Les hackers privilégient le «drive-by download»

Les hackers privilégient le «drive-by download»

Les cybercriminels sont constamment à la recherche de possibilités d'infecter les appareils, selon un rapport paru jeudi.

MELANI a observé une augmentation des attaques contre des sites Web au deuxième semestre 2015. Les criminels sont constamment à la recherche de possibilités d'infecter commodément un maximum d'appareils de victimes potentielles.
Dans son rapport semestriel, publié jeudi, la Centrale d«enregistrement et d'analyse pour la sûreté de l«information (MELANI) constate que si les hackers privilégiaient par le passé l'envoi de courriels, qui demande peu de connaissances techniques, c'est désormais le «drive-by download» qui a la cote: il consiste à propager des logiciels malveillants (maliciels) à grande échelle, à travers des sites web très fréquentés.
Les portails des journaux et les réseaux publicitaires sont les cibles préférées des escrocs, explique MELANI. Une infection chez un fournisseur de contenu publicitaire peut se révéler lourde de conséquences, en infectant plus loin de nombreux sites clients.

Familles de maliciels

Au deuxième semestre de l'année dernière, l'extorsion est restée une des méthodes favorites des cybercriminels afin d'obtenir des gains rapides. Les familles de maliciels de cryptages sont toujours plus nombreuses, avertit MELANI. Les attaques DDoS (déni de service distribué), qui visent à rendre des sites inaccessibles pour ensuite exiger une rançon, se sont multipliées en 2015.
Les criminels choisissent avant tout des entreprises qui dépendent de l'accès à leur site Internet, car elles sont plus faciles à faire chanter. Sous la menace d'une éventuelle perturbation de l'accès à leur site, certaines sont prêtes à mettre la main au porte-monnaie. «Mais en payant, elles donnent aux hackers les moyens financiers pour renforcer leur infrastructure d'attaque et intensifier leurs actions», souligne la centrale.

En 2015, MELANI a ouvert le site «antiphishing.ch», qui permet à chacun de signaler des sites de hameçonnage. Quelque 2500 sites ont été dénoncés la première année. A côté du phishing par usage abusif du logo de l'administration fédérale, constaté plusieurs fois, le recours au phishing à l'aide de fichiers PDF est en recrudescence: au lieu d'un lien HTML, le courriel contient un fichier .pdf en annexe, qui lui-même incite à cliquer sur un lien malveillant.

Zurich et Valais

Comme au premier semestre 2015, Zurich et le Valais affichent au deuxième semestre un taux d«infection par habitant supérieur aux autres cantons. «Alors qu'à Zurich ce résultat tient à la forte densité d«ordinateurs, les raisons du taux d'infection élevé en Valais ne sont pas connues à l'heure actuelle», écrit MELANI dans son rapport.
Consultable en ligne, ce document permet de découvrir les innombrables techniques développées par les cybercriminels pour gagner de l'argent illégalement, et suggère des moyens pour se prémunir d'une attaque.
(ats)… [Lire la suite]

Réagissez à cet article

1. Source : *Les hackers privilégient le «drive-by download» – Tribune de Genève – l’actualité en direct: politique, sports, people, culture, économie, multimédia*