**Sélection du mois de décembre 2014**

***Quelle est la réelle capacité de nuisance des Anonymous?***

Entre les cyberattaques issues des réseaux criminels, qui ont pour l'exemple coûté 62 millions de dollars à Home Dépôt selon les estimations des dirigeants, ou bien celle menée contre Sony, piratant cinq films non sortis en salle dont la Corée du Nord est vraisemblablement à l'origine, et les attaques des Anonymous, un pas n'a pas encore été franchi.

Jusqu'à présent, les cyberattaques de « contestation » de ce groupe n'ont pas eu d'autres effets que de bloquer un site internet par la technique du déni de service, dite aussi attaque en Ddos. Elle consiste à submerger un site de demandes, produit une saturation du système et donc le blocage du site. Lors de la contestation du barrage de Sivens, les Anonymous ont bloqué une trentaine de sites institutionnels du Tarn. Ils ont également saturé à plusieurs reprises le site du ministère de la Défense et celui de l'Andra pour protester contre le projet Cigéo d'enfouissement des déchets nucléaires. Il n'y a pas à proprement parler de grand péril. A chaque fois, ce n'est pas le système informatique interne qui est bloqué en lui-même, mais la façade Internet, celle où ne vont finalement que les particuliers. Les attaques des Anonymous sont, pour l'instant, plus symboliques qu'autre chose.

***Volonté ou capacité ?***

Ce serait plus grave, cependant, si le site visé était celui d'un groupe d'e-commerce et pourtant les Anonymous ne s'y risquent pas. Anonymous, qui conteste régulièrement les méthodes de management appliquées aux employés du groupe Amazon n'a jamais bloqué l'accès à la plate-forme en ligne dont les conséquences financières pourraient être très importantes pour l'entreprise. Tout récemment, pendant les fêtes de Noël, alors que l'activité du site Amazon battait son plein de commandes, une action a été menée. Elle a consisté en un appel au boycott du site. Les activistes ont invité les consommateurs à ne pas faire leurs achats sur la plate-forme en ligne et à se diriger vers des sites plus « éthiques » en terme de salaires, notamment, dont ils fournissaient la liste, mais cette mobilisation a été, somme toute, marginale.

Soit les Anonymous n'ont pas les capacités de hacking pour véritablement nuire à l'entreprise ou à l'Etat visé, soit ce n'est pas leur motivation. C'est surtout à eux que leurs cyberattaques profitent en leur donnant une visibilité médiatique allant très certainement au delà de leur réelle capacité de nuisance. Il ne s'agit là que d'une forme virtuelle de manifestation en somme. Le danger des cyberattaques pour une entreprise ne vient pas d'eux, mais bien des réseaux criminels ou des services de renseignements des Etats. Suite à l'arrestation d'un jeune homme de 19 ans par Scotland Yard en 2011, présenté comme le porte-parole du collectif, arrestation qui avait suivi une interpellation de 21 personnes présumées membres, Anonymous avait lancé une opération de blocage de PayPal où le collectif affirmait que 35000 comptes avaient été clôturés. Mais PayPal a annoncé n'avoir constaté aucun changement particulier dans ses opérations (Zdnet, 28/07/14). En 2010, Anonymous avait plusieurs fois attaqué PayPal, Visa et Mastercard afin de soutenir WikiLeaks. Ils avaient également bloqué en 2010 le service de jeux de ligne de Sony et viennent de réitérer en

décembre de cette année, provoquant le mécontentement des joueurs qui viennent de s'offrir leurs consoles. Pour autant rien ne permet d'affirmer que les Anonymous sont derrière cette attaque massive que Sony Picture vient de subir et qui a été attribuée à la Corée du Nord, mais il n'est pas impossible qu'ils s'agrègent à cette action.

***De l'opposition à l'intrusion***

Dernièrement, les cyberattaques menées par les Anonymous sont devenues plus intrusives. Les sites ne sont plus seulement bloqués. Des informations y sont récoltées. En décembre 2014, un collectif de hackers, Opantirep, utilisant la bannière Anonymous a piraté des bases de données de sites de la police et de la gendarmerie française et italienne. Une attaque en Ddos a provoqué l'indisponibilité du site du syndicat Alliance de la police française et le collectif a fournit une capture d'écran comme preuve du piratage du site Internet dédié aux réservistes de la gendarmerie où les noms, adresses e-mails, adresses IP et mots de passe de quelque 2000 membres ont « fuité ». Le calendrier de positionnement et de relève des unités CRS dans le cadre des missions permanentes jusqu'à la fin de l'année 2014 en France a pu être récupéré par les activistes (Numérama, 24/11/14). Reste à savoir le bénéfice qu'ils peuvent tirer de ces informations. A priori pas grand-chose, sauf s'ils revendent les données, mais est-ce vraiment là leur motivation ? Il serait tout de même judicieux que la sécurité informatique de tels sites soit revue de manière à éviter que des informations cette fois-ci confidentielles ne soient « aspirées ». En 2011, après une série d'interpellations par le FBI de membres présumés de ce collectif, ce dernier revendiquait une attaque informatique sur le réseau de l'OTAN où 1Go de données avaient été piratées et, notamment, des documents classifiés confidentiels. Alors que l'OTAN n'avait pas communiqué sur l'authenticité des documents, les Anonymous ont fait savoir que, hormis les deux fichiers mis en ligne pour prouver leur intrusion, aucune divulgation massive des documents ne serait réalisée, jugeant « *irresponsable* » un tel acte (Zdnet, 21/07/11). En revanche, le collectif vient de revendiquer un piratage de données concernant le mandat de Moncef Marzouki (Tunisie) qui, si elles sont authentifiées, impliqueraient que cet ancien chef d'Etat rende des comptes à la justice, en particulier, concernant des factures assez importantes (Businessnews, 22/11/14).

***L'heure de vérité***

Les Anonymous ont annoncé sur Twitter leur intention de riposter après l'attentat au siège de Charlie Hebdo. Les sites relayant cette annonce font part de potentielles attaques contre certains comptes Twitter de prêcheurs radicaux ou de sites islamistes. Toutefois, il ne pourra s'agir que de blocages temporaires et les sites islamistes, dont certains en France ont déjà été fermés par les services de renseignement, arrivent régulièrement à réouvrir sur d'autres hébergeurs.

Toute la difficulté d'appréciation de la menace est liée à la structure même de ce mouvement hacktiviste : horizontalité et absence de hiérarchie. N'importe quel hacker peut agir sous son nom. C'est donc une bannière sujette à la manipulation et, pour certains, les Anonymous sont une création de la CIA pour mener des campagnes clandestines « False Flag », sous le couvert de l'activisme politique (blog conscience du peuple, 04/05/12).