Proposition de recherche doctorale

Lutte contre les botnets: analyse et stratégie

Mots clés :

- **Directeur de thèse** : Matthieu Latapy
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire d'informatique de Paris 6
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

Les botnets, ou réseaux d'ordinateurs zombies, constituent l'un des premiers outils de la délinquance sur Internet aujourd'hui. La création d'un botnet consiste à prendre le contrôle d'un maximum de systèmes informatiques connectés à Internet, par la diffusion d'un logiciel malveillant qui se connecte à un système de commande, placé sous le contrôle du malfaiteur. Ces systèmes de commande peuvent être de nature différente, mais le plus souvent il s'agira de l'utilisation du protocole HTTP (celui du Web) ou IRC (Internet relay chat, protocole permettant la discussion ou l'échange de fichiers). Celui qui contrôle un tel réseau est traditionnellement appelé « pasteur ». Par la suite, l'ensemble de ces machines, lorsqu'elles sont connectées à Internet, et à l'insu de leur utilisateur légitime, répondent aux directives de leur « pasteur » et peuvent être utilisées pour conduire des attaques en déni de service distribué, la distribution de contenus illicites ou malveillants, la diffusion de courriers électroniques non sollicités (ou « spam »), la collecte des données personnelles des usagers de ces machines, du calcul distribué ou toute autre activité qu'il souhaitera. Ces botnets constituent, selon les juridictions, l'élément matériel d'infractions contre des systèmes informatiques – et en particulier en France de l'ensemble des infractions d'atteintes aux systèmes de traitement automatisé de données. Ils peuvent être aussi les outils permettant d'effectuer toutes les activités illégales décrites précédemment et donc permettent la commission de l'ensemble des infractions correspondantes. Ils permettent aussi de concrétiser le développement d'un nouveau type d'activités criminelles : le crime comme un service (ou « crime as a service », CaaS), avec ici la possibilité de louer un botnet pour quelques heures ou quelques jours : sa puissance de calcul, sa puissance de frappe ou sa capacité à collecter des données personnelles ou diffuser des contenus illicites discrètement et efficacement. Les botnets constituent un défi en matière de répression. D'abord par l'importance de leur impact sur la sécurité des réseaux et la commission d'infractions sur Internet. Ensuite par la dimension extrêmement internationale de leur diffusion et donc une certaine difficulté à mener des investigations. Enfin, par le grand nombre des acteurs qui peuvent être impliqués (les codeurs qui écrivent les programmes du logiciel malveillant, le pasteur évoqué plus haut, les mules chargées éventuellement de relayer les gains financiers issus des activités illégales, les commanditaires ou les commerçants de services). On retrouve même parfois de véritables sociétés, chargées de gérer des infrastructures pour ces botnets ou de commercialiser leurs services. Elles sont souvent liées à d'autres activités illégales telles que la commercialisation de faux logiciels de sécurité ou l'accès à des contenus illicites tels la pédopornographie. La réponse à l'enjeu des botnets rassemble de nombreux acteurs : les opérateurs de communications électroniques, des entreprises de sécurité des systèmes d'information, des éditeurs de solutions de sécurisation, les services de police et la justice ; et comme souvent en matière de sécurité sur Internet les usagers jouent un rôle important. Les méthodes employées sont pour l'instant assez inefficaces et le nombre d'interpellations d'auteurs et de gestionnaires de botnets est limité par rapport à l'ampleur du phénomène. Et très rapidement les méthodes employées dans une première affaire s'avèrent ensuite inefficace sur la suivante car les méthodes des délinquants eux-mêmes évoluent très rapidement. L'étude portera donc dans un premier temps sur un état des lieux aussi complet que possible des botnets : leur fonctionnement, les acteurs et leur organisation, ainsi que les évolutions observées. Pour chacun de ces éléments seront proposés une approche historique, une taxonomie et autant que possible une vision géographique. Évidemment cette première partie s'appuiera sur l'étude d'exemples concrets tels qu'ils ont pu être observés et étudiés. La seconde partie décrit les réponses apportées par les différents acteurs qui ont cherché à en apporter, qu'il s'agisse d'institutions gouvernementales, d'initiatives privées isolées ou structurées. Cette partie s'attachera notamment à mettre en évidence les clés des succès éventuels et les raisons des échecs. Si nécessaire des adaptations de ces solutions seront proposées. La troisième partie enfin proposera une stratégie d'ensemble pour lutter durablement contre les botnets, dans un esprit comparable à celui d'une véritable politique de santé publique à l'échelle mondiale. Cette stratégie devra en particulier mettre l'accent sur la prise en compte des évolutions prévisibles tant sur le plan technique qu'organisationnel des botnets. L'étude sera menée sous la forme d'une ample recherche bibliographique, d'analyse techniques de logiciels malveillants et de solutions de sécurisation, le développement éventuel de telles solutions ou de concepts pour la création de ces solutions, et enfin, d'entretiens avec des acteurs de cette lutte ou d'autres équipes de recherche sur ces sujets.