Vade Secure
Predictive Email Defense

Les botnets : acteurs majeurs de l'ombre

Auteur
Sébastien GOUTAL
Chief Science Officer

Index

Introduction

L'écosystème d'Internet est d'une complexité insoupçonnée, et en particulier sa part obscure. Au coeur de cet écosystème, les botnets tiennent une place de choix, et sont à l'origine d'un très grand nombre de menaces qui occupent à plein temps les différents acteurs de la sécurité informatique.

Mais tout d'abord, qu'est-ce qu'un botnet ? Littéralement, un botnet est la contraction de deux termes: «robot» et «network». Il s'agit donc d'un réseau de robots - robot désignant un agent ou un programme informatique - dont la finalité est malveillante. Les exemples d'activité malveillante sont nombreux, et l'envoi de spam et de virus par email sont des exemples-types de l'activité des botnets. Un botnet est contrôlé par une personne physique: il s'agit du *botmaster* (1).

Nous allons présenter plus en détail les botnets, en nous intéressant au cycle de vie de ces derniers : ce choix de perspective permettra d'appréhender toute la problématique relative aux botnets, autant d'un point de vue technique que d'un point de vue économique et juridique.

(1) Il peut évidemment y avoir plusieurs botmasters pour un même botnet.

Naissance d'un botnet

Le support physique d'un agent malveillant – ou *malware* - est une *machine zombie* : il s'agit en général d'un ordinateur contrôlé par le botnet, à l'insu de son utilisateur légitime. Un exemple typique de machine zombie est un ordinateur familial placé derrière une connexion ADSL, dont des éléments essentiels à la sécurité ne sont pas à jour (système d'exploitation, navigateur internet, anti-virus...) et qui a été compromis soit par l'exécution d'une pièce jointe contenant un virus, soit par la visite d'un site web infecté. S'appuyer sur une telle infrastructure a des avantages indéniables d'un point de vue économique : les coûts, que ce soit le hardware, la bande passante ou l'électricité sont intégralement à la charge de son utilisateur légitime.

Donner naissance à un botnet revient à constituer un réseau de machines zombies, par l'intermédiaire d'une phase d'infection virale de grande ampleur. Cette phase d'infection se déroule en plusieurs étapes :

1. Le développement d'un malware qui permettra à la machine zombie de communiquer avec le botnet, et d'effectuer les activités malveillantes. Ce développement nécessitera en outre l'exploitation d'une faille de sécurité, qui peut être innovante, ou bien déjà connue, pour installer le malware à l'insu de l'utilisateur légitime. A noter que certaines failles de sécurité innovantes – et pouvant potentiellement affecter des systèmes d'exploitation ou des logiciels récents - peuvent être achetées ou vendues sur le marché noir.

2. La constitution d'un carnet d'adresses, qui est la liste des utilisateurs cibles de la phase d'infection virale. Ces listes peuvent être constituées par des robots qui collectent des adresses emails trouvées sur Internet [(2)] ou bien être achetées directement sur le marché noir.

3. L'envoi d'une campagne d'emails qui, soit contient le malware sous forme de pièce attachée, soit fait référence à ce malware par l'intermédiaire d'un lien vers un site web infecté. L'envoi de cette campagne peut d'ailleurs être sous-traité en sollicitant les services d'un autre botnet.

4. La réception d'un email contenant le malware sous une des formes précisées précédemment et l'installation de ce dernier par certains utilisateurs cibles de la phase d'infection virale. Le taux d'infection est très variable et dépend d'une part du niveau de protection de chaque utilisateur, et d'autre part de la qualité de la faille de sécurité exploitée.

Suite à cette phase d'infection initiale qui permet au botnet de prendre vie, d'autres phases d'infection peuvent avoir lieu pour agrandir le botnet [(3)]. Un botnet peut atteindre une taille considérable : on estime par exemple que le botnet Bredolab était constitué à son paroxysme de près de 30.000.000 de machines zombies.

(2) En parcourant des forums de discussion par exemple.

(3) De la même manière, des phases d'infection peuvent avoir lieu pour reconstituer un botnet qui a été partiellement démantelé.

Vie d'un botnet

Suite à l'installation du malware sur la machine cible, ce dernier va contacter un des nombreux serveurs de contrôle et de commande (4) du botnet. Ces serveurs servent à piloter (5) les activités des machines zombies, à collecter des informations, et également à mettre à jour le malware : ils constituent la clé de voûte de l'infrastructure de communication du botnet.

