Le business model du Botnet

Février 2008

La marche des zombies

Lorsque, contaminés par un code malicieux, des PC se réveillent, c'est tout un monde des ténèbres qui s'active sur le Net et ces PC, devenus zombies, sortent de leur léthargie pour envahir la toile, dévorer les bandes passantes des réseaux et laisser sur les messageries des honnêtes gens de bien étranges missives.

Percevez-vous dans la nuit cette marche des zombies qui approchent de votre poste de travail ?

Mais qui sont ces spammeurs ?

D'où viennent ces masses de SPAM que vous recevez sans cesse et qui saturent vos boîtes aux lettres ?

L'examen des e-mails des expéditeurs montre que ce sont rarement des mêmes adresses que partent ces messages et les adresses semblent être de vraies adresses électroniques. Et c'est le cas ; ces expéditeurs existent bel et bien dans le monde réel et seraient très étonnés si vous leur demandez d'arrêter de vous envoyer des SPAM car ils n'ont pas conscience d'être des spammeurs et pourtant ils le sont.

Leurs postes de travail ne sont plus exclusivement sous leur contrôle mais sont aussi sous le contrôle d'un personnage occulte, tapi dans un endroit obscur de l'Internet. Ce personnage commande à distance une armée de PC, et parmi eux peut-être le vôtre.

Le vôtre ? Mais alors vous envoyez aussi des SPAM ? Oui, en effet, vous ne le savez pas mais vous envoyez des e-mails pour promouvoir telle marque de pilules de Vi Agra, des montres de contrefaçon, des diplômes usurpés, des actions à bas prix et dont le cours monte rapidement et encore d'autres produits connus pour être des arnaques. Peut-être un jour une de vos connaissances, destinataire d'un e-mail qui vient de vous, s'en étonnera. Peut-être même recevrez vous un SPAM de vous-même !

Des enquêtes récentes indiquent que près de 95% des SPAM sont envoyés par des ordinateurs « zombies » qui exécutent, à l'insu de leur propriétaire, des ordres venus d'ailleurs. La France est au 6eme rang des pays qui émettent des SPAM, les Etats Unis occupent la première place, pourtant, ni les Français ni les Américains ne sont connus pour avoir comme passe temps l'envoi de SPAM. C'est bien dans ces pays que l'on compte le plus d'ordinateurs devenus des zombies.

Il y a un zombie dans ma sacoche !

Un ordinateur devient zombie après contamination par un virus ou un ver spécialisé appelé le bot. Ce code malicieux arrive par la voie classique empruntée par les virus : la messagerie, le Web, le Peer to Peer … Le ver Storm Worm s'est ainsi abattu sur nos ressources informatiques, il y a quelques mois, causant l'infection de millions de victimes. Le programme malicieux installe sur le PC cible, un service client qui ouvre un canal, souvent un canal IRC (Internet Relay Chat), par lequel le PC contaminé se met à l'écoute sur le Net, d'ordres qui proviennent d'un serveur IRC dont l'adresse a été communiquée à la victime au cours de l'infection. Ce serveur peut contrôler des centaines, des milliers, des millions de PC contaminés par un bot. On appelle botnet, l'ensemble de ces PC zombies qui agissent en réseaux virtuels, aux ordres d'un maître.

Le bot ne détruit pas les données du PC et n'altère pas le fonctionnement des services, mais en utilise les ressources. Le propriétaire du PC ne perçoit aucune anomalie si ce n'est parfois une petite ou une grande lenteur sur le fonctionnement habituel.

La question qui se pose aujourd'hui n'est pas de savoir si vous êtes contaminés mais combien de bots se battent en duel pour prendre le contrôle de vos postes de travail.

Le maître du botnet

Supervisant les PC contaminés règne, tout puissant et très écouté, le maître du botnet. Si le réseau virtuel, à sa disposition, se compose de cent mille PC devenus zombies, une activation par le maître de ses zombies, parmi lesquels se trouve peut-être votre poste de travail, qui leur demande d'envoyer chacun dix e-mails à une liste communiquée, différente pour chaque zombie et c'est un million de SPAM qui partent sur l'Internet, alimentant la prolifération des milliards de SPAM quotidiens.

Le maître du botnet qui enverrait directement de son poste de travail un million de e-mails, passerait immanquablement pour un spammeur. Dans ce modèle, ce sont des dizaines de milliers de PC qui envoient chacun dix mails, quoi de plus naturel et qui pourrait s'en inquiéter ?

