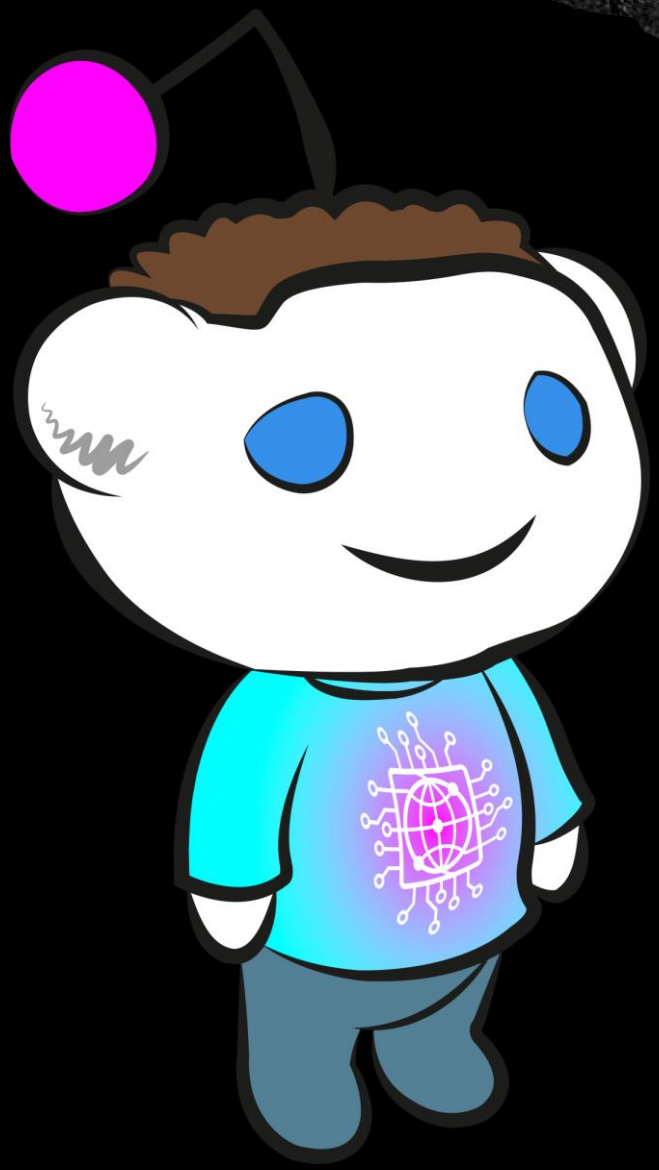
Mi baj lehet egy PDF-fel?

Matek Kamilló (k4m1ll0)
Business & Security 2026
2026.03.04



Whoami?

- Offenzív Security Researcher
- Etikus Hacker
- https://k4m1ll0.com
- 15+ CVE, publikációk
- Szakterület: Red Teaming, Exploit Fejlesztés és Penetrációs Tesztek
- Kapcsolat: k4m1ll0@protonmail.com

A PDF mítosza

- “Statikus” dokumentum
- Nincs benne makró, ezért biztonságos(abb).
- Csak megjelenít, nem futtat kódot.
- A vírusirtó úgyis átnézi.
- A fájlkiterjesztés (.pdf) garancia arra, hogy az tényleg PDF.
- Ha az X program nyitja meg, akkor rendben van.
- A Gateway kiszűri.
- „A PDF nem tud kommunikálni kifelé”.

Mitől PDF egy PDF valójában?

- %PDF-1.x fejléc a fájl elején
- Objektumok (obj / endobj)
- stream blokkok (bináris, tömörített adat)
- xref és trailer
- A reader parzerének toleranciája

Nem a kiterjesztés dönti el. A parzer dönti el.

