Les PDF piégés toujours d'actualité

Baptisé « Neosploit », ce **kit d'outil pour pirates** a attiré l'attention des chercheurs de **l'US CERT** (US Computer Emergency Response Team) et de Secure Computing. Ce kit, dont la presse traite sous forme de retour en force (*Neosploit's back*), est capable de faire **tomber les sécurités des fichiers pdf.**

Des « exploits » particulièrement **dangereux** car ils cataloguent les utilisateurs infectés et choisissent de ne les **attaquer qu'une seule fois,** ce qui rend plus difficile pour les fabricants de repérer la source des attaques et d'empêcher d'autres infections. De plus, la nouvelle mouture de cet exploit dispose de **nouveaux composants ajoutés à des systèmes d'attaque existants**. Les chercheurs avaient pourtant déjà repéré ce kit d'exploit en juillet dernier, les premières traces remontant même en **2007**, Neosploit faisait alors partie du pack d'exploits appelé **WebAttacker**.

Secure Computing considère la menace comme sérieuse du fait de la popularité du format pdf : « *Le PDF (Portable Document Format) est l'un des formats de fichiers de prédilection pour de nombreuses entreprises actuelles, à cause de l'étendue de son déploiement sur différents systèmes d'exploitation.****L'inconvénient est que ce format est affecté par des vulnérabilités connues*** *et largement exploitées*« .

Une popularité qui s'ajoute au fait que le kit permettrait selon certains spécialistes de faire tomber la licence officielle Adobe.

Les principales recommandations pour s'en protéger restent les mêmes. L'US-CERT recommande que les utilisateurs se **protègent de ces attaques** en évitant les **téléchargements de fichiers à risque ou non sollicités,** qu'ils proviennent d'Internet ou de leurs e-mails.