Cybersécurité : la France dans le Top 5 des puissances du mal

Cocorico ? Selon l'éditeur américain FireEye, la France figure **dans le top 5 des pays d'où émanent les cyberattaques**. Un classement en nette progression, même si, évidemment, il n'y a guère lieu de s'en réjouir. Pour David de Walt, le Pdg de l'éditeur de passage à Paris, l'Hexagone apparaît comme une parfaite plate-forme pour ce faire. Et d'énumérer différentes raisons dont le cadre législatif, la disponibilité d'une solide infrastructure Internet ou de « *faibles barrières à l'immigration* » (sic). Pour le Pdg de FireEye, si la France fait figure avant tout de relais dans des opérations offensives, mais elle n'en intègre pas moins le Top 5 des pays où les activités malveillantes sont les plus importantes, derrière les Etats-Unis, la Chine, la Russie et la Corée du Sud.

Cette montée en puissance de l'Hexagone est assez symptomatique de que David de Walt perçoit comme **une course aux armements dans le cyberespace**. « *Sur les 204 pays aujourd'hui impliqués dans des activités de cyberespionnage et de cybercrime, 50 nations ont acquis un niveau leur permettant de lancer des opérations de type militaire sur Internet* », assure le Pdg. Pour qui il ne s'agit pas là d'une surprise : « *si vous examinez l'histoire de l'Humanité, vous vous apercevez que chaque champ nouveau – la mer, l'air – a amené des conflits* ». Pour lui, l'Internet, du fait de la faiblesse de sa régulation, est même un environnement idéal pour que les puissances se défient. « *C'est la parfaite plate-forme du mal* », résume David de Walt. Une expression qu'on dirait tout droit sortie de la bouche de Georges W. Bush…

Sabotages : déjà plus de la science-fiction

Le dirigeant définit 4 niveaux de danger relatifs au cyberattaques. Le premier, le cybercrime, est bien connu. Dave de Walt met tout de même en lumière des formes moins popularisées, comme le ciblage d'individus susceptibles de détenir des informations utiles sur les marchés financiers. En France toutefois, le premier secteur ciblé – et totalisant environ un quart des attaques recensées par l'éditeur contre les entreprises de l'Hexagone – est plutôt la grande distribution, qui demeure mal protégée. Le second niveau est, lui aussi, bien identifié, et recouvre toutes les activités de cyberespionnage. « *Le fait nouveau, c'est que certains états ciblent désormais des entreprises privées* », précise le dirigeant. Enfin, David de Walt isole deux autres types de menaces, « *celles qui me font le plus peur* » : le cybersabotage et le cyberterrorisme. Le premier n'est d'ores et déjà plus de la science-fiction comme l'ont montré les attaques dévastatrices subies par Sony Pictures ou par la chaîne de casinos et d'hôtels Sands début 2014. « *Et il y en a eu d'autres qui ne sont pas parvenues jusqu'aux oreilles des média* », précise de Walt, qui estime que **9 attaques significatives sur 10 restent confidentielles**.

Les formes les plus dangereuses de cyberterrorisme, autrement dit des actions initiées dans le cyberespace et ayant un effet dans le monde réel, restent du domaine de la science-fiction (c'est notamment le scénario du film Hacker de Michael Mann, qui sort sur les écrans ce 18 mars). Mais jusqu'à quand ? Car, FireEye constate que les capacités à mener ce type d'attaques existent déjà, notamment en raison des **faiblesses des systèmes Scada**, contre lesquels plusieurs attaques

réussies sont désormais connues (Lire à ce sujet notre article : Sécurité des Scada : pourquoi la côte d'alerte est atteinte). « *Notre système bancaire tout entier, notre système énergétique, le transport aérien… Tout cela repose sur Internet et n'est pas très sûr. Ce qui manque pour qu'on assiste à ce type d'attaques, c'est plutôt un assaillant extrêmement motivé* », dit David de Walt, qui explique que sa société décèle l'activité de groupes explorant les possibilités offertes par les attaques de Scada. Sans que cela se concrétise forcément par un passage à l'acte. « *Mais il y a aussi le risque qu'un accident se produise, créant une panne géante dans une infrastructure*, ajoute le Pdg. *De nombreux acteurs explorent le cyberespace et testent les possibilités offertes par les Bios, les disques durs ou les OS* ». Avec le risque qu'un malware échappe à son créateur.

FireEye explique que la majorité des serveurs de contrôle et commande utilisés pour piloter des attaques contre des systèmes tiers émanent de serveurs tournant sur des plates-formes des plus officielles. David de Walt assure que 75 % d'entre eux sont hébergés par des acteurs des plus reconnus. « *Amazon est ainsi la première plate-forme d'hébergement d'activités malfaisantes dans le monde* ».

A lire aussi :

FIC 2015 : les hackers ont gagné une bataille, pas la guerre
Selon FireEye, 184 pays sont déjà engagés dans la cyberguerre
Cyber-espionnage : les Etats-Unis mouillent la Chine pour faire oublier la NSA

crédit photo © GlebStock – Shutterstock