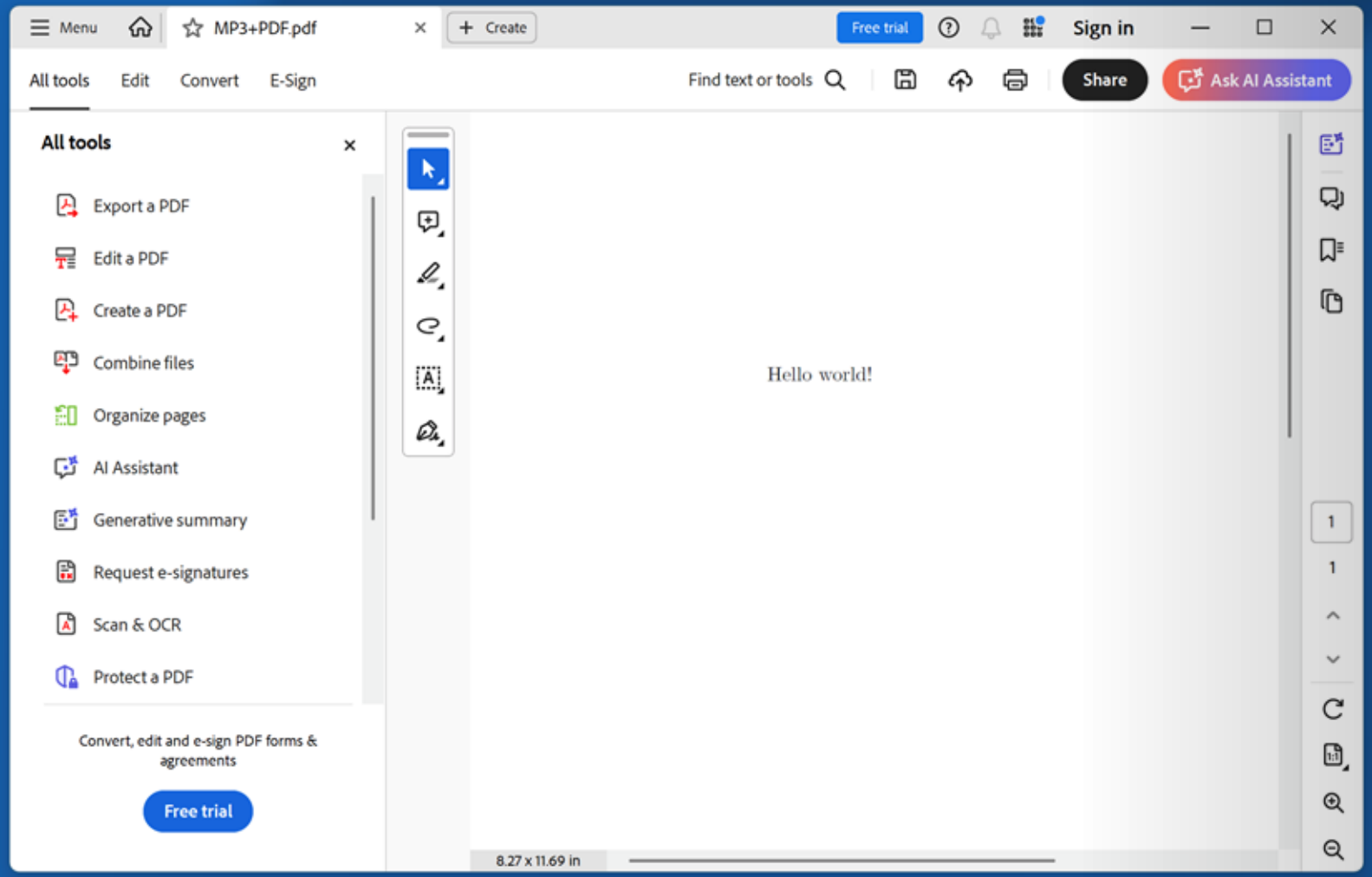
```
%PDF-1.1
1 0 obj
<< /Type /Catalog
   /Pages 2 0 R
>>
endobj

2 0 obj
<< /Type /Pages
   /Kids [3 0 R]
   /Count 1
>>
endobj

3 0 obj
<< /Type /Page
   /Parent 2 0 R
   /MediaBox [0 0 300 144]
   /Contents 4 0 R
   /Resources <<
      /Font <<
         /F1 5 0 R
      >>
   >>
>>
endobj
```