Le malware va espionner la machine cible, et remonter toute information utile : numéro de cartes bancaires, mots de passe, données personnelles (nom, prénom, numéro de sécurité sociale... utilisés à des fins d'usurpation d'identité), carnet d'adresses.... Ces données seront ensuite agrégées, et utilisées directement ou bien revendues sur le marché noir par le botmaster. A noter que les adresses email collectées sont d'une grande importance pour le botnet, car elles permettent d'effectuer de nouvelles phases d'infection virale permettant d'agrandir ce dernier.

En outre, le malware va effectuer les différentes tâches qui lui seront affectées, parmi lesquelles :

- L'envoi d'une campagne de spam ou de virus, en utilisant un modèle d'email et une liste de destinataires : à ce modèle seront ajoutés des éléments variables et aléatoires, de manière à échapper aux systèmes de filtrage par signature.
- Effectuer une attaque par déni de service distribué (6).
- Effectuer de la fraude au clic (7) pour générer des revenus publicitaires frauduleux.
- Effectuer du calcul intensif, en particulier pour casser certaines clés de cryptage.

(4) Les serveurs de contrôle et de commande sont généralement installés chez des hébergeurs, car ils doivent avoir une capacité - en terme de bande passante, de stockage et de traitement – importante. Le pilotage et la supervision de millions de machines zombies nécessite des ressources importantes et un niveau de compétence technique élevé.

(5) La communication entre les machines zombies et les serveurs de contrôle et de commande est effectuée selon un protocole propre au botnet, qui peut être éventuellement crypté.

(6) Une attaque par déni de service consiste à rendre indisponible un service internet en le saturant de demandes de connexion. On parle d'une attaque par déni de service distribué si un grand nombre de machines participe à cette opération, ce qui est toujours le cas pour un botnet. On pourra citer par exemple l'attaque menée en décembre 2010 par le groupe Anonymous contre les sites de Paypal, Visa et Mastercard, lors de l'affaire Wikileaks, et qui a été largement médiatisée.

(7) La fraude au clic consiste à effectuer de manière automatisée des clics sur des liens publicitaires, ce qui remet en cause le modèle économique des liens sponsorisés, qui est très populaire sur Internet. On estime que plus de 20% des clics sur les liens publicitaires sont d'origine frauduleuse.

Modèle de la campagne de spam

```
From: "<firstname> <lastname>" <<firstname><lastname><randomnumber>@<<randomdomain>.<randomtld>>
To: <recipient>
Subject: Watches Rolex. <rate>% off

Lux for cheap. with <rate>% Off
View... <url>
```

Génération des spams

Spam #1

```
From: "Dusty Mayo" <DustyMayo1460829@brasilinspired.com>
To: <xxxxxx.xxxx@xxxxxxxx.xxx>
Subject: Watches Rolex. 85% off

Lux for cheap. with 85% Off
View... http://fixedfeeble.com/
```

Spam #2

```
From: "Amanda Boggs" <AmandaBoggs99@recipeflower.net>
To: <xxxxxxxxx@xxxxxxxxx.xxx>
Subject: Watches Rolex. 66% off

Lux for cheap. with 66% Off
View... http://fixdefeeble.ru/
```

Exemple de génération de spams à partir d'un modèle de campagne

Ces activités peuvent être exercées pour le compte du botmaster, mais dans la plupart des cas elles sont vendues comme une prestation à d'autres acteurs : industriels de la contrefaçon [8], organisations criminelles...

Prenons l'exemple classique du spam :

1. Une organisation souhaite proposer à la vente des contrefaçons (montres de prestige, produits de luxe...).
2. Elle contacte le botmaster, et lui demande d'envoyer une campagne publicitaire à grande échelle. Le botmaster joue donc le rôle de prestataire de service pour le routage des emails : il fournit - contre rémunération [9] - les moyens techniques d'envoi ainsi que les carnets d'adresses des destinataires.
3. La campagne de spam est envoyée, avec une volumétrie souvent considérable [10]. Du fait des moyens techniques mis en œuvre pour limiter le spam, un pourcentage assez faible atteindra le destinataire final, et le taux de transformation sur le site de contrefaçon sera d'autant réduit. Toutefois, la volumétrie considérable en amont – souvent plusieurs millions voire milliards d'emails - lié au coût quasi-nul en terme d'infrastructure – le coût financier étant à la charge des propriétaires des machines zombies - font que ce modèle reste très rentable.

(8) La contrefaçon concerne principalement les montres de prestige, les produits de luxe, les médicaments - dont le fameux Viagra - et l'édition logicielle.

