que de générer du chiffre d'affaires par envoi de spams ou phishings, par chantage via des attaques de déni de service distribuées ou par récupération d'informations personnelles et confidentielles (numéros de CB, licences de logiciels...).

Laurent Butti, expert senior en sécurité des réseaux, France Télécom R&D/Orange Labs

Des améliorations notables sur les techniques de protection

Depuis quelques années, la situation aurait pu s'améliorer. Les antivirus et pare-feu personnels font maintenant partie du paysage informatique de l'utilisateur résidentiel qui est de loin le plus visé par la majorité des attaques. Les « boxes » des différents fournisseurs d'accès Internet qui se mettent en coupure entre la machine de l'utilisateur et l'Internet empêchent toute attaque directe de l'extérieur vers l'intérieur (pour peu que les règles du pare-feu de la « box » soient bien configurées). Bien qu'il existe toujours des Microsoft Windows XP SP1 en direct sur Internet sans pare-feu ni antivirus, cela devient quand même bien plus rare qu'auparavant !

Mais aussi sur les stratégies d'attaque

Les techniques de protection se démocratisant, les techniques d'attaques et les ruses associées ont aussi évolué très rapidement. Les exploitations directes de vulnérabilité dans les services présents dans des Microsoft Windows [2] ou les essais exhaustifs sur des serveurs SSH [3] existent toujours, en attestent les nombreuses tentatives de connexion repérées par des observatoires de l'Internet [4], mais cela devient de plus en plus marginal en comparaison avec les deux approches suivantes...

Une première approche consiste à berner l'utilisateur en l'incitant à récupérer et à exécuter un binaire inconnu (via une URL dans un mail précédemment reçu ou sur un site web malveillant). Cela peut être aussi un utilisateur à la recherche d'un « crack¹ », d'un « keygen² » ou de tout autre application qu'il jugera intéressante à exécuter. L'utilisateur naïf, exécutant alors le binaire, se compromet en installant alors un « rootkit³ » qui se camouflera au mieux dans le système d'exploitation compromis. Des études récentes sur les binaires relatifs au piratage de logiciels ont montré qu'environ un binaire sur deux contient du code malveillant (cheval de Troie ou tout autre spécimen) [5].

La deuxième approche consiste à héberger un outil d'exploitation web sur un site web (légitime, et donc préalablement compromis, ou spécialement conçu pour des actions malveillantes) et d'attendre⁴ que l'utilisateur s'y connecte. Cet outil va être en charge de repérer la connexion d'un naviga-

Exemple d'identification de navigateurs Internet. User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv: 1.8.1.6) Gecko/20061201 Firefox/2.0.0.6 (Ubuntu-feisty). User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

teur Internet sur le site web en question et va être capable de sélectionner l'exploitation de vulnérabilité la plus appropriée en fonction du navigateur de l'utilisateur. Cela est généralement réalisé grâce aux en-têtes présents dans la requête HTTP du navigateur Internet. Une exploitation de vulnérabilité réussie permet alors d'exécuter du code arbitraire sur la machine compromise. Par ce biais, un exécutable est alors récupéré et exécuté sur la machine compromise, et ce bien entendu à l'insu de l'utilisateur.

Un « business » toujours changeant

Récemment, un outil commercial (i.e. en vente, mais de manière illégale) permettant l'exploitation de vulnérabilités sur les navigateurs Internet a beaucoup fait parler de lui. Il s'agit de MPack, qui a été utilisé pour compromettre des centaines de milliers de machines via des serveurs web préalablement infectés par diverses failles de sécurité [6]. Une fois cet outil installé et configuré, il a permis l'installation de différents malwares sur de nombreuses machines compromises. En effet, MPack est un outil d'exploitation de vulnérabilité et non un outil de création de malwares, i.e. il n'est utilisé que pour la propagation. À charge ensuite à l'utilisateur de cet outil de faire les malwares les plus pertinents pour s'assurer un bon chiffre d'affaires ! Une interview instructive d'un des auteurs de MPack est disponible [7].

