Code injection into a pdf file

Or how to take advantage of someone who just wanted to read a scientific paper

Table of contents

Embedding JavaScript

- How to embed code into a PDF file ?
- What are the effects of such an attack and how to prevent it ?

Exploiting all kinds of vulnerabilities

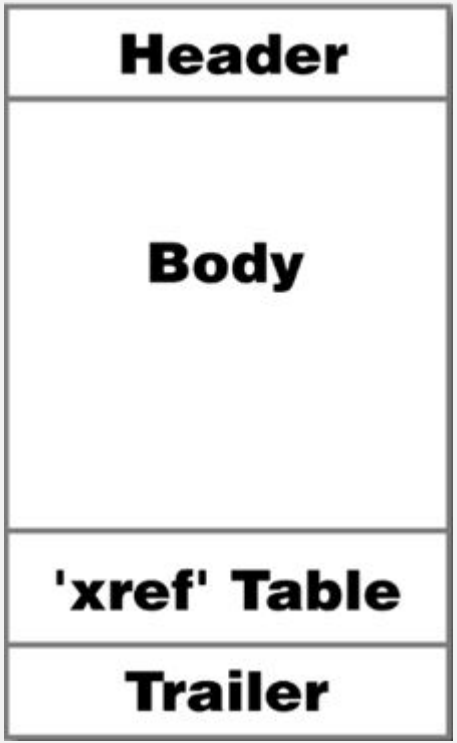
- How easy is it to exploit a vulnerability ?
- What is MetaSploit ?
- How is social engineering essential for an attack ?

Several examples and demonstrations will be shown

JavaScript injection

Basic structure of PDF files

- Header
  - Informations on the PDF specification used in the doc
- Body
  - Holds all the data in the document
- xref table
  - Contains references to all the objects in the document to allow random access within the file
- Trailer
  - Basically a “guide” for the application reading the PDF to find where special objects are located (e.g. the xref table)



Demonstration

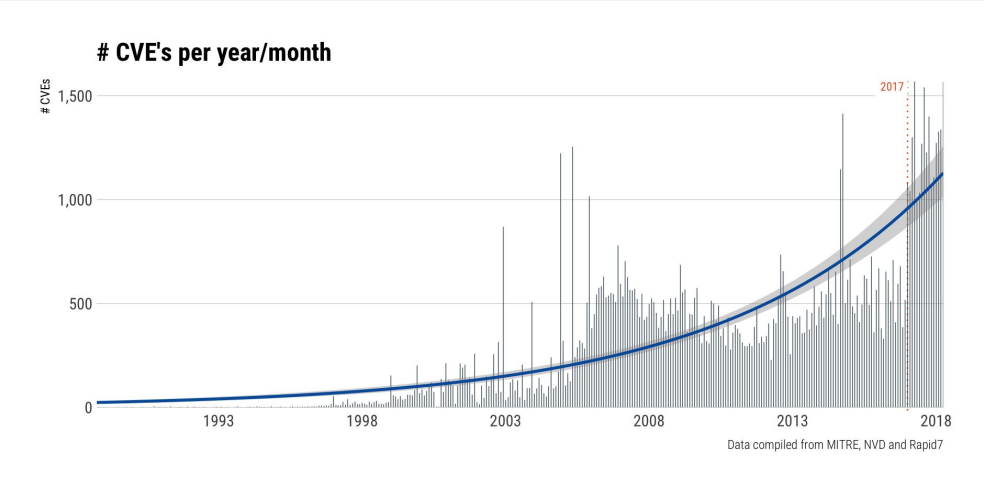
What can JavaScript do ?

- Javascript allows to download some malicious program on the machine where the file is open
- JavaScript can read the fingerprint of the running environment and send it to an attacker, that will now be able to target this user specifically
  - PDF reader specificities (software, version …)
  - Operating system
  - Screen size…
- Javascript can also obfuscate another exploit by having it encrypted somewhere else, and decoding it on-the-go when the file opens.
  - Avoid detection by anti-malwares and email filters
  - Can load, decode and execute the hidden code

