

INFORMATIQUE

Cinq jours après la fermeture du site de téléchargement Megaupload, les hackers multiplient les attaques contre les institutions et les grandes entreprises comme Vivendi.

Anonymous poursuit l'offensive sur le Web

La liste des victimes s'allonge. Après avoir piraté les sites du FBI, du département américain de la Justice et d'Universal Music, le collectif de « hackers » - combinaison de hackers et activistes - Anonymous continue de faire des dégâts sur Internet. Il vient d'inscrire à son tableau de chasse les sites Web de l'Élysée, du ministère de la Défense, de « L'Express » et de Vivendi. Ce dernier était indisponible pendant une bonne partie de la journée, hier, alors que dans le même temps, des documents financiers publics (rapports annuels, communiqués...) du groupe circulaient sur le Web. La rumeur a même enflé sur un éventuel blocage des réseaux sociaux Facebook et Twitter, avant d'être rapidement démentie par le collec-

tif : les pirates utilisent en effet ces réseaux sociaux pour s'exprimer.

Ces attaques font suite à la fermeture jeudi soir, sur ordre du FBI, de la plate-forme de téléchargement et de partage de fichiers Megaupload, et à l'arrestation de ses principaux dirigeants. Elles s'inscrivent toutefois dans un mouvement de contestation plus général, après les initiatives prises par le Parlement américain pour limiter le piratage sur Internet, avec les projets de loi SOPA et PIPA, soutenus par Hollywood et les grandes maisons de disques. « Il s'agit davantage d'une volonté de défendre le cyberspace contre la tentative de régulation des gouvernements que de la simple défense de Megaupload et de ses fondateurs, à la réputation controversée

dans le milieu », décrypte Frédéric Bardeau, auteur du livre « Anonymous, pirates ou altermondialistes numériques » (FYP éditions). Dans ce contexte, la France et la loi Hadopi font figure de cibles naturelles pour les hackers.

Manifestation à Paris

Ces attaques ne sont pas véritablement dangereuses. Mais leur succession et la rapidité avec laquelle elles sont menées surprennent. La méthode utilisée reste classique : il s'agit d'attaques de déni de services (DDOS), qui consistent à envoyer depuis un réseau d'ordinateurs infectés des centaines de milliers de requêtes sur les sites visés afin de les rendre indisponibles. La nouveauté vient de la mise à disposition des

liens nécessaires pour installer ces logiciels malveillants, afin de permettre aux internautes « militants » de « mener le combat » aux côtés des hackers. « L'efficacité des attaques dépend du nombre de machines qui y participent », explique Renaud Bidou, de la société de sécurité Deny All.

Le phénomène pourrait s'amplifier. « Ce n'est que le début, pronostique Frédéric Bardeau. On assiste à une forme de démocratisation du hacking, comme en témoignent le nombre et la diversité des personnes enrôlées dans ce genre d'attaques. » Le collectif français des Anonymous a prévu d'organiser une manifestation, début mars, dans les rues de Paris.

ROMAIN GUEUGNEAU

Déni de service, défiguration, intrusion : les trois armes des cyber-attaques

Les moyens de se défendre existent. Ils coûtent cher. L'invulnérabilité ne peut être assurée

Conséquence du coup de filet musclé contre le site de téléchargement Megaupload, le 19 janvier, nombre de sites web ont subi, en représailles, des cyber-attaques ces derniers jours. Elles sont attribuées à la nébuleuse des « Anonymous », qui protestent contre ce qu'ils considèrent être une atteinte aux libertés de l'Internet.

En fin de semaine dernière, aux États-Unis, ils s'en sont pris aux sites du FBI ou de la maison de disque Universal. En France, ceux de l'Élysée ou de l'hédomadaire *l'Express* ont été perturbés. Celui de Vivendi, maison mère d'Universal, est resté inaccessible 48 heures et n'a été remis en service que mardi 24 janvier au soir.

Comment ces activistes agissent-ils ?

Le « déni de service » C'est l'attaque la plus courante, la plus facile à mettre en œuvre. Il s'agit de rendre un site indisponible, en obstruant son réseau d'accès avec des paquets d'informations trop lourds, ou en saturant ses serveurs avec un flot de requêtes. « *Quelques requêtes mal formatées, incomprises des serveurs, suffisent aussi* », note Pascal Lointier, président du Clusif (Club de la sécurité de l'information français). La plupart des dénis sont « distribués » : un grand nombre d'ordinateurs, souvent enrôlés automatiquement, s'en prennent simultanément à une même cible. Internet regorge de fichiers pour planifier ces offensives.

C'est ce qui est arrivé au site de *l'Express*, « planté » une heure et demi, lundi 23 janvier, à la suite des propos de son directeur de la rédaction Christophe Barbier, qui reprochait aux Anonymous d'agir masqués. « *C'est une action imbécile, mais pas très grave. Nous envisageons de porter plainte* », assurait, mardi, Eric Mettoux, rédacteur en chef du site.

« *Certains pirates utilisent cette technique pour faire du chantage. Ils menacent de planter un site de paris en ligne la veille d'une grosse journée et réclament de l'argent* », selon Renaud Bidou, de l'éditeur de logiciels de sécurité Deny All.

La « défiguration » de sites Les pirates parviennent à prendre le contrôle de pages web, et en modifient le contenu. C'est ce qui est arrivé à l'Élysée, vendredi 20 janvier. Un bref moment, d'étranges messages (« *Sarko, le peuple aura ta peau*... ») sont apparus dans la barre de navigation du site.

« *Certains préfèrent, quand ils font l'objet d'une attaque, fermer leur site plutôt que de risquer une défiguration, c'est peut-être ce qui s'est passé avec Vivendi* », relève M. Bidou. Le groupe n'a pas souhaité s'exprimer.

L'intrusion C'est la technique la plus élaborée et potentiellement la plus dangereuse. Les pirates parviennent à percer le système d'information des entreprises. Souvent par le site web, partie la plus vulnérable.

« *Les pirates ne veulent surtout pas que le site tombe, pour en tirer le maximum d'informations* », selon M. Bidou. La motivation ? Espionnage industriel, appât du gain ? A priori, ce sont moins les motivations des Anonymous.

Les contre-attaques possibles Face à un déni, un site peut demander à son hébergeur d'identifier l'adresse « IP » des machines hostiles (identifiant sur internet) : les requêtes qu'elles envoient sont alors rejetées par les pare-feu des serveurs. Difficile à mettre en œuvre quand il

y a trop de machines. « *On peut aussi allouer une nouvelle adresse IP au site, pour que les requêtes ratent leur cible* », ajoute M. Lointier.

Contre la « défiguration » ou l'intrusion, les éditeurs spécialisés vendent des « pare-feu » en tous genres, souvent basés sur le comportement des internautes, pour détecter les anomalies.

Tout cela a un coût. « *Se protéger en permanence d'un déni coûte 10 000 euros, puis 2 000 euros annuels de maintenance* », précise M. Bidou. « *On nous a proposé une solution radicale pour contrer l'attaque, à 10 000 euros, c'est trop cher pour nous* », témoigne M. Mettoux. Même protégé, « *aucun site n'est invulnérable* », prévient M. Lointier, le combat est inégal. ■

CÉCILE DUCOURTIEUX