La principale particularité de MPack est son approche business. « MPack offre les mêmes types de services que des programmes licites, par exemple, des mises à jour. Les mises à jour de MPack sont de nouvelles versions de l'application comprenant de nouveaux exploits pour profiter des dernières vulnérabilités découvertes. Une nouvelle mise à jour est disponible tous les mois en moyenne et coûte entre 50 et 150 \$ », explique Luis Corrons, le directeur technique de PandaLabs. Aujourd'hui, de nombreux dérivés de MPack apparaissent et rendent accessible au plus grand nombre l'exploitation de navigateurs Internet.

Les vulnérabilités côté client

L'exploitation des vulnérabilités sur les applications clientes n'est pas un nouveau concept. Des initiatives telles que le « Month of Browser Bugs » [8] et le « Month of Kernel Bugs » [9] ont réellement contribué à la prise de conscience que de nombreux vecteurs d'attaque existent et que les erreurs d'implantation logicielle sont toujours légion, en particulier dans les applications clientes (navigateurs Internet, drivers Wi-Fi...).

Un autre exemple édifiant concerne les antivirus qui constituent l'outil de sécurité le plus répandu, aussi bien dans le contexte entreprise → suite page 5

Références

- [1] BBC News, « Criminals 'may overwhelm the web' », <http://news.bbc.co.uk/1/hi/business/6298641.stm>
- [2] Metasploit.LLC, « Metasploit Framework Exploits », <http://framework.metasploit.com/exploits/list>
- [3] SecurityFocus, « Analyzing Malicious SSH Login Attempts », <http://www.securityfocus.com/infocus/1876>
- [4] Arbor Networks, « Active Threat Level Analysis System (ATLAS) », <http://atlas.arbor.net/>
- [5] Jacomo Picolini, « Malware distribution through software piracy: a case study », <http://www.first.org/conference/2007/papers/picolini-jacomo-slides.pdf>
- [6] TrendLabs Malware Blog, « Another malware pulls an Italian job », <http://blog.trendmicro.com/another-malware-pulls-an-italian-job/>
- [7] SecurityFocus, « Newsmaker: DCT, MPack developer », <http://www.securityfocus.com/news/11476>
- [8] Month of Browser Bugs, <http://browserfun.blogspot.com/>
- [9] Month of Kernel Bugs, <http://projects.info-pull.com/mokb/>
- [10] Références Common Vulnerabilities and Exposure, <http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=antivirus>
- [11] Laurent Butti, « Wi-Fi Advanced Fuzzing », <http://www.blackhat.com/presentations/bh-europe-07/Butti/Presentation/bh-eu-07-Butti.pdf>

... suite de la page 4

que résidentiel. Le reproche classique à l'encontre de ces logiciels concerne la facilité de contournement de leurs règles de détection des codes malveillants. Une autre problématique mise en exergue plus récemment concerne la qualité de leur implantation logicielle. En effet, aujourd'hui il est plus qu'envisageable que votre antivirus se fasse compromettre par une pièce jointe spécifiquement formatée à cet effet [10]. Et c'est bien le comble que l'intégrité du système d'exploitation soit compromise par l'intermédiaire d'un outil censé rajouter une couche de sécurité... C'est une bonne piqûre de rappel sur le fait que tous ces outils ne sortent pas de terre tout seuls, et qu'il faut bien les programmer avec toutes les erreurs classiques de programmation en C/C++. Vous me direz alors que ces erreurs de programmation sont peut-être complexes à découvrir, que nenni! Aujourd'hui, la plupart des vulnérabilités découvertes dans les différents logiciels antivirus le sont par des techniques de «fuzzing». Le «fuzzing» est une technique de tests logiciels visant à découvrir des dysfonctionnements en termes d'implantation logicielle, typiquement les débordements de tampons («buffer overflows»). Selon la complexité de l'application ou du protocole réseau audité, un simple fuzzer en quelques lignes de Python/Ruby est suffisant pour découvrir des vulnérabilités critiques et exploitables [11].

