Europol prédit une vague de cybercrimes par objets connectés

Le Centre européen sur le cybercrime (EC3) d'Europol a dressé un bilan de la cybercriminalité dans son rapport iOCTA (Internet Organised Crime Threat Assessment) 2014. Plusieurs enseignements sont à tirer de cette enquête.

Le premier est que la cybercriminalité se démocratise au point que cette activité devient un service. De plus en plus de pirates proposent des méthodes pour contourner, éprouver ou s'introduire sur des sites. Ce modèle de « **Crime as a service** » casse les barrières à l'entrée de ce marché le rendant plus accessible à des groupes manquant traditionnellement de compétences techniques.

Les objets connectés un futur eldorado du cybercrime

Et ce modèle service peut aller loin notamment en direction des objets connectés. Cette démocratisation fait craindre à Europol que **le premier meurtre** via le piratage de ces objets se déroulera avant **la fin de l'année 2014**. Une analyse empruntée à une autre étude d'une firme américaine IID qui prévoyait-elle qu'une vague de cybermeurtres arriverait dans les deux prochaines années.

Cette crainte n'est pas formalisée, mais les scénarios existent et ont été démontrés dans des conférences sur la sécurité. On pense notamment au piratage à distance d'un pacemaker de l'expert en sécurité Barnaby Jack avec comme objectif de modifier le niveau des impulsions et ainsi faire mourir le patient. Cet exemple peut être transposé aux pompes à insuline, aux défibrillateurs, etc. Sur ce dernier point, l'ancien vice-président des États-Unis, Dick Cheney a indiqué dans une récente interview avoir désactivé la connectivité sans fil de son stimulateur cardiaque. Europol indique dans son rapport, « *l'Internet des objets représente un nouveau vecteur d'attaque et tout ce que nous considérons comme criminels travaillent pour l'exploiter* ». D'autres scénarios impliquent la voiture connectée ou autonome que le FBI a considéré comme une arme létale si elle venait à être piratée.

L'Internet caché se développe fortement

Un autre enseignement est la montée en puissance de l'« **Internet caché** » qui regroupe à la fois des solutions d'**anonymisation (Tor, etc)**, le **chiffrement**, mais également l'usage des **monnaies virtuelles** comme Bitcoin. Les darknets sont devenus des lieux de trafics illégaux comme les drogues, les armes, les médicaments, mais aussi les documents d'identité ou des contenus pédopornographiques. Par ailleurs, ils sont l'endroit pour s'échanger des exploits et notamment des failles concernant les objets connectés.

Enfin dernier élément d'analyse, l'EC3 d'Europol constate que l'Internet caché pose un vrai défi au droit européen. La plupart des sites ou des hébergements opèrent en dehors de l'UE dans des pays

qui ne disposent pas d’outils juridiques ni de compétences suffisantes pour les arrêter.