Symantec dévoile les activités des hackers chinois de Hidden Lynx

Selon un rapport de Symantec, un groupe de 50 à 100 hackers professionnels opérant depuis la Chine est à l'origine d'une vague d'attaques informatiques visant des entreprises, des gouvernements ou des organisations militaires depuis au moins 2009.

Ce groupe, appelé **Hidden Lynx**, serait notamment à l'origine de l'opération Aurora, qui en 2010 a ciblé des dizaines de très grandes entreprises, dont Google et Microsoft, ou, en 2012, de l'attaque contre le spécialiste de la sécurité Bit9, une opération qui visait in fine les clients américains de Bit9 dans la défense.

Une équipe d'élite et des soldats

Selon Symantec, plus de la moitié des attaques menées par ce groupe concernent des entreprises basées aux États-Unis. Hidden Lynx ayant une attirance pour des cibles dans le complexe militaro-industriel, la finance, l'éducation, les instances gouvernementales, la chaîne logistique ou l'ingénierie.

Symantec relève que le groupe a accès à un arsenal sophistiqué, y compris des failles zero-day. Selon l'éditeur, le groupe serait subdivisé en deux équipes : une équipe d'élite, aux rangs resserrés, ayant accès aux outils les plus sophistiqués (comme le **Troyen Naid** utilisé lors d'Aurora ou une faille zero-day Oracle utilisée cette année pour une attaque au Japon) et une équipe composée de hackers moins pointus, dédiée avant tout aux attaques à grande échelle.

Selon **Kevin Haley**, directeur du Symantec Security Response, cite par nos confrères de *Computerworld*, il n'existe aucune preuve que Hidden Lynx soit directement soutenu par l'État chinois. Et de noter que certaines cibles des hackers sont elles-mêmes basées en Chine. Pour Symantec, le groupe apparaît davantage comme une organisation louant ces services à des entreprises ou des États.

Voir aussi
Quiz Silicon.fr – Crimes et châtiments sur Internet