G Data Communiqué de presse 2010

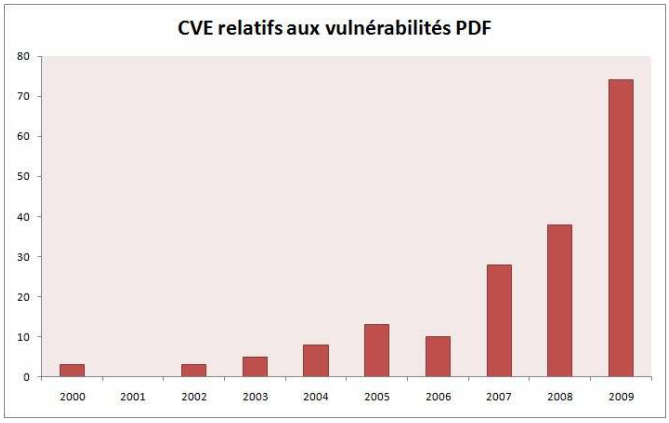
Vulnérabilité 0 Day d'Adobe Reader
Pourquoi les failles PDF se multiplient-elles ?

Paris, le 11 janvier 2010 – Une vulnérabilité importante affectant les logiciels PDF d'Adobe sera corrigée le 12 janvier. G Data saisie cet évènement pour faire un point sur les techniques d'attaques impliquant des fichiers PDF. Une pratique très à la mode chez les cybercriminels.

La faille de sécurité (CVE-2009-4324) rapportée le 15 décembre 2009 par l'éditeur Adobe sur ses logiciels Adobe Reader et Adobe Acrobat sera bientôt de l'histoire ancienne : une mise à jour prévue pour le 12 janvier corrigera cette vulnérabilité. Le délai important pour cette correction restera une des situations marquantes de la fin 2009. G Data profite de cet évènement pour faire un point complet sur les attaques exploitant le format PDF.

Malware PDF, une tendance à la hausse

L'analyse du nombre de vulnérabilités PDF découvertes durant ces dernières années montre une croissance importante. En 2009, l'organisme MITRE (http://cve.mitre.org) a recensé 74 CVE (Common Vulnerabilities and Exposures) relatives aux PDF dans son dictionnaire relatif aux vulnérabilités de sécurité. Soit deux fois plus qu'en 2008 !



Pourquoi une telle croissance ?

Plusieurs avantages font du Portable Document Format (PDF) l'un des fichiers les plus couramment utilisé aujourd'hui. Il peut tout d'abord être affiché sur tous les ordinateurs. Beaucoup de lecteurs PDF gratuits et d'outils de personnalisation sont ensuite disponibles. Des atouts qui se révèlent très attractifs pour les utilisateurs privés, les entreprises et les administrations. Mais Au fil de ses évolutions, les possibilités de ce format de fichier ont augmenté, et avec elles sa complexité. Une situation qui facilite aujourd'hui l'exploitation de failles de sécurité. Beaucoup d'outils d'exploit automatiques, tels qu'Eleonore, Liberty Exploit System ou Elfiesta, peuvent créer des PDF infectés, sans qu'aucune connaissance ne soit requise par le cybercriminel.

Déroulement d'une attaque PDF

Les attaques exploitant les vulnérabilités PDF sont variées. Une des plus courantes se déroule comme ceci :

1. Un Javascript intégré dans un PDF infecté est exécuté à l'ouverture du document. Ce fichier nuisible est obfusqué et donc invisible lors d'une analyse manuelle du PDF.
2. Le Javascript noie alors les blocs mémoires (méthode du Heap-Spraying) par la multiplication des commandes NOP (commande de non opération) et par le chargement de shellcode.
3. La vulnérabilité Javascript dans le PDF peut alors être exploitée pour exécuter le shellcode.
4. Le Shellcode exécuté télécharge alors le malware additionnel, par exemple un composant botnet.

Comment se protéger ?

Equiper son ordinateur d'une solution de sécurité est une démarche importante. Les utilisateurs des solutions G Data étaient, et sont, protégés contre les attaques exploitant la faille 0 Day d'Adobe.
La désactivation de la fonction Javascript dans les programmes d'Adobe doit aussi être effectuée. Sur Adobe Reader, elle se réalise à partir du menu Edition => Préférences. Dans la catégorie JavaScript il suffit de décocher « Activer Acrobat JavaScript ». L'activation de la fonction DEP (Data Execution Prevention) est une autre possibilité. Disponible dans les systèmes Windows, cette option permet d'interdire l'exécution de codes malveillants dans les zones mémoire de l'ordinateur. Mais de nombreux logiciels demeurent incompatibles avec cette protection.

Pour toute question :
Jérôme Granger - G Data Software AG
Tél. : 01 41 48 51 46 – mob. 06 08 77 32 26 – e-mail : jerome.granger@gdata.fr