# Les entreprises de l'énergie attaquées par des pirates chinois

L'opération *Night Dragon* bat son plein. Démarrée en novembre 2009, voire dès 2007 selon McAfee, cette opération ce traduit aujourd'hui par des **attaques répétées et coordonnées contre une douzaine de grandes entreprises du secteur de l'énergie** basées en occident. Cinq multinationales ont clairement été identifiées mais leurs noms restent confidentiels. Il s'agirait essentiellement d'organisations opérant dans le secteur pétrolier et gazier. BP, ExxonMobil, Chevron… elles ne sont pas si nombreuses. Mais, certaines étant clientes de McAfee, l'éditeur s'en tient aux règles de confidentialités habituelles. Tout en déclarant avoir prévenus les autorités de sécurité américaines, le FBI au premier plan.

Les attaques visent essentiellement à **dérober des informations spécifiques et des données technologiques**. Du pur espionnage industriel, en apparence, qui tend à dédouaner les organisations criminelles habituellement purement motivées par l'appât du gain. Selon l'éditeur de sécurité, des gigaoctets de données d'informations sensibles auraient été dérobés, notamment dans les secteurs des projets financiers.

**Tous les regards se tournent vers la Chine**. *« Les outils, les techniques et les activités du réseau utilisé dans ces attaques proviennent principalement de Chine*, écrit **George Kurtz**, directeur technique chez McAfee. *Ces outils sont largement disponibles sur les forums Internet chinois et ont tendance à être largement utilisés par les pirates chinois. »* On ne peut être plus clair.

Les attaques sont multiformes et leurs auteurs utilisent des techniques variées comme le *social engineering*, le phishing ciblé, l'exploitation des failles de sécurité Windows, la compromission des annuaires d'entreprise Active Directory. Des outils d'administration à distance sont également exploités. Des outils standards de gestion basés sur des informations d'identification administrative classiques. Ce qui, selon McAfee, leur permet d'**échapper aux outils de vérification et politiques de sécurité habituels des entreprises**. *« Les techniques d'intrusion que nous évoquions en 1999 […] fonctionnent toujours une décennie plus tard »*, note George Kurtz. Effrayant!

**Ce n'est pas la première fois que la Chine est montrée du doigt** en matière d'attaques d'entreprises américaine. Début 2010, Google avait dénoncé des tentatives d'intrusion sur son système d'information, notamment, et menacé de quitter le territoire (une initiative à laquelle la firme renoncera finalement). Reste à savoir si ces attaques en provenance de l'empire du Milieu est le fait d'initiatives privées ou gouvernementales.

*« Les faits indiquent que **l'activité pirate chinoise est organisée**, ainsi [elle est] potentiellement dirigées soit par le secteur privé ou par le secteur public*, déclare au *Wall Street Journal* **Dmitri Alperovitch**, vice président de l'unité recherche antivirale chez McAfee. *Mais c'est impossible pour moi de savoir lequel de ces secteur avec certitude. »* De son côté, la Chine dément toute tentative d'attaques. *« La Chine a des lois très strictes contre les activités de piratage, et la Chine est également victime de telles activités »*, justifie **Wang Baodong**, porte-parole de l'ambassade de Chine à Washington.

Pour sa part, McAfee propose un livre blanc visant à aider les entreprises à se prémunir contre les

charges du « dragon nocturne ».