Exploiting vulnerabilities of PDF readers

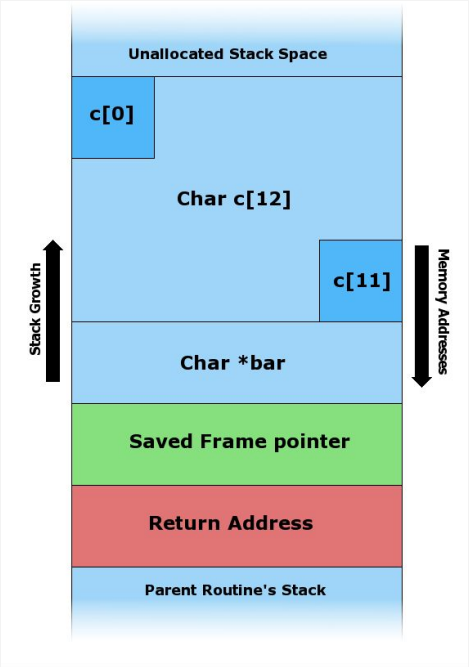
Readers vulnerabilities

- PDF viewers are programs, reading the PDF file and interpreting it
- This interpretation can be corrupted to into running some code
- A lot of these vulnerabilities are often discovered



Buffer overflow

- When a program writes too far into a buffer
- This not supposed to happen
- Can be used to execute malicious code
- Can happen because of vulnerabilities in the PDF reader



What is MetaSploit ?

- Open-source framework described as a pen-testing tool
- Developed in 2003 by H.D Moore, licenced to Rapid7 since 2009

Features contained

- Framework to operate vulnerabilities and actually attack systems
- Facilitates the submission of new **exploits** found on newer systems

Exploits

- An exploit is the attack on the reported vulnerability
- Exploits are specific to a reader and to a system

Demonstration

Limits

When an exploit is submitted to metasploit:

- It will quickly make its way to the antivirus database
- A PDF infected will soon be filtered out by email filters
- The targeted reader may fix the vulnerability in the next versions

This will limit the readers and systems that can be targeted

It will also make it harder to send the file without it being flagged as malicious

Exploiting vulnerabilities of human readers

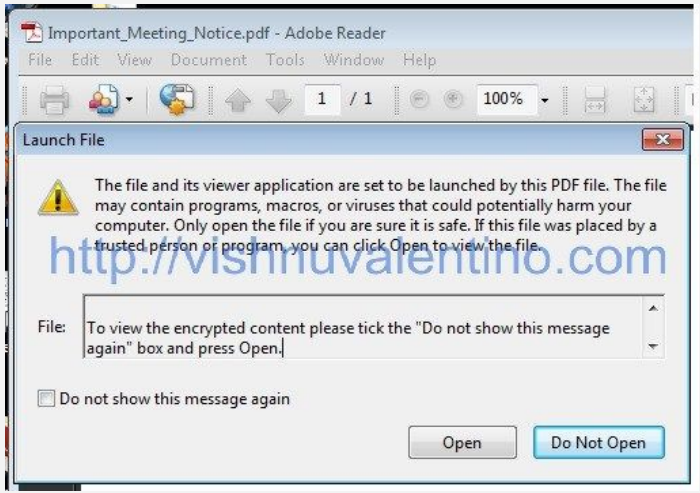
Social engineering

How do attackers convince people to open the files they are sending ?

- Make the email convincing
  - Coming from a trusted source
  - Naming your file with a clickbaity name
- Example : the LoveLetter virus
  - Email from a coworker with an attached file named LOVELETTER
  - Spreads using the victim’s outlook contact book
  - Caused between 5 and 9 billion dollars in damages from 1995 to 2000 and cost 15 billion to remove

Social engineering

- As a feature, some PDF readers are able to execute an embedded .exe file
- The user has to knowingly accept the execution of the .exe
- The dialog box asking for confirmation allows the message to be modified



How to protect yourself

- Disable JavaScript in your PDF reader (including the one in your browser)
- Don’t open any file you aren’t sure about
- Download your files from a trustworthy source
- Use an up-to-date version of your PDF reader
- And an up-to-date antivirus

Thank you

Sources

- Embedding JS into a file :
  - http://mariomalwareanalysis.blogspot.com/2012/02/how-to-embed-javascript-into-pdf.html
  - http://pralab.diee.unica.it/sites/default/files/aisec09f-corona.pdf
- Metasploit :
  - https://www.varonis.com/blog/what-is-metasploit/
- .exe embedding
  - https://www.hacking-tutorial.com/hacking-tutorial/client-side-attack-using-adobe-pdf-escape-exe-social-engineering/