PDF = Potencijalno Destruktivan Fajl

Filip Vlašić,
NCERT

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Sadržaj

- O PDF formatu
- Struktura PDF dokumenta
- Rizici
- Ranjivosti
- Exploit - primjeri
- Zaštita

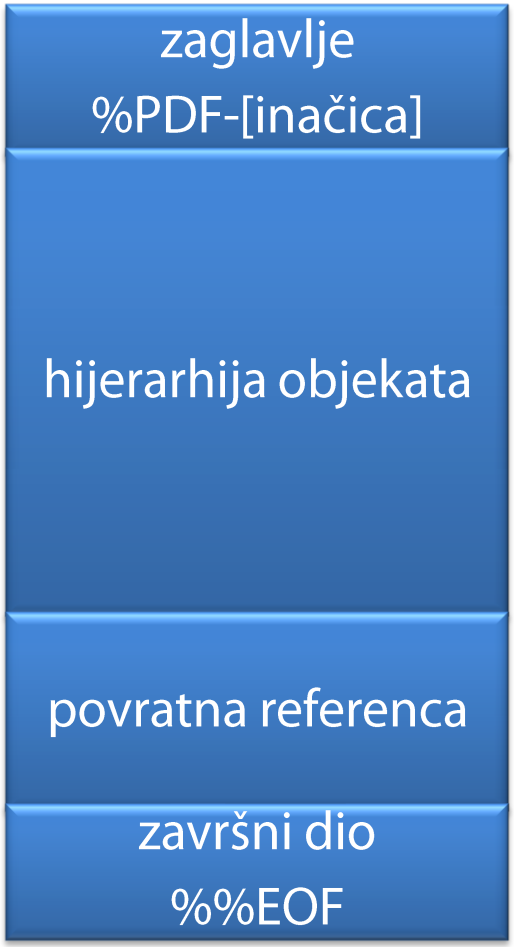
O PDF formatu

- Portable Document Format, nastao 1993. (Adobe)
- 2008. – otvoreni ISO standard
- velika popularnost zbog činjenice da čuva integritet dokumenta kroz različite platforme
- glavni format za pohranjivanje i distribuciju dokumenata
- različiti čitači

O PDF formatu - mogućnosti

- prikaz teksta, grafike i slika
- interaktivni elementi – zabilješke, zvukovi i video-zapisi (Flash), okidači, forme …
- PDF jezik podržava osam vrsti objekata (tipova podataka)
- grafički model temelji se na jeziku PostScript, grafička stanja su kolekcija 24 parametra
- podržani različiti filtri za kodiranje (kompresiju) slika
- mogućnost dodavanja JavaScript koda
- enkripcija, digitalno potpisivanje dokumenta

Struktura PDF dokumenta



•format oznake za objekt:

•**[objnum] [genid] obj (value) endobj**

[objnum] – redni broj objekta

obj, endobj – ključne riječi

[genid] – identifikator verzije objekta koji sa objnum čini jedinstvenu oznaku objekta preko koje se objekt može referencirati

(value) – vrijednosti u objektu (vrsta fonta, akcije itd.)

•objekti su u odnosu **roditelj-dijete**

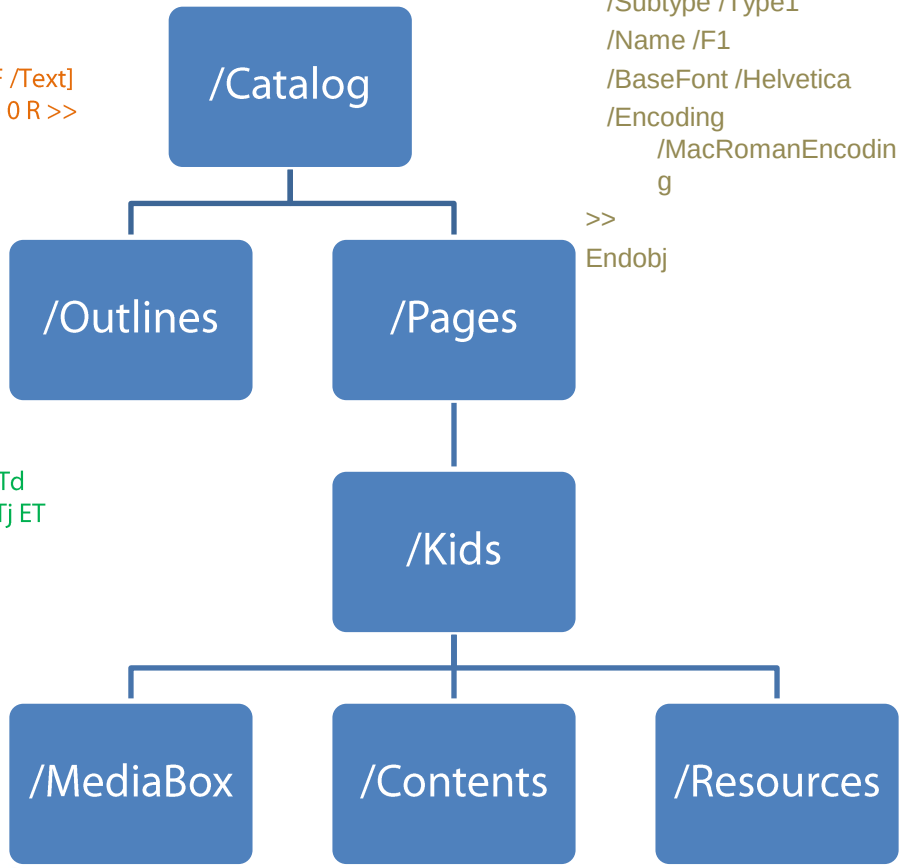
•PDF jezik je “Case-Sensitive”

