LE TEMPS

Wikileaks 18:53

Cinq hackers, trois serveurs et un réseau planétaire de serveurs relais

Par Mehdi Atmani

Les explications techniques de l'affaire des câbles diplomatiques

■ Comment procède WikiLeaks?

Le noyau central de WikiLeaks est principalement géré par cinq hackers (pirates), tous nomades comme Julian Assange. Ils travaillent à distance sur des ordinateurs portables. De leur position, ils alimentent trois serveurs – l'infrastructure matérielle – du site WikiLeaks.org. Le principal est hébergé en Suède. Le second en Belgique. Le dernier, dont le lieu est tenu secret, permet l'accès aux informations. WikiLeaks utilise ensuite un réseau planétaire de serveurs relais pour fonctionner tout en anonymisant ses sources.

Seuls les cinq pirates ont accès à l'ensemble de la structure (les trois serveurs). Toutes les communications et documents sont cryptés. Pour se contacter, les pirates ont constitué une variante du système de communication Tor, un procédé garantissant l'anonymat en ligne. Il est composé d'un logiciel (programme qui permet le traitement de l'information par ordinateur) et d'un réseau de serveurs cachant toutes les informations qui pourraient permettre d'identifier l'utilisateur et le localiser. L'information est ainsi transmise en toute sécurité d'un émetteur A au destinataire B.

■ Le réseau secret SIPRNet

Les 251 287 câbles diplomatiques proviennent tous du réseau Secret Internet Protocol Router Network, ou SIPRNet. Ce système de réseau internet, né après le 11 septembre 2001, permet aux employés des Départements d'Etat et de la Défense américains de se communiquer des informations potentiellement sensibles. Un document diplomatique marqué du sceau SIPDIS est automatiquement téléchargé sur le site confidentiel de son ambassade. De là, il peut être consulté depuis un ordinateur connecté à SIPRNet.

Seuls les membres de l'armée américaine, en possession d'un mot de passe levant le niveau de classification «secret», y ont accès. Le soldat américain Bradley Manning par exemple, fortement suspecté d'avoir transmis à WikiLeaks les 250 000 câbles diplomatiques. Un nombre croissant d'ambassades américaines s'est rattaché à SIPRNet ces dernières années. A partir de 2002, 125 ambassades étaient sur le réseau sécurisé. Elles étaient 180 en 2005. Aujourd'hui, la grande majorité des missions américaines dans le monde sont sur SIPRNet.

■ WikiLeaks, victime de cyberattaques

Plusieurs jours après la publication des documents diplomatiques, le site cablegate.wikileaks.org est la cible d'attaques informatiques. Elles visent à paralyser le serveur qui héberge le site. Pour les hackers, le jeu est simple: il s'agit d'inonder la plate-forme de connexions et demandes simultanées d'informations qui le met à plat.

Ces attaques classiques sont appelées DDOS (Distributed Denial of Service). Elles sont possibles lorsque l'attaquant mobilise, durant l'offensive, des ordinateurs du monde entier dans lesquels a été implanté un petit programme pirate baptisé «Cheval de Troie». Sans nous en rendre compte, l'attaque peut utiliser notre ordinateur comme rampe de lancement pour atteindre sa cible. Dans le cas du serveur de WikiLeaks, elle revenait à lui demander environ 150 fois par seconde le téléchargement des 400 000 pages complètes du dossier irakien de l'organisation de Julian Assange.

Mais wikileaks.org n'a pas flanché. S'il était impossible de s'y connecter dans la nuit du 2 au 3 décembre, c'est que le fournisseur de service américain EveryDNS.net a retiré le nom de domaine WikiLeaks.org, par peur de problèmes sur le fonctionnement de son infrastructure informatique.

■ Adresses IP, noms de domaine et sites miroirs

Tout fournisseur de contenu sur le Net dispose d'une adresse IP (une succession de chiffres). C'est le numéro internet des utilisateurs, comme il existe des numéros de téléphone. Plusieurs sociétés, dont EveryDNS.net font correspondre un nom de domaine à ces chiffres: 192 168 143.687 pour Le Temps.ch par exemple. Dans le cas de WikiLeaks, c'est le lien entre le chiffre et le nom qui a été rompu. Il a fallu près de six heures au site pour constater la panne et rebondir. Il a donc développé des plates-formes miroirs – qui hébergent l'exact contenu du site mère – au bénéfice d'un nouveau nom de domaine. C'est de cette manière que WikiLeaks.org a disparu pour renaître en .ch, .be.

Les noms de domaines .org, .com, .net et .uk sont centralisés. Ils sont tous gérés par l'Icann (Internet Corporation for Assigned Names and Numbers), une société américaine. Elle supervise la création de nouveaux noms et les assigne à différents groupes. Par exemple, l'extension .com est administrée par la compagnie américaine VeriSign, alors que .uk est géré par la société Nominet UK. La centralisation de ces noms de domaine est une arme redoutable contre WikiLeaks, qui n'a pas d'autre choix que de trouver des extensions de noms annexes. Mais la multiplication de sites miroirs permet de compliquer la censure. A ce rythme, le jeu entre hackers ennemis peut durer encore longtemps.