Attaques sur les fichiers PDFs

Introduction

Les fichiers PDFs sont un vecteur d'attaque intéressant.

Ils sont tout d'abord très utilisés, par des millions de personnes, et sont disponibles sur les trois systèmes d'exploitation utilisateurs majeurs: Windows, MacOS, et (GNU/)Linux.

En lui-même, le PDF est un fichier de présentation. Il vise à transmettre des informations données sous une forme visuelle donnée. Ainsi, son format est complexe, car il décrit précisément l'organisation visuelle des différents éléments: texte, police, encadrés, couleurs, ...
Il peut usuellement inclure des images, et pour les versions les plus riches[1], des vidéos, des pistes sonores, ou des modèles 3D[2]. Enfin, un fichier PDF peut contenir des formulaires (basés notamment HTML ou XML)[3], et même, pour encore plus d'interactivités, peut exécuter du code en Javascript.

Cette richesse accroît la surface d'attaque sur le format en lui-même.
Cela permet également, comme il sera illustré par la suite (!!!), une certaine créativité pour l'attaquant.

Pour analyser et faire un rendu de ce format complexe, les fichiers PDFs sont lus et affichés par des lecteurs appropriés. Le lecteur est ainsi un vecteur d'attaque supplémentaire. Les lecteurs de PDFs doivent être capable de comprendre un format complexe, ce qui accroît les possibilités d'erreur d'implémentation.

Enfin, les PDFs, de part leur universalité d'utilisation, proposent d'encrypter un document, ou de le signer numériquement (avec une signature digitale). Ces services de sécurité présentes sont également sujets à des attaques.

Ce document se concentre ainsi sur les:

- Attaques sur le format PDF
- Attaques sur les lecteurs de PDF
- Attaques sur les services de sécurité associés à un fichier PDF

Attaques sur le format PDF

Attaques sur les lecteurs de PDF

Attaques sur les services de sécurité associés à un fichier PDF

[1] https://helpx.adobe.com/fr/acrobat/using/rich-media.html
[2] https://fr.wikipedia.org/wiki/Portable_Document_Format#3D
[3] https://en.wikipedia.org/wiki/PDF#Forms

Conclusion

Pour se protéger d'un fichier PDF potentiellement malveillant, les recommendations usuelles adaptables à n'importe quel fichier potentiellement malveillant s'appliquent:

- Ne pas ouvrir ce fichier.
- N'ouvrir ce fichier que dans des environnements sûrs, par exemple:
  - un ordinateur dédié à cela,
  - une VM
  - utiliser les lecteurs de PDF inclut dans les navigateurs internet (e.g. `pdf.js`) plutôt qu'une application de bureau. En effet, on peut espérer que même s'il y a une faille de sécurité, la sandbox du navigateur offrira plus de protection qu'une application, qui elle est directement en contact avec le système.
- Toujours utiliser des logiciels (dans le cas des PDFs, les lecteurs de PDFs notamment[4]) à jour.

Pour ce qui est des recommendations propres aux PDFs:

[4] On pourrait également penser aux logiciels qui génèrent ou éditent des PDFs, par exemple *LibreOffice* ou *Microsoft Word*.