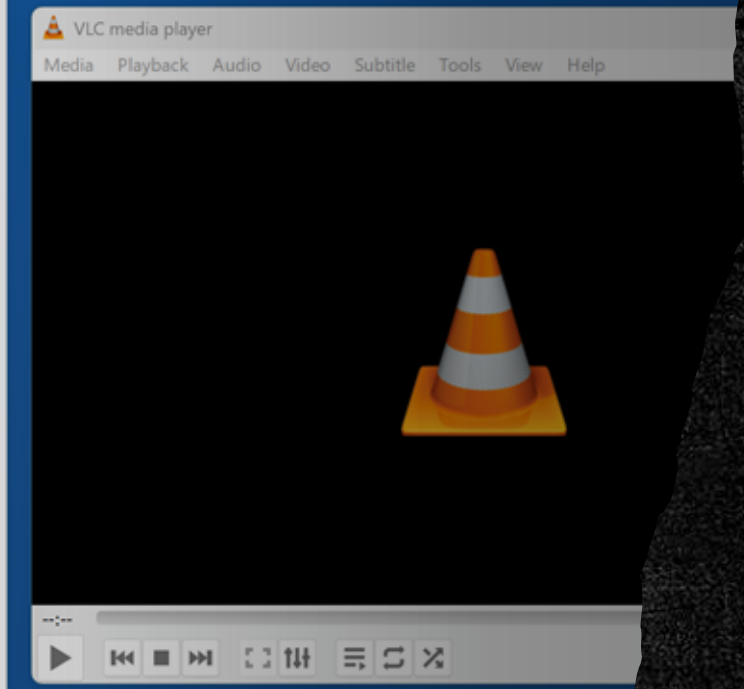
```

4 0 obj
<< /Length 44 >>
stream
BT
/F1 18 Tf
72 72 Td
(Hello, PDF.) Tj
ET
endstream
endobj

5 0 obj
<< /Type /Font
   /Subtype /Type1
   /BaseFont /Helvetica
>>
endobj

xref
0 6
0000000000 65535 f
0000000009 00000 n
0000000060 00000 n
0000000117 00000 n
0000000278 00000 n
0000000390 00000 n

trailer
<< /Size 6
   /Root 1 0 R
>>
startxref
482
%%EOF
```

```
 Volume in drive C has no label.
 Volume Serial Number is 546A-31A5

 Directory of C:\Users\x\Desktop

02/27/2026  07:15 AM    <DIR>          .
01/22/2026  12:15 PM    <DIR>          ..
02/27/2026  07:15 AM           455,842 MP3+PDF.pdf
               1 File(s)        455,842 bytes
               2 Dir(s)  31,254,081,536 bytes free
```

Hallgassunk meg egy PDF-et?