(9) Les prix sont variables, et dépendent surtout de la qualité du carnet d'adresses. On estime que l'envoi d'un million de spams coûte en moyenne moins de 100$ pour le client.

(10) On a estimé par exemple la capacité d'envoi quotidienne du botnet Rustock à environ 30.000.000.000 d'emails. C'est un volume considérable, et cela donne la mesure de la dangerosité des botnets.

4. L'organisation qui vend les contrefaçons reçoit par la suite un grand nombre de commandes, qu'elle pourra choisir d'honorer ou pas : si elle honore la commande, elle enverra donc la contrefaçon au client et crée ainsi une relation commerciale classique ; si elle ne l'honore pas, elle utilise les données bancaires capturées pour un autre usage.
5. L'argent gagné par l'organisation vendant des contrefaçons restant dans un cadre illégal, elle devra le blanchir. A ce titre, elle pourra encore une fois utiliser les services proposés par le botmaster en envoyant une campagne d'emails pour recruter des *money mules* [11]. Une money mule est une personne physique acceptant - contre forte rémunération - d'effectuer des opérations bancaires pour le compte d'une entreprise : ces opérations bancaires permettent à l'entreprise de blanchir des sommes d'argent, et la money mule prend à son insu toutes les responsabilités légales relatives à cette opération.

```
From: alexis luong [mailto:downsj@cableone.net]
Sent: Tuesday, 5 February 2011 11:37 PM
To: xxxxxxx xxxxxxx
Subject: start your career with us

Welcome to the Arcandor Service!

We are very glad that you wish to join our team, will be delighted to have you work with us. The
position of Assistant provides support filling the transactions of our customers.

We deal exclusively with private clients- that have special requirements for high speed of
receiving funds for their business.

This way we can offer a new kind of financial and banking service to our clients - and we would
like you to work as an Assistant (part-time job 3-4 hours a day except holidays).

At first your work would be very basic, yet meticulous -you will make transfers for our clients to
suit their needs. Our managers will assist you during the trial period and explain everything you
will need to know.

We offer an extremely competitive graduated salary: for the first month you will receive up to
$2000 for your work the next month your salary will be increased if you do your work accurately and
on time.

Now you are only one step away from successful career.

All you need is to send an e-mail to: arcandorservice2@gmail.com

With phone numbers and times to reach you, and one of our representatives will contact you and
answer all your questions.

Thank you in advance,

Helen Jones
Manager
Arcandor Service
```

Exemple d'email de recrutement d'une money mule

(11) A noter que le terme de *mule* désigne dans le langage courant une personne transportant de la drogue d'un pays à l'autre, et parfois à son insu.

Mort d'un botnet

Étant donné le rôle essentiel donné aux serveurs de contrôle et de commande, le démantèlement d'un botnet passe par la mise hors service de ces derniers, et cette opération nécessite une intervention des autorités auprès des sociétés hébergeant les serveurs de contrôle et de commande.

On pourra ainsi citer le cas du botnet Bredolab, qui le 25 octobre 2010, a été fortement affaibli suite à la saisie par les autorités hollandaises de 143 serveurs auprès de l'hébergeur hollandais LeaseWeb. Toutefois, le botnet est toujours en vie, grâce à la présence d'autres serveurs de contrôle et de commande en Russie et au Kazakhstan.

Autre exemple: le botnet Grum, qui a été complètement démantelé en juillet 2012, avec des opérations menées conjointement par les autorités en Hollande, au Panama et en Ukraine.

La capacité à mettre hors service un botnet est par conséquent principalement conditionnée par la bonne volonté des autorités des pays où sont hébergés les serveurs de contrôle et de commande : la problématique n'est plus d'ordre technique, mais d'ordre juridique et politique.

A propos de Vade Secure

Vade Secure est le leader reconnu de la lutte, à base d'une technologie de filtre heuristique, contre les phishing, spear-phishing, malware et ransomware. Indépendant du langage, le filtre analyse individuellement les emails dans leur globalité (méthode d'envoi, liens, pièces jointes, contenu…) pour détecter toutes les menaces, même les attaques très ciblées en zero-day. Vade Secure complète son offre avec des solutions innovantes de gestion du graymail. La classification automatique des emails ainsi que la désinscription en 1 clic permettent aux utilisateurs de gérer leur boite de réception très simplement.

Protégeant plus de 400 millions de boîtes aux lettres dans plus de 76 pays, nos solutions sont utilisées par les plus grands FAI, OEM et entreprises. Vade Secure est implanté dans 5 pays (USA, Canada, France, Hong Kong et Japon) pour assurer un support 24/7.