Laurent Heslaut (Symantec): «Stuxnet est le H1N1 des virus informatiques»

« Il y aura clairement un avant et un après Stuxnet, lâche **Laurent Heslault**, directeur des techniques de sécurité pour Symantec Europe de l'Ouest. *C'est la première fois que l'on voit un tel développement, une telle complexité. Il pèse 600 Ko [contre 20 à 30 Ko habituellement pour ce type de malware, NDLR]. Trois personnes travaillent dessus à plein temps chez Symantec. »* Stuxnet n'a pas seulement défrayé la chronique en s'attaquant à des centrales nucléaires iraniennes. Pour le responsable sécurité, il constitue la troisième vague de menaces informatique.

Après les *script kiddies* des années 90, et l'appat du gain avec la génération des maliciels en tout genre (du simple virus au phishing en passant par le logiciel espion) des années 2005, voici les menaces « hacktivistes» initiées en 2007 avec l'attaque des infrastructures informatiques de l'Estonie. *« Les motivation ont changé*, confirme Laurent Heslault sans néanmoins remettre en cause le dynamisme des cyber-criminels « traditionnels ». *Le cyberespace constitue le nouveau terrain de guerre. »* Ce n'est pas le Lieutenant-Colonel Régis Fohrer qui le contredira. Pour ce dernier, la cyberguerre a déjà commencé.

Des infrastructures critiques mal protégées

Un constat d'autant plus inquiétant que les infrastructures critiques sont mal protégées. Ainsi, 53 % des entreprises chargées de les exploiter reconnaissent avoir subi des attaques ou ont rencontré des problèmes de nature informatique, selon Symantec. *« Les infrastructures techniques de ces sites ne sont pas les mêmes que les infrastructures de bureau, et ce ne sont pas les mêmes équipes*, explique le porte-parole de Symantec qui ajoute que *les systèmes sont « arrêtés » sur de vieux OS [Windows 2000 notamment, NDLR] particulièrement vulnérables car non patchés. »* Cela s'explique par le caractère critique des opérations à gérées, souvent liées à la fourniture d'énergie, des systèmes que l'on modifie le moins possible pour éviter au maximum un incident informatique qui entrainerait un arrêt de service.

Plus grave, *« le protocole Scada commence à être discuté sur les forums underground. »*. Scada (pour Supervisory Control And Data Acquisition ou télésurveillance et acquisition de données) est un dispositif de contrôle qui permet de piloter à distance un site industriel, notamment les centres de production ou de distribution d'énergie (électricité, gaz) et de gestion de l'eau. La prise de contrôle d'un tel site par des cyber-criminel pourrait vite tourner au cauchemar pour les autorités (et les populations) d'un pays. *« Ce sont des environnements censés être clos et pourtant, ils sont connectés à Internet. »*

Point positif de l'affaire, Stuxnet pourrait se révéler comme le catalyseur des nouvelles menaces. *« Stuxnet est le H1N1 du virus informatique*, s'amuse Laurent Heslault, *il pousse les entreprises à se poser des questions sur la sécurité de leur site. »* Laquelle concerne le système d'information et tous les périphériques qui s'y rattachent (y compris les photocopieurs) aux politiques d'accès des locaux.

Consumerisation de l'IT et l'IT–ization du grand public

S'il est aujourd'hui difficile d'éradiquer Stuxnet, les technologies actuelles permettent néanmoins de s'en protéger. *« On peut imaginer qu'un ver de type Stuxnet pourrait être arrêté par les technologies de réputation de Norton [qui classe les sites selon un niveau potentiel de dangerosité, NDLR]. »* Technologies de réputation qui vont glisser des applications grand public vers les solutions destinées aux entreprises en 2011. Ce que **Eric Soares**, récemment nommé à la direction générale Europe de l'Ouest de l'éditeur de sécurité, résume par *« la consumerisation de l'IT et l'IT–ization du grand public »*. Autrement dit, l'effacement de la frontière entre les usages privés et professionnels dans des environnements mouvant où la mobilité prend une place toujours plus grande.

Autant d'évolutions des usages dont il faut assurer la sécurité, que ce soit au niveau de la protection des données, des postes de travail, la gestion des identités, la sécurisation du cloud, etc. Une sécurisation de bout en bout à laquelle Symantec, aidé en 2010 par des acquisitions majeures (Verisign, GuardianEdge et PGP), entend aujourd'hui être en mesure de répondre intégralement.