Struktura PDF dokumenta - PDF dokument pod povećalom

```
%PDF-1.1

1 0 obj
<<
  /Type /Catalog
  /Outlines 2 0 R
  /Pages 3 0 R
>>
endobj

2 0 obj
<<
  /Type /Outlines
  /Count 0
>>
endobj

3 0 obj
<<
  /Type /Pages
  /Kids [4 0 R]
  /Count 1
>>
endobj
```

```
4 0 obj
<<
  /Type /Page
  /Parent 3 0 R
  /MediaBox [0 0 612 792]
  /Contents 5 0 R
  /Resources <<
        /ProcSet [/PDF /Text]
        /Font << /F1 6 0 R >>
>>
endobj
```

```
5 0 obj
stream
BT /F1 24 Tf 100 700 Td
      (Hello World) Tj ET
endstream
endobj
```




```
6 0 obj
<<
  /Type /Font
  /Subtype /Type1
  /Name /F1
  /BaseFont /Helvetica
  /Encoding
      /MacRomanEncodin
      g
>>
Endobj
```

```
xref
0 7
0000000000 65535 f
0000000012 00000 n
0000000089 00000 n
0000000145 00000 n
0000000214 00000 n
0000000419 00000 n
0000000520 00000 n
trailer

<<
  /Size 7
  /Root 1 0 R
>>
startxref
644
%%EOF
```

