

G-Data : Pourquoi les failles PDF se multiplient-elles ?

S curit 

Post  par : JerryG

Publi e le : 11/1/2010 15:00:00

Une vuln rabilit  importante affectant les logiciels PDF d  Adobe sera corrig e le 12 janvier. G Data saisie cet  v nement pour faire **un point sur les techniques d  attaques impliquant des fichiers PDF**. Une pratique tr s   la mode chez les cybercriminels.

La faille de s curit  (CVE-2009-4324) rapport e le 15 d cembre 2009 par l  diteur Adobe sur ses logiciels Adobe Reader et Adobe Acrobat sera bient t de l histoire ancienne : une mise   jour pr vue pour le 12 janvier corrigera cette vuln rabilit . Le d lai important pour cette correction restera une des situations marquantes de la fin 2009. G Data profite de cet  v nement pour faire un point complet sur les attaques exploitant le format PDF.



Malware PDF, une tendance   la hausse

L analyse du nombre de vuln rabilit s PDF d couvertes durant ces derni res ann es montre une croissance importante. En 2009, l'organisme MITRE (<http://cve.mitre.org>) a recens  74 CVE (Common Vulnerabilities

and Exposures) relatives aux PDF dans son dictionnaire relatif aux vuln rabilit s de s curit . 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 utilis  aujourd hui. Il peut tout d abord  tre affich  sur tous les ordinateurs. Beaucoup de lecteurs PDF gratuits et d outils de personnalisation sont ensuite disponibles. Des atouts qui se r v lent tr s attractifs pour les utilisateurs priv s, les entreprises et les administrations. Mais Au fil de ses  volutions, les possibilit s de ce format de fichier ont augment , et avec elles sa complexit .

Une situation qui facilite aujourd hui l exploitation de failles de s curit . Beaucoup d outils d exploit automatiques, tels qu Eleonore, Liberty Exploit System ou Elfiesta, peuvent cr er des PDF infect s, sans qu aucune connaissance ne soit requise par le cybercriminel.

D  roulement d  une attaque PDF

Les attaques exploitant les vuln  abilit  s PDF sont vari  es. Une des plus courantes se d  roule comme ceci :

1. Un Javascript int  gr   dans un PDF infect   est ex  cut      l  ouverture du document. Ce fichier nuisible est obfusqu   et donc invisible lors d  une analyse manuelle du PDF.

2. Le Javascript noie alors les blocs m  moires (m  thode du Heap-Spraying) par la multiplication des commandes NOP (commande de non op  ration) et par le chargement de shellcode.

3. La vuln  abilit   Javascript dans le PDF peut alors   tre exploit  e pour ex  cuter le shellcode.

4. Le Shellcode ex  cut   t  l  charge alors le malware additionnel, par exemple un composant botnet.

Comment se prot  ger ?

  quiper son ordinateur d   **une solution de s  curit   est une d  marche importante.** Les utilisateurs des solutions G Data   taient, et sont, prot  g  s contre les attaques exploitant la faille 0 Day d  Adobe. La d  sactivation de la fonction Javascript dans les programmes d  Adobe doit aussi   tre effectu  e.

Sur Adobe Reader, elle se r  alise    partir du menu Edition => Pr  f  rences. Dans la cat  gorie JavaScript il suffit de d  cocher   « Activer Acrobat JavaScript   ». L  activation de la fonction DEP (Data Execution Prevention) est une autre possibilit  . Disponible dans les syst  mes Windows, cette option permet d  interdire l  ex  cution de codes malveillants dans les zones m  moire de l  ordinateur.

Mais de nombreux logiciels demeurent incompatibles avec cette protection.