Conclusion

Il faut garder en tête que les attaques directes sont de moins en moins efficaces de par la démocratisation des pare-feu sur les «boxes» et les systèmes d'exploitation (Microsoft Windows XP SP2 étant un bon exemple). Par conséquent, les techniques des attaquants ont évolué vers les applications clientes et les utilisateurs afin de maintenir une forte hausse de leur chiffre d'affaires, et ce malgré tous les efforts dans la lutte contre les propagations de code malveillants.

Conclusion

De manière générale, la sécurité doit être assurée par un savant mélange entre la sensibilisation des utilisateurs et la technique.

laurent.butti@orange-ftgroup.com

laurent.butti@orange-ftgroup.com

... suite de la page 3

Effets pour l'administrateur

Pour le responsable d'un réseau, la simple présence de machines faisant partie d'un botnet à l'intérieur de son réseau peut avoir des effets non négligeables. Certains des effets négatifs des botnets se font sentir dès la contamination des machines, d'autres ne se font sentir que lorsque le botnet reçoit des commandes.

Le premier problème est que la première machine infectée cherchera à contaminer ses voisines et des machines extérieures. On retrouve ici le comportement d'un ver. À ce moment, un déni de service peut se produire si le volume de trafic généré par le bot est supérieur à la capacité des éléments réseaux. Cela peut se produire au niveau des liaisons réseaux, des routeurs de sortie ou d'entrée de site ou des serveurs de courrier électronique.

En février 2006, on a annoncé que la présence d'un botnet avait provoqué des pannes informatiques perturbant le fonctionnement d'un hôpital de Seattle [11]. Ces pannes semblent avoir eu pour origine une tentative du système automatique de sécurité informatique de contenir l'infection qui a perturbé le fonctionnement d'équipements vitaux.

En dépit du fait que les effets du vol d'identité ne concernent pas directement le réseau ou son gestionnaire, il ne faut pas en négliger les conséquences pour le travail du responsable. Le fait que des données personnelles des utilisateurs aient été dérobées via des machines sous sa responsabilité peut lui causer des ennuis, en particulier si ces informations ont été employées de façon à nuire à l'image et/ou à l'activité de son employeur. Faire partie d'un botnet signifie que à toutes

les étapes de la vie de celui-ci, vos machines commettront des actes répréhensibles. La source de l'attaque sera le réseau infecté. Il convient donc de prendre en compte les conséquences, en termes d'image ou sur le plan judiciaire, de ces actions.

Être à la source de l'émission de spams peut conduire à l'inscription de ses plages d'adresse IP dans des listes noires. Cela peut avoir pour conséquence le rejet du courrier légitime de vos utilisateurs par des sites extérieurs consultant ces listes noires. La participation à un déni de service, distribué ou non, entraîne rarement des représailles. Toutefois, cela peut conduire à une hausse insupportable du trafic au niveau local, entraînant ainsi une saturation de la connectivité à l'intérieur du réseau.

Recommandations

La première manière de se protéger des botnets consiste à éviter que ses machines en fassent partie. Il faut donc mettre en œuvre des moyens de prévention permettant sinon d'éliminer complètement le risque (la sécurité à 100% n'existant pas), au moins de le limiter. À ce niveau, il faut se rappeler que la construction d'un botnet se sert des mécanismes de propagation des vers. Des mesures peuvent être prises à deux niveaux : l'utilisateur et l'équipe chargée de gérer un réseau.

Perspective utilisateur

Protection du poste client

Quelques mesures de protection logicielles peuvent être mises en place :

- mettre son système à jour régulièrement ;
- installer un logiciel antivirus et s'assurer de sa mise à jour régulière ;
- installer un pare-feu personnel ;

- installer un outil chargé de la détection des logiciels espions ;
- mettre à jour les applications logicielles (logiciels de bureautique, navigateurs web, clients de messagerie, clients de messagerie instantanée, lecteurs multimédias, etc.) du poste dès que des nouveaux correctifs de sécurité sont publiés.

