# Recrudescence des cas d'espionnage et de vol de données - onzième rapport de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information

Date de mise en ligne : mardi 2 novembre 2010

- Informatique - Sécurité Informatique -

**Spyworld Actu**

**Les affaires d'espionnage et de vol de données ont augmenté au premier semestre 2010 sur le plan mondial. Bien souvent, des sites Web ou des réseaux sont piratés à cet effet. De telles intrusions servent également à répandre des logiciels malveillants ou à mener des attaques à connotation politique. La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) emploie depuis cette année un nouvel outil servant à identifier les sites Web suisses infectés. En outre, elle peut désormais faire bloquer les domaines « .ch » pour protéger les adresses Internet suisses contre les abus.**

La soustraction de données est commise soit par des escrocs mus par l'appât du gain, soit dans le cadre de l'espionnage étatique. Les entreprises économiques et les services publics s'avèrent des cibles de choix.

**Espionnage en vogue**

Des géants des technologies de l'information et de la communication comme Google ou le fabricant de logiciels Adobe ont été victimes d'actes d'espionnage ciblés au premier semestre 2010. De tels incidents présentent, au niveau des infrastructures, des similitudes frappantes que l'on aurait tort d'attribuer au hasard. On est plutôt enclin à croire qu'un seul agresseur est à l'origine de tous ces incidents.

**Contrôle par MELANI des sites suisses infectés**

Des sites Web continuent d'être infectés, dans le but de causer du tort à des internautes inconscients d'un tel risque. Les méthodes les plus fréquentes pour manipuler les sites Web et y introduire des maliciels consistent à utiliser des données d'accès FTP dérobées (mot de passe et nom d'utilisateur) afin d'accéder au serveur Web, ou à utiliser les vulnérabilités des applications Web. MELANI exploite depuis avril de cette année un outil de contrôle servant à vérifier si les sites en « .ch » sont infectés. Lors d'un premier bilan, portant sur les mois de juin à août 2010, MELANI a identifié 148 sites infectés sur quelque 237 000 sites contrôlés.

**Blocage des domaines « .ch » suspects**

Si une adresse Internet suisse est soupçonnée de servir à accéder à des données sensibles ou à diffuser des logiciels malveillants, un blocage s'impose. Depuis sa révision partielle en début d'année, l'ordonnance sur les ressources d'adressage dans le domaine des télécommunications (ORAT) offre les bases légales pour une telle intervention. SWITCH, le registre gérant les noms de domaine « .ch », est habilité à bloquer les adresses Internet suisses et à supprimer l'assignation y relative à un serveur de noms, en cas de soupçon fondé d'abus et si un service de lutte contre la criminalité reconnu par l'Office fédéral de la communication (OFCOM) en a fait la demande. Le 15 juin dernier, MELANI a été agréé comme tel par l'OFCOM et peut dès lors proposer à SWITCH de bloquer un domaine.

- Rapport semestriel 2010/1

*Post-scriptum :*

http://www.melani.admin.ch/dienstle...