Bien sûr il peut sembler facile de remonter jusqu'au poste de travail qui active les zombies composant un large botnet. C'est pourquoi le poste de travail du maître du botnet change souvent d'adresse. L'adresse repérée est alors celle d'un serveur qui n'existe plus. Mais alors le serveur parti sans laisser d'adresse perd automatiquement la possibilité d'être

entendu s'il n'est plus à l'endroit que les zombies écoutent ? Non car avant de partir pour s'établir sous d'autres cieux momentanément plus sereins, avec une adresse provisoire pour quelques jours ou quelques heures, le serveur demande à chaque PC zombie de se mettre à jour en téléchargeant la nouvelle adresse qu'il devra désormais écouter après le départ du maître.

Pas vu, pas pris mais quand bien même il serait repéré, qui porterait plainte, et contre qui et quelles lois s'appliqueraient ? Le maître du botnet n'agit bien sûr pas sur le sol de pays où la législation pourrait l'inquiéter.

Le SPAM et le déni de service

Le SPAM n'est qu'un des services inavouables que le botnet permet. Le déni de service est une autre attaque pratiquée par les zombies à la demande du maître. Qui peut envoyer des mails peut aussi consulter un Web, alors quand le maître du botnet ordonne à ses cent mille PC zombies de solliciter, chacun cent fois, le Web institutionnel de votre société … Félicitation pour le succès de votre vitrine, elle recevra dix millions de sollicitations en un temps record mais malheureusement pour vos vrais clients, votre Web, incapable d'absorber une telle charge sera vite rendu indisponible par saturation de sa bande passante.

Et cette attaque en déni de service se produit au pire moment, celui où vos affaires exigeront que votre Web soit en parfait état de fonctionnement et qu'il réponde rapidement aux sollicitations, comme c'est le cas quand vous sortez un nouveau produit ou un nouveau service en ligne.

Le commanditaire

Un point important a été jusque là laissé de côté. Pourquoi le maître du botnet commet-il ces actions néfastes qui de plus, dans certains pays, constituent parfois un déli pénal sanctionné, par exemple en France par les lois Godfrain, articles 323-1 à 323-3 du code pénal ? Il faut savoir que les cybercriminels aujourd'hui n'agissent plus, en général, pour la gloire ou pour la délicieuse poussée d'adrénaline ressentie suite à une attaque destructive qui réussit. Aujourd'hui c'est le business qui motive les attaques et c'est bien pour gagner un argent facile que le maître du botnet a conquis son réseau de zombies et l'exploite.

Là intervient le commanditaire, personnage le moins recommandable de ce modèle économique. Le maître du botnet n'est qu'un exécutant, et si je puis me permettre en me plaçant du côté obscur de la force, un commerçant qui offre un service. Possédant, sous sa cyber-autorité un nombre impressionnant de postes de travail prêts à lui obéir, le maître du botnet va proposer aux enchères l'utilisation de son réseau de PC infectés en passant par des moyens occultes comme des forums spécialisés ou le bouche à oreilles. Sa notoriété s'acquiert par le nombre de PC qui composent son botnet et par l'importance des sites attaqués.

Pour attaquer en déni de services une grande banque durant telle plage horaire, en activant tel nombre de PC zombies, ce sera fait moyennant un tarif à discuter. Pour attaquer votre concurrent, en déni de services, ce sera un autre tarif dépendant de sa notoriété. Pour l'envoi de quelques millions de SPAM, ce sera encore un autre prix, de toute façon moins élevé que si les messages partaient par la poste. La loi de l'offre et de la demande joue aussi pour le cyber criminel.

Nous voici revenus au temps des assignats qui remplissaient de gens, peut-être honnêtes, les cachots de la Bastille.

Les contre-mesures pour un monde sans zombies

Des contre-mesures peuvent être mises en œuvre mais sont-elles efficaces ? Tout dépend, comme c'est souvent les cas en matière de défense, si c'est l'attaquant ou le défenseur qui prend une longueur d'avance et du temps de réaction.

Le modèle du botnet repose sur les communications entre maître et zombies en utilisant un canal IRC. Il suffirait de bloquer ce canal, sur le PC infecté, par un firewall personnel bien configuré. Mais les botnets passent de plus en plus aujourd'hui par le port 80 qui est celui du Web et utilisent le protocole du Web. Vous ne pouvez bloquer le port 80 sinon, vous n'auriez plus d'accès possible à la toile.

Le PC devient zombie quand il est contaminé par un bot, qui n'est en fait qu'un virus ou un ver particulier. Il suffit donc d'éradiquer ce code malfaisant par un anti-virus efficace, mais les bots aujourd'hui ont atteint un haut niveau de sophistication et sont d'autant plus difficiles à déceler qu'ils sont souvent accompagnés d'un rootkit qui les rend furtifs.

