Une cyberattaque paralyse le Web

Que sait-on de la cyberattaque ayant paralysé de nombreux sites internet ? Qu'est-ce que la cybercriminalité ? Quels sont les moyens mis en œuvre en France pour y faire face ?

- **Comment s'est déroulée la cyberattaque ?**

Vendredi 21 octobre 2016, une cyberattaque de masse, menée en plusieurs vagues, a perturbé le fonctionnement d'Internet privant des millions d'internautes, principalement américains, d'accès à de nombreux sites tels que Twitter, Spotify, Amazon, eBay, Reddit, Airbnb, Netflix, Paypal mais aussi les sites de plusieurs médias (CNN, New York Times, Boston Globe, Financial Times, The Guardian...).

Aucun de ces sites internet n'était cependant directement visé par l'attaque informatique. En effet, les pirates ont ciblé spécifiquement la société américaine Dyn qui fournit des services de gestion de noms de domaine (Domain Name System – DNS). Concrètement, le serveur DNS transforme un nom de domaine (www.siteweb.fr), tapé par l'internaute dans son navigateur, en instructions techniques lui permettant de se connecter au site désiré. Ce service est crucial pour le bon fonctionnement du Web car sans cet aiguillage, les sites internet sont inaccessibles.

Cette cyberattaque a pris la forme d'un « déni de service distribué » (Distributed Denial of Service - DDoS). Elle a saturé artificiellement le serveur DNS de la société Dyn en le surchargeant de requêtes ou en accaparant ses ressources jusqu'à épuisement, ce qui a rendu une partie du Web difficile, voire impossible, à atteindre.

Pour saturer ce DNS, les pirates ont eu recours à un réseau de machines zombies elles-mêmes piratées et utilisées à l'insu de leurs propriétaires (des «botnets»). Ainsi, des dizaines de millions d'objets connectés (webcams, caméras de surveillance, enregistreurs numériques, thermostats, imprimantes ...) ont été infectées par un virus malveillant qui, une fois déclenché par les pirates, leur ont fait multiplier les demandes de connexions simultanément, ce qui a saturé le réseau à l'est des Etats-Unis et au Texas avant de toucher l'ouest du pays.

Il semblerait qu'une partie des objets connectés impliqués dans l'attaque était pilotée par Mirai, logiciel déjà utilisé pour plusieurs attaques similaires ces dernières semaines. Ce logiciel profite de failles présentes dans certains objets connectés pour s'y introduire (ex : le mot de passe, défini lors de la fabrication du produit, n'a pas été changé par l'utilisateur). Une fois infecté, l'objet est piloté à distance. En outre, ce virus a la faculté de se propager de façon autonome à des objets connectés présentant les mêmes vulnérabilités.

- **Que sait-on des auteurs de l'attaque informatique ?**

Le FBI s'est saisi de l'affaire, conjointement avec le département de la sécurité intérieure (DHS). L'identité et l'origine géographique des auteurs demeurent encore inconnues. Cependant, plusieurs théories circulent quant aux auteurs de l'attaque.

JURIS AUXILIUM
2 Rue des Amidonniers
31000 Toulouse

Le site Wikileaks, qui a publié des milliers d'emails du directeur de campagne d'Hillary Clinton, candidate démocrate à la présidentielle, a cru déceler dans cette attaque une marque de soutien à son fondateur Julian Assange, réfugié dans l'ambassade d'Equateur à Londres et dont l'accès à Internet a été récemment coupé. « *Julian Assange est toujours en vie et Wikileaks continue de publier. Nous demandons à nos soutiens d'arrêter de bloquer l'internet américain. Vous avez été entendus* », a tweeté le site.

D'autres mettent en cause le groupe de hackers Anonymous qui a tweeté : « *Le toit, le toit, le toit est en feu. Nous n'avons pas besoin d'eau. Laissez l'enfoiré brûler* ».

James Scott, expert en cybercriminalité de l'Institute for Critical Infrastructure Technology, trouve des similitudes avec des attaques menées en décembre 2015 par des cyber-djihadistes à l'aide de 18 000 appareils mobiles.

Enfin, Bruce Schneier, grand spécialiste américain de la sécurité informatique, estime qu'en raison de la sophistication et de la précision de l'attaque, un pays qui aurait intérêt à déstabiliser l'économie américaine, tel que la Chine ou la Russie, pourrait en être l'auteur. Selon lui, cette attaque pourrait n'être qu'un test avant une offensive plus importante qui viserait à paralyser des pans entiers de l'économie comme la finance, le pétrole ou l'électricité...