Il est arrivé parfois que l'utilisateur désactive la mise à jour automatique de son poste. Cette manipulation doit absolument être évitée car elle rend le poste vulnérable. Il convient de se rappeler que la durée de vie d'une machine non mise à jour est inférieure à 15 minutes. La gêne limitée induite par la mise à jour est moindre que le nettoyage d'une infection.

Dans la chaîne de l'organisation de la sécurité, il est fréquent de dire que l'humain est le maillon faible. À ce niveau-là, on peut cependant limiter les dégâts en adoptant quelques bonnes habitudes.

Précautions relatives à la messagerie électronique

Il est ainsi recommandé de se montrer méfiant quant au contenu des messages et notamment :

- de lire ses messages au format texte plutôt que HTML dans la mesure du possible ;
- d'éviter de répondre aux messages de type spam ou de suivre des liens dans ceux-ci. Quelques spams échappent toujours à la vigilance des divers moyens de filtrage mis en place. Il faut donc apprendre à les repérer afin d'éviter d'ouvrir un message piégé et d'être la victime d'une attaque nouvelle sur votre client de messagerie ;
- dans le même ordre d'idées, évitez d'ouvrir inconsidérément toutes les pièces jointes que vous recevez. N'hésitez pas à vérifier que ce message

... suite page 6

provient bien d'une source de confiance si vous n'attendez pas de documents. Si vous devez vraiment l'ouvrir, enregistrer la pièce jointe sur votre disque. Avant exécution, passez-la au crible de votre antivirus ;

- ne jamais oublier que vos éditeurs de logiciels ou de systèmes n'envoient jamais de correctifs par le biais de la messagerie électronique.

Précautions pour la navigation sur Internet

- Privilégiez la navigation sur des sites de confiance, des sites institutionnels, des sites d'organismes bien connus. Évitez les sites bizarres ou comportant des contenus inappropriés qui hébergent souvent des codes malveillants.
- Configurez votre navigateur de manière à limiter aux sites web autorisés l'exécution de code dynamique par votre navigateur (Javascripts, contrôles ActiveX, etc.). Il est possible par exemple de désactiver ces fonctionnalités et de les réactiver au cas par cas seulement.

Précautions pour le téléchargement de fichiers

Quel que soit le canal utilisé (IRC, web, messagerie électronique, P2P), il faut absolument éviter de télécharger n'importe quel programme trouvé sur Internet. Si possible, télécharger l'outil depuis le site de son éditeur (ou du développeur) est toujours préférable. Si vous téléchargez un programme inconnu, il est prudent de le vérifier à l'aide d'un antivirus.

Perspective équipe technique

- Apporter une attention particulière à la gestion des mots de passe et des comptes utilisateurs.
- Il est primordial de penser à mettre en place une bonne politique de gestion des correctifs de sécurité (systèmes et logiciels) aussi bien sur les serveurs et équipements réseau que sur les postes clients.
- Prendre en compte cette même gestion en ce qui concerne les postes nomades, trop souvent vecteurs d'entrée de codes malveillants sur des réseaux autrement bien cloisonnés de ce point de vue.
- Installer une application permettant de nettoyer le flux de messages électroniques entrant au niveau de votre passerelle de messagerie.
- Dans la mesure du possible, n'accorder que des droits restreints aux utilisateurs pour limiter les droits du code malveillant.
- Suivre avec vigilance les applications PHP,

ASP et serveurs installées sur les serveurs web.

