"Hacktivistes" et cyberguerriers, les nouveaux visages du crime sur le net

Technologie

Posté par: Visiteur

Publié le : 07-01-2011 23:05:35

Avec des attaques de type Stuxnet ou l'affaire Wikileaks, internet a vu en 2010 émerger de nouveaux profils de criminels : des "hacktivistes" aux motivations idéologiques ou cyberguerriers cherchant à semer le chaos, dont les actions devraient encore s'intensifier cette année

"Il y a dix ans, nous avions surtout à gérer des cybervandales qui ne cherchaient qu'à pénétrer les systèmes d'information pour jouer avec ce qu'ils y trouvaient. Nous assistons aujourd'hui à l'éclosion de nouvelles menaces sous la forme de cyberterrorisme", résume Eugene Kaspersky, président de la société de sécurité informatique Kaspersky Lab, dans une récente analyse. "On est passé d'un gamin bricolant dans un garage à des groupes professionnels et organisés", renchérit François Paget, "chercheur de menaces" chez le concurrent McAfee. Mais l'année 2010 "a vu un changement radical : la percée des +hacktivistes+" (contraction de "hacker" --pirate informatique-- et d'"activiste" --militant). Leurs motivations sont "idéologiques ou politiques, et plus du tout financières", souligne-t-il.

Dans l'affaire Wikileaks, des pirates informatiques du groupe "Anonymous" ont ainsi mené des attaques contre le site des cartes de crédit Visa et Mastercard, qui avaient rompu leurs liens d'affaires avec le site diffusant des télégrammes secrets américains, en soutien à son fondateur Julian Assange. Autre exemple de cybermilitantisme, en mai après le raid d'Israël contre une flottille d'aide humanitaire à destination de Gaza, des sympathisants palestiniens s'en sont pris à des sites israéliens et ont piraté des comptes Facebook pour protester contre l'opération. Les Etats se sont aussi invités en 2010 dans la cybercriminalité, menant "sous couvert d'+hacktivisme+ une forme de cyberguerre", affirme François Paget, interrogé par l'AFP. Baptisées "menaces persistantes avancées", ces attaques de cyberespionnage ou de cybersabotage ciblées "sont menées avec l'approbation ou sous la direction d'un Etat autoritaire ou corrompu", indique-t-il. Et de citer l'exemple, il y un an, d'un piratage de Google pour laquelle "la Chine a été pointée du doigt". Mais l'opération qui a le plus marqué les esprits en 2010 est Stuxnet, du nom d'un virus qui a touché cet automne des infrastructures sensibles, en particulier en Iran. Il se propageait via Windows et ciblait plus particulièrement des logiciels de la firme Siemens contrôlant des automates industriels. "Si la piste +étatique+ est établie, il n'y a pas d'information pointant un Etat plutôt qu'un autre", ajoute M. Paget. "Qui est derrière ça ? On n'en a aucune idée, pourquoi pas Greenpeace ? Israël ? ou l'Iran lui-même ?", s'interroge pour sa part Laurent Heslault, qui estime qu'il y a "clairement un +avant+ et un +après+ Stuxnet : c'est une arme de cybersabotage". En 2011, "l'objectif poursuivi par les créateurs de programmes malveillants et les organisateurs d'attaques sera clairement l'obtention d'informations et la lutte d?influence", prévient Jean-Philippe Bichard, analyste chez Kaspersky Lab. A l'avenir, "cyberguerre, cyberguerilla ou cyberterrorisme, le but sera toujours politique. Cela va aller toujours plus loin : ce ne sera plus seulement de la +gesticulation+, mais des attaques d'infrastructures critiques pour provoquer le chaos", prédit Laurent Heslault.
afp.com