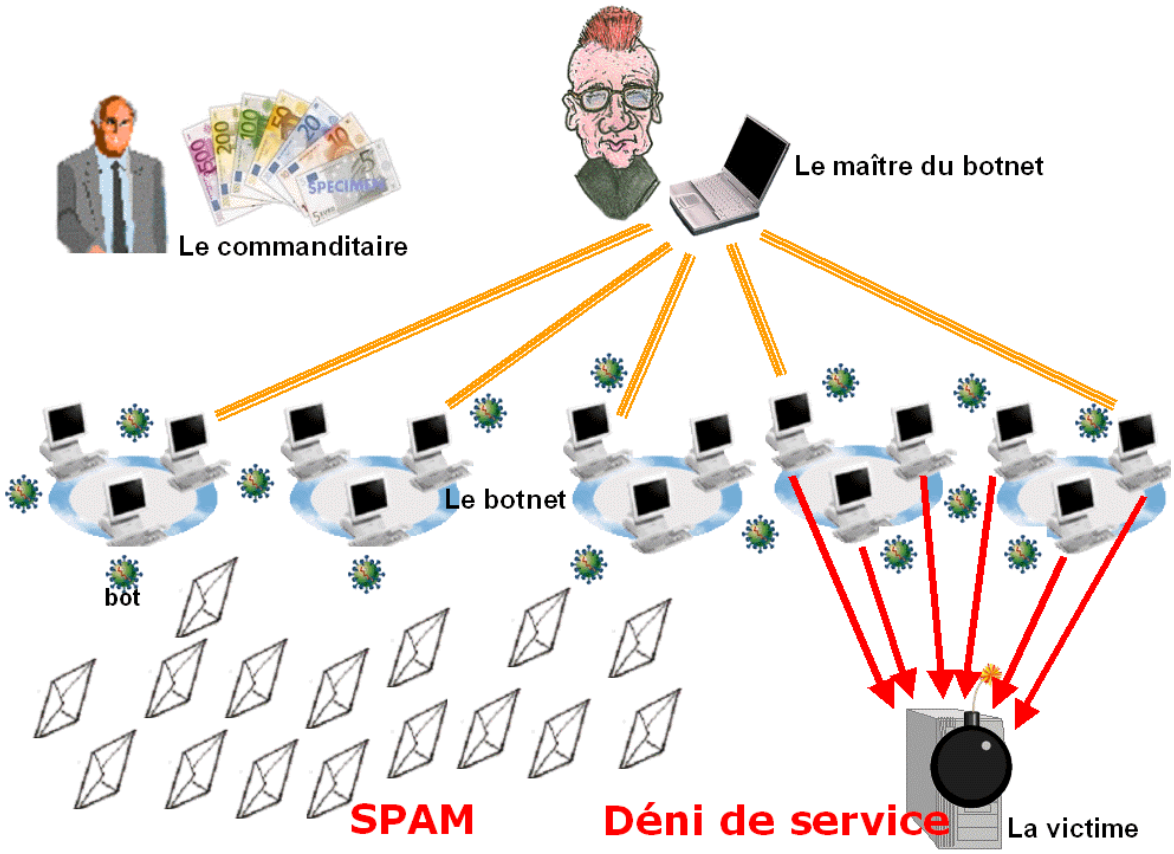
En observant un PC contaminé durant sa phase d'activation, on peut essayer de remonter au maître du botnet ? En fait chaque PC zombie n'est pas systématiquement activé lors d'une attaque. Le maître d'un botnet de plusieurs centaines de milliers de PC zombies peut en activer une dizaine de milliers pour telle attaque, une autre dizaine de milliers pour telle autre. Ceci explique qu'il peut se

passer du temps entre deux attaques qu'on demande à un PC de perpétrer.

Le personnage à coincer, judiciairement parlant, devrait être le commanditaire qui, moyennant finance, profite de l'existence des botnets. Celui-ci, contrairement au maître du botnet ne réside pas, en général, dans un pays où les lois anti cybercriminalité n'existent qu'en théorie. Mais là encore, si toutes les précautions sont prises, il est difficile de réunir les preuves des pratiques malveillantes qui l'accusent.

La cybercriminalité recherche des gains moins risqués sur le monde virtuel que ceux des attaques et des arnaques faites dans le monde réel, et les botnets sont un parfait exemple de cette nouvelle tendance.

Gérard Peliks
Président de l'atelier sécurité
Forum ATENA
www.forumatena.org



Le botnet utilisé comme générateur de SPAM et de déni de services