MP3+PDF DEMO

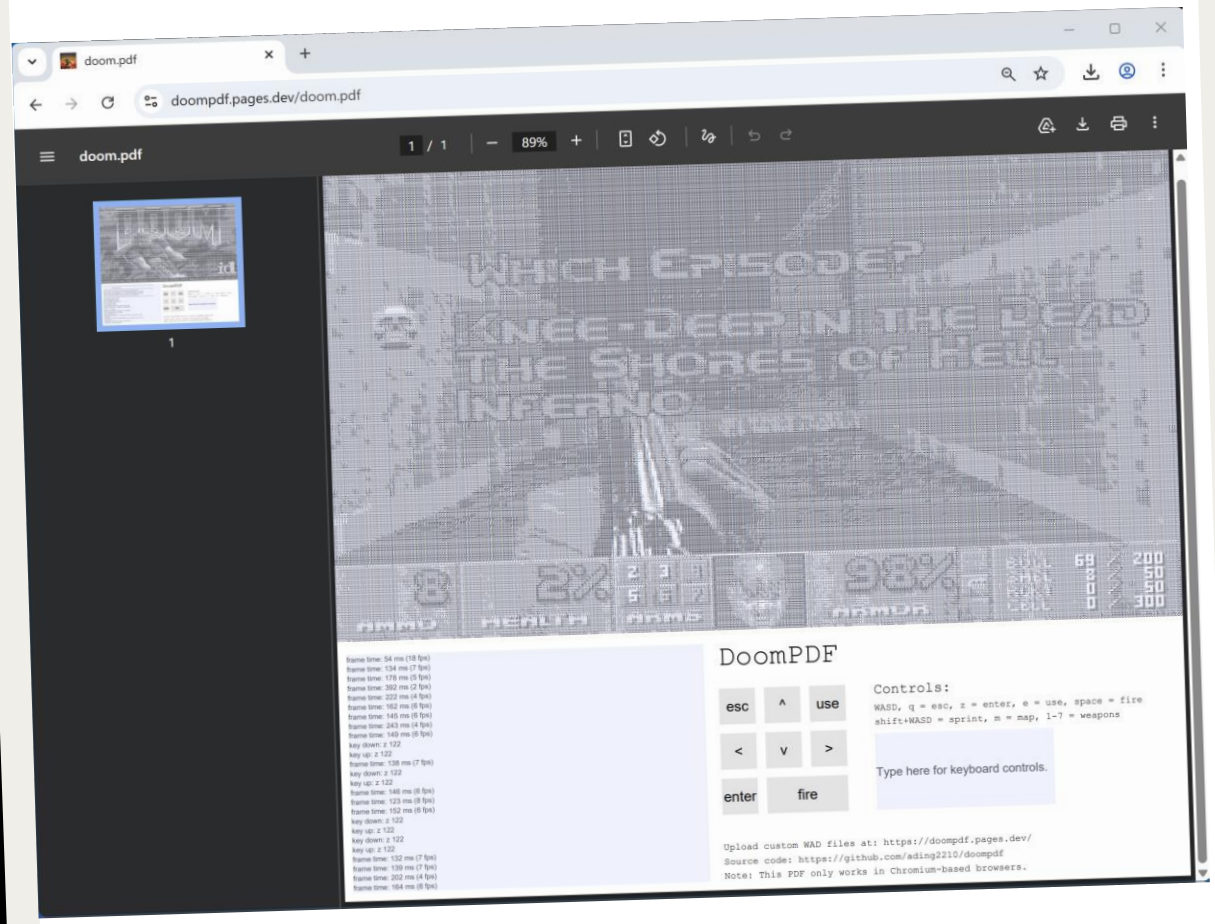




A PDF valójában

- **Konténer**
  - más dokumentumokat, fájlokat tartalmazhat
- **Esemény vezérelt**
  - megnyitás, kattintás, fókusz, lapozás
- **Kódot futtat**
  - JavaScript runtime a readerben
- **Tartalmat tölt be**
  - linkek, külső erőforrások
- **Interaktív**
  - űrlapok, annotációk, beágyazott objektumok
- **Több formátum egy fájlban**
  - HTML, média, bináris adat
- **Alkalmazás-szerűen viselkedik**

PDF DOOM DEMÓ



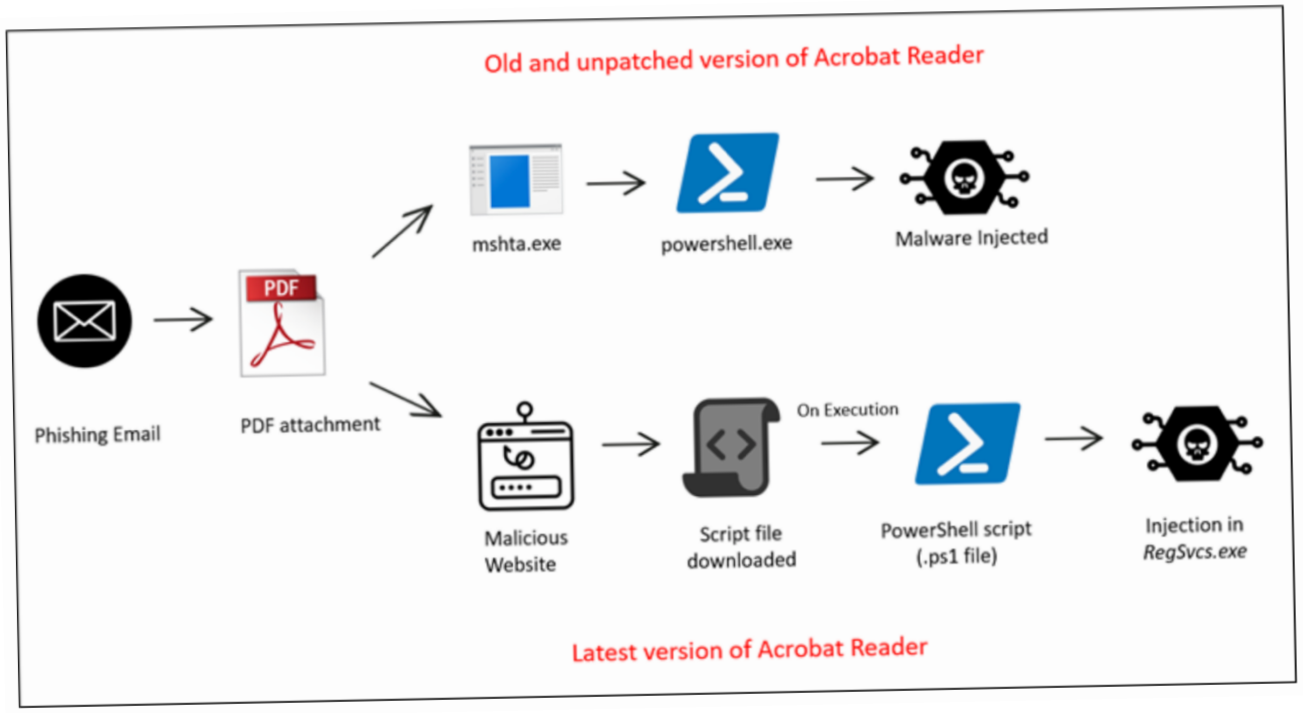
Miért ideális támadási hordozó?