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

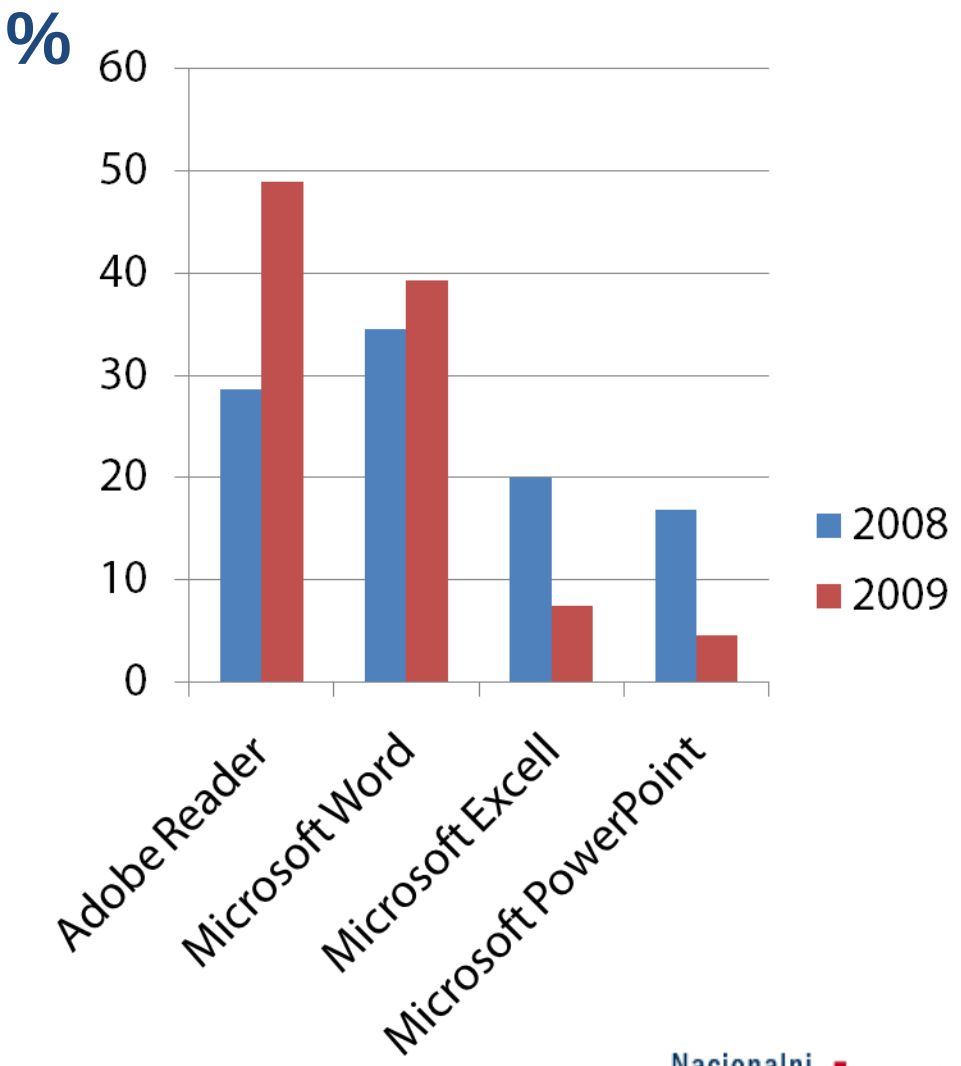
Nacionalni CERT

Rizici

- popularnost
- korisnici imaju naviku automatski otvarati PDF dokumente unutar web preglednika
- 83.5% korisnika ne vrši redovitu nadogradnju Adobe alata
  - (McAffe, 8/2009.)
- socijalni inženjering

Ranjivosti

- (Adobe) JavaScript
- naredba /Launch /Action
- dodatne mogućnosti (mailto: ranjivost IE7)
- nekonzistentni PDF parser – nedefinirani iznimni slučajevi
- leksička labavost
- formati za kodiranje i kompresiju slika (TIFF), mogu se koristiti za prikrivanje koda
- ranjivost vanjskih biblioteka (TrueType, Flash)



Exploiti – primjeri I

- zloćudni PDF dokument se širi kao privitak u e-mail porukama koje socijalnim inženjeringom navode korisnika na otvaranje dokumenta ili putem web stranice
- socijalni inženjering – napadi obično oslovljavanju potencijalne žrtve radi stjecanja kredibiliteta
- tehnička priroda, primjer 1: zloćudni JavaScript kod kodiran (FlatDecode) u neki od objekata i u njemu se nalazi kod za ljusku (shellcode) koji služi za dohvaćanje malvera (keylogger) putem URL-a, JavaScript kod provjerava inačicu korištenog Adobe Reader-a kako bi odredio koju će ranjivost iskoristiti

Exploiti – primjeri II

- Pr. 2: zlćudni kod u objektu koristi mailto naredbu za isključivanje Windows vatrozida, preuzimanje i pokretanje crva (<= Adobe Reader 8.1)
- Pr. 3: XML datoteka unutar PDF dokumenta koja u sebi sadrži zlćudnu TIFF datoteku (sliku), koristi 2 ranjivosti
- Pr. 4: naredba /Launch /Action služi za pokretanje bilo koje vrste datoteke, napadač može izmijeniti upozorenje o otvaranju vanjske datoteke (ranjivost PDF jezika)
- Pr. 5: zlćudni Flash sadržaj unutar PDF dokumenta, koristi ranjivost datoteke authplay.dll (<= Adobe Reader 9.3)

Zaštita

- otvaranje dokumenata isključivo iz pouzdanih izvora
- redovite nadogradnje PDF preglednika i anti-virusnog softvera
- isključivanje podrške za JavaScript
- korištenje alternativnih preglednika
- isključivanje automatskog otvaranja dokumenata unutar web preglednika

Za one koje zanima više

- blog Didiera Stevensa, http://blog.didierstevens.com
- pdftk, alat za analizu PDF datoteka, http://www.pdflabs.com/tools/pdftk-the-pdf-toolkit/
- http://www.adobe.com/support/security/, službena web stranice na kojoj Adobe izdaje sigurnosne preporuke
- http://isc.sans.edu/
- www.cert.hr ☺