

La CyberMenace jihadiste grandit



La
CyberMenace
jihadiste
grandit

Un cyber-attentat de grande ampleur, qui causerait des dégâts physiques ou même des morts, n'est peut-être pas encore à la portée des groupes jihadistes mais cela pourrait changer sous peu et il faut s'y préparer, estiment des spécialistes.

D'autant qu'ils sont déjà en mesure de trouver, auprès de hackers et de mercenaires de l'ère digitale prêts à tout pour de l'argent, les capacités techniques qui leur manquent pour utiliser internet pour autre chose que de la propagande et du recrutement, ajoutent-ils.

« Daech (acronyme arabe du groupe État islamique), Al Qaïda, tous les groupes terroristes aujourd'hui : nous avons le sentiment que pour l'instant, ils ne disposent pas des compétences offensives cyber », déclare à l'AFP Guillaume Poupard, directeur de l'Agence nationale des systèmes d'information (ANSSI).

« Ces compétences sont compliquées à acquérir, même si ce n'est pas l'arme atomique. Avec quelques dizaines de personnes, un petit peu d'argent mais pas tant que ça, il y a la possibilité d'être efficace. Ils pourraient monter en compétence. Nous avons le sentiment que pour l'instant ils n'y sont pas. Ils ont d'autres soucis, et c'est compliqué pour eux », ajoute-t-il à Lille, où il a participé mercredi au 9e Forum international de la Cybersécurité.

« Les voir à court terme mener des attaques informatiques avec des impacts majeurs, on n'y croit pas trop. En revanche ça pourrait changer très vite. Notre vraie crainte, et on y est peut-être déjà, c'est qu'ils utilisent les services de mercenaires. Ce sont des gens qui feraient tout et n'importe quoi pour de l'argent », ajoute-t-il.

– Inscrit dans l'ADN –

Ce recours par des groupes jihadistes à des sous-traitants informatiques pour monter des cyber-attentats (mise en panne de réseaux électriques, paralysie de réseaux de transport ou de systèmes bancaires, prise de contrôle de sites ou de médias officiels, sabotage à distance de sites industriels critiques, par exemple), le directeur d'Europol, Rob Wainwright, l'évoquait le 17 janvier à Davos.

« Même s'il leur manque des savoir-faire, ils peuvent aisément les acheter sur le darknet (partie d'internet cryptée et non référencée dans les moteurs de recherche classiques qui offre un plus grand degré d'anonymat à ses utilisateurs, ndlr), où le commerce d'instruments de cyber-criminalité est florissant », estimait-il lors d'une table ronde intitulée « Terrorisme à l'âge digital »...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRIEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article