Támadói szemmel nézve egy fájltípus akkor jó, ha:

- **Ismert és elfogadott formátum**
  – nem kelt gyanút
- **Mindenkinél telepítve van a megfelelő program**
  – nincs telepítési akadály
- **Megbízhatónak gondolják**
  – „ez csak egy számla / CV”
- **Valami mindig parzolja**
  – desktop, mobil, böngésző, library
- **Platformok engedik**
  – LinkedIn, Google Drive, stb..
- **Social engineering-re tökéletes**
  – önéletrajz, szerződés, ajánlat, riport

Ezeket a PDF mind tudja.

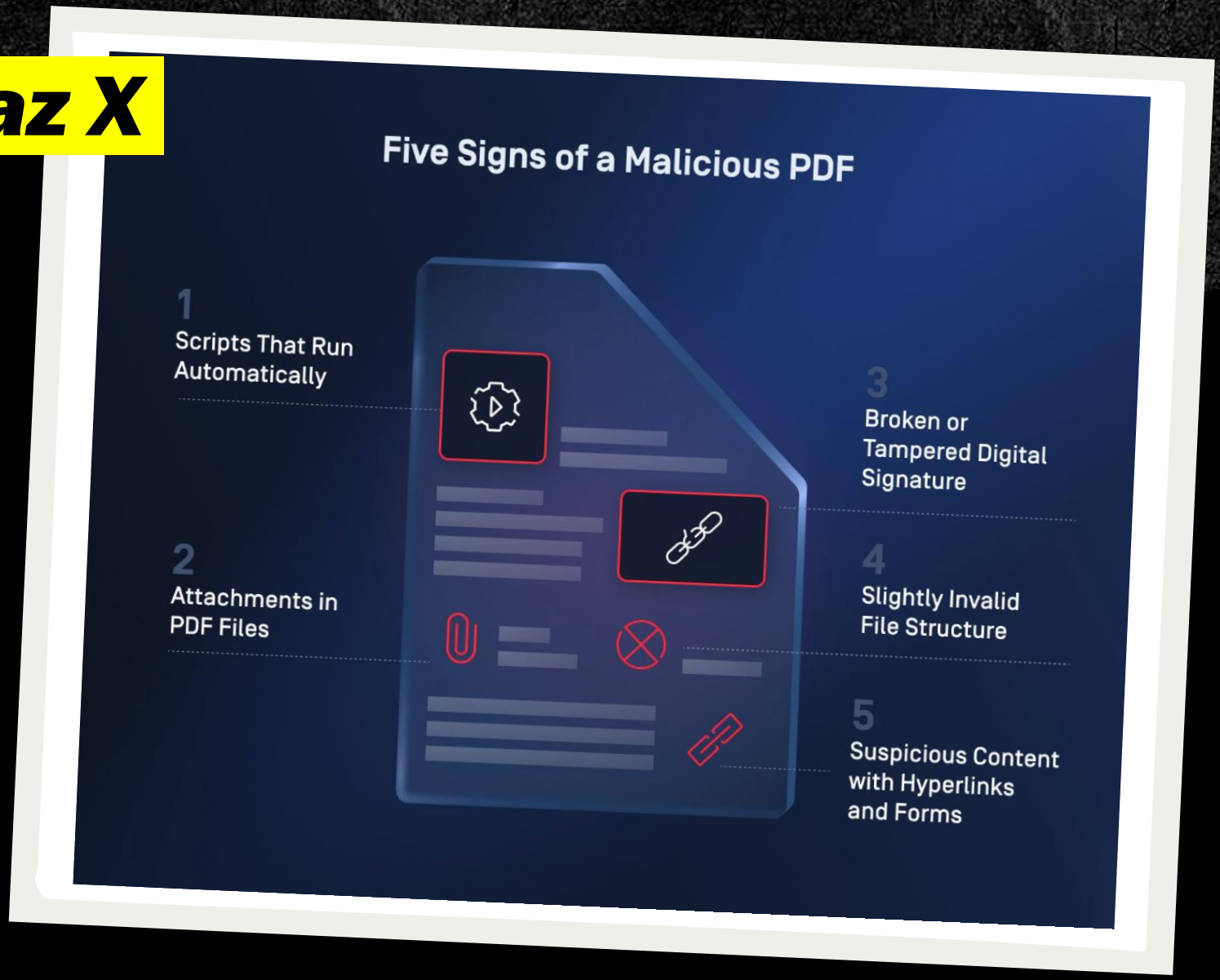
PDF a valódi támadásokban



- A PDF az egyik leggyakoribb malware-hordozó e-mailben
- Rendszeresen szerepel
- targeted phishing kampányokban