- **<u>En quoi cela inquiète les autorités</u> ?**

Quelle qu'en soit l'origine, l'attaque a mis en lumière les dangers posés par l'utilisation croissante des objets connectés. En effet, les fabricants d'équipements connectent leurs objets à Internet, les rendant ainsi « intelligents ». Toutefois, lorsque ces appareils comportent des failles informatiques majeures, ceux-ci deviennent vulnérables et peuvent être utilisés par des pirates, à l'insu de leurs propriétaires, au profit d'une cyberattaque.

Ben Johnson, ex-hacker pour l'agence de renseignement NSA et co-fondateur de la société de sécurité informatique Carbon Black prédit que : «*Les attaques par déni de service, en particulier avec l'essor d'objets connectés non sécurisés, vont continuer à harceler nos organisations. Malheureusement, ce que nous voyons n'est que le début en termes de botnets à grande échelle et de dommages disproportionnés* ».

Le 10 octobre 2016, le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques français (CERT-FR), qui dépend du secrétariat général de la défense nationale, recommandait la plus grande prudence lors de l'installation de tels objets : « *Les logiciels embarqués dans ces objets [connectés] peuvent contenir des vulnérabilités, ou présenter des défauts de configuration permettant d'en prendre le contrôle. Si ces objets sont connectés directement sur Internet, ils peuvent représenter des cibles faciles pour des attaquants qui pourront les utiliser […] comme vecteur d'attaque*. ».

Aujourd'hui, ce sont des millions d'appareils, intelligents mais dangereux, qui se retrouvent sur le marché. La cyberattaque, qui s'est abattue le vendredi 21 octobre sur le Web américain, intervient en pleine recrudescence d'attaques informatiques et autres actes de piratage aux Etats-Unis et dans les autres pays industrialisés.

JURIS AUXILIUM
2 Rue des Amidonniers
31000 Toulouse

Ainsi, Yahoo a récemment reconnu avoir été victime d'une vaste attaque, il y a deux ans, qui avait compromis les données personnelles de 500 millions de ses utilisateurs. Plusieurs attaques ont également visé le secteur financier et certaines banques centrales, conduisant les pays industrialisés du G7 à adopter, mi-octobre, une série de règles de protection.

- **Qu'est-ce que la cybercriminalité ?**

À l'heure où Internet est omniprésent, jusqu'à s'immiscer dans nos objets connectés du quotidien, et que le Dark Web monte en puissance, la cybercriminalité s'impose comme « la menace du XXIe siècle » et pose un défi d'une ampleur inégalée aux autorités.

La cybercriminalité apparaît comme une nébuleuse, d'autant plus difficile à cerner qu'elle renvoie à des procédés techniques essentiellement évolutifs maîtrisés par les seuls initiés.

En juin 2013, un groupe de travail interministériel[i] chargé de faire des propositions en matière de lutte contre la cybercriminalité a été constitué. Cette initiative faisait suite au séminaire gouvernemental sur le numérique du 28 février 2013 et s'inscrivait, plus généralement, dans la stratégie définie au plan européen, le 7 février de la même année. Le groupe de travail interministériel a remis son rapport le 30 juin 2014, aux ministres Christiane Taubira, Arnaud Montebourg et Bernard Cazeneuve et à la secrétaire d'Etat au Numérique Axelle Lemaire.

Tout comme les instruments internationaux, le droit français ne donne aucune définition de la cybercriminalité. Suite à ce constat, le groupe de travail a proposé de clarifier cette notion en mettant en exergue Internet comme le principal système concerné par la cybercriminalité : « *La cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet* ».

Ce concept recouvre :

- Les infractions dirigées contre le système d'information lui-même : les attaques contre les systèmes automatisés de traitement de données (intrusion, entrave, altération ou destruction de données)[ii] ; les atteintes portées aux libertés individuelles par le biais de traitements automatisés de données à caractère personnel[iii] ; des infractions dites "préventives" relatives, par exemple, au commerce, à la fabrication et à la diffusion non autorisés d'outils logiciels destinés à de telles activités illégales, notamment la cryptologie.