- La mise en place d'un cloisonnement du réseau à l'aide de filtres sur les routeurs, de pare-feu et « VLAN » réduit la vulnérabilité face à l'extérieur et à l'extension d'une éventuelle contamination.
- Mettre en place des outils de détection d'intrusion (IDS) en combinaison avec les journaux de filtrage. Cela vous permet de repérer les machines infectées et donc de procéder rapidement au nettoyage de la machine.
- L'utilisation de la métrologie peut aider à détecter les machines contaminées en repérant le serveur maître IRC à partir d'une première machine, puis en analysant toutes les autres qui peuvent contacter ce serveur. Alternativement, l'analyse des traces réseaux produites par le « bot » peut permettre de localiser les machines infectées. Ces traces peuvent provenir d'outils de métrologie, de fichiers journaux de routeurs, de pare-feu et de systèmes de détection d'intrusion.

Cette liste de mesures n'a pas la prétention d'être exhaustive. Bien d'autres choses peuvent être mises en œuvre pour assurer la sécurité de vos systèmes. Elle peut cependant contribuer à vous aider à vous protéger d'un grand nombre d'attaques et être le point de départ d'une réflexion plus poussée sur ce que vous pouvez faire pour améliorer la sécurité dans votre environnement.

Premières actions en cas d'infection

De nouvelles attaques et de nouveaux codes apparaissent constamment. On assiste à une course permanente entre l'épée et la cuirasse informatiques. Des

moyens de contourner les dispositifs de sécurité en place sont légion. Rappelons qu'en cas d'infection la plupart des codes malveillants cherchent à désactiver les protections activées sur les systèmes.

Il est donc fort probable que, malgré tout, des infections soient à déplorer. En cas d'infection, la solution idéale serait de faire une sauvegarde des données et de réinstaller le système. Après cette procédure, il convient de s'assurer que le système et les logiciels sont à jour afin d'éviter la répétition de l'attaque. Il est aussi utile de prendre en compte le caractère virulent du « bot » : il est très possible que d'autres machines de votre périmètre aient aussi été infectées.

Conclusion

Les botnets sont une épine dans le pied de tout responsable de système d'information désireux de protéger son réseau. En dépit de quelques condamnations spectaculaires, il est hautement improbable que ceux-ci disparaissent. Ils sont symptomatiques de l'évolution vers la criminalité organisée de l'« underground informatique » et l'un des principaux outils permettant aux pirates de monnayer leurs actions. La combinaison du développement des méthodes de camouflage face aux antivirus et IDS et du nombre de machines non administrées, connectées en permanence à haut débit, permet de supposer que ce problème restera longtemps à l'esprit des personnes s'intéressant à la sécurité réseau. ■

ducrot@renater.fr, danho@renater.fr,
marronnier@renater.fr

Définitions

IRC : Internet Relay Chat, mode de communication instantané développé au début des années 1990. Un utilisateur se connecte à un canal IRC pour discuter avec d'autres.

Peer-to-Peer (P2P) : modèle d'organisation dans lequel il n'existe pas de serveur central, les utilisateurs étant interconnectés entre eux. Chaque nœud de réseau peut agir indifféremment en tant que client ou serveur.

Scans : sondage réseau permettant de recenser des cibles d'attaques potentielles.

Déni de service : attaque consistant à provoquer des perturbations au niveau de la machine cible ou de sa connexion réseau de telle sorte qu'elle ne puisse plus répondre aux demandes de services de ses utilisateurs légitimes.

Spam : courrier électronique non désiré, généralement envoyé à des fins publicitaires par de parfaits inconnus.

SÉCURITÉ INFORMATIQUE

numéro 61 octobre 2007
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 4 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :

JOSEPH ILLAND
Fonctionnaire de Sécurité de Défense
Centre national de la recherche scientifique
3, rue Michel-Ange, 75794 Paris-XVI
Tél. : 01 44 96 41 88
Courriel : Joseph.Illand@cnrs-dir.fr
<http://www.sg.cnrs.fr/fsd>

Rédacteur en chef de ce numéro :

ROBERT LONGEON
Chargé de mission SSI du CNRS
Courriel : robert.longeon@cnrs-dir.fr

ISSN 1257-8819

Commission paritaire n° 1010 B 07548
La reproduction totale ou partielle des articles est autorisée sous réserve de mention d'origine.