- APT műveletekben
- üzleti e-mail kompromittációban
- CV-k, számlák, szerződések formájában
- Nem feltétlenül zero-day kell hozzá, hanem jó időzítés és kontextus is elég lehet. (De azért egy jó kis zeroday is jól jöhet.)

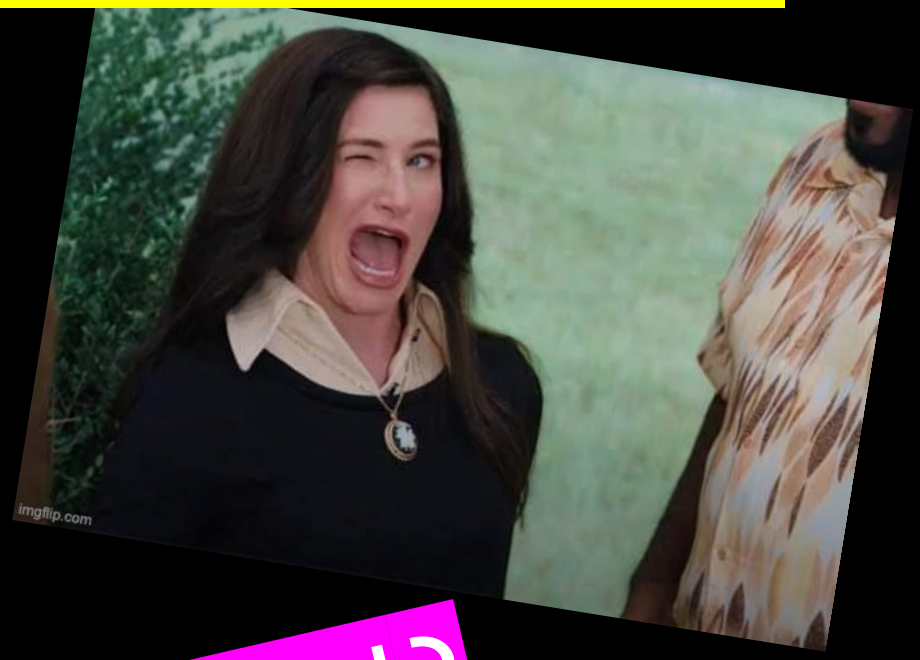
Megvéd minket az X vírusírtó?

- A felismerés mintaalapú
- A PDF struktúrája végtelenül variálható
- Ugyanaz a logika
- más sorrend
- más tömörítés
- más szerializáció
- A parzer megpróbálja értelmezni
- A detekció gyakran lemarad



Az előadás diái PDF-ben elérhetőek... ☺

Nem kell félni, teljesen ártalmatlanok.
De tényleg.



Te letöltenéd?

Köszönöm a figyelmet!

Kérdések?