- Les infractions de droit commun commises au moyen de ces nouvelles technologies de l'information et de la communication : l'utilisation de telles technologies pour véhiculer des contenus illicites (images de pédopornographie, apologie de crimes contre l'humanité ou du terrorisme, provocation à la haine raciale, à la xénophobie, au négationnisme, au révisionnisme…)[iv] ; l'utilisation de ces technologies en tant que moyen permettant de faciliter la commission de toute autre infraction (terrorisme, proxénétisme, atteintes à la vie privée, injures et menaces, infractions à la législation sur les stupéfiants, escroqueries, falsifications et usages de cartes de paiement contrefaites, atteintes au secret professionnel, atteintes à la propriété intellectuelle et aux droits d'auteur...).

JURIS AUXILIUM
2 Rue des Amidonniers
31000 Toulouse

- **<u>Quels sont les moyens mis en œuvre en France pour y faire face</u> ?**

Avec les États-Unis et l'Allemagne, la France est l'un des pays précurseurs dans la lutte contre la cybercriminalité. L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) a été créé en 2001 par le ministère de l'Intérieur. Elle est l'une des premières structures d'un vaste réseau international dont l'objectif est de garantir une réponse coordonnée face aux cybermenaces.

En France, l'action face à la cybercriminalité est coordonnée par le ministère de l'Intérieur, où le rôle de Jean-Yves Latournerie est de coordonner les différents services. La police judiciaire dispose d'une division spéciale, la Sous-direction de lutte contre la cybercriminalité (SDLC). Depuis avril 2014, elle remplace et étend l'action de l'OCLCTIC. Quatre-vingts policiers et gendarmes y travaillent pour surveiller le Web afin d'identifier et anticiper les cybermenaces. Elle prend en compte aussi bien les attaques subies par les entreprises que celles des particuliers.

De plus, plusieurs plateformes de signalement ont été mises en place : la Plate-forme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements (PHAROS) qui permet de signaler les contenus et comportements illicites rencontrés sur internet ; la plateforme téléphonique d'information et de prévention sur les escroqueries sur Internet qui est destinée aux victimes ou aux potentielles victimes d'escroqueries et qui leur permet de recevoir des conseils en termes d'information et de prévention ; le numéro INFO ESCROQUERIE[v] mis en place pour renseigner le public ou signaler une tentative d'escroquerie.

En outre, le rapport remis par le groupe de travail interministériel formule 55 recommandations pour une réponse répressive plus efficace et mieux adaptée aux nouvelles méthodes des cyberdélinquants tout en respectant les libertés fondamentales. Parmi les points essentiels développés par le rapport, figure la prévention de la cybercriminalité. Pour la renforcer, les membres préconisent notamment le lancement de campagnes de sensibilisation destinées au grand public, la formation de l'internaute (premier acteur de sa propre sécurité) et la mobilisation de tous les professionnels concernés pour trouver des réponses techniques appropriées. Pour les auteurs de ce rapport, il apparaît également nécessaire de renforcer les moyens de lutte contre la cybercriminalité. Plusieurs dispositions sont proposées pour parvenir à cette fin : la mise en place d'un centre d'alerte et de réaction aux attaques informatiques ; un renforcement de la formation des magistrats, des policiers, des gendarmes et des douaniers ; ainsi que la création d'une délégation interministérielle et d'une Mission au sein du ministère de la Justice.

MP

JURIS AUXILIUM
2 Rue des Amidonniers
31000 Toulouse

[i] Ce groupe de travail interministériel a été constitué par les ministres de la Justice, de l'Economie et des finances, de l'Intérieur, ainsi que la ministre déléguée chargée des petites et moyennes entreprises, de l'innovation et de l'économie numérique.
Le groupe de travail interministériel se composait notamment d'avocats généraux à la Cour de cassation, de responsables du ministère public, de policiers, de gendarmes et de douaniers. Il était présidé par le procureur général près la Cour d'appel de Riom, Marc Robert. Ils avaient pour objectif d'élaborer une stratégie globale de lutte contre la cybercriminalité intégrant notamment les questions de prévention et de sensibilisation des publics, afin de contribuer à créer un espace de confiance sur Internet.

[ii] Articles 323-1 s. du Code pénal français.

[iii] Articles 226-16 s. du Code pénal (dispositions résultant de la Loi n° 78-17 du 6 janvier 1978, dite Loi Informatique et libertés).

[iv] Notamment, le protocole additionnel du 7novembre 2002 à la Convention de Budapest.

[v] Numéro INFO ESCROQUERIE : 0 805 805 817.

JURIS AUXILIUM
2 Rue des Amidonniers
31000 Toulouse