COSCUP 2008

輕鬆偵測惡意文件

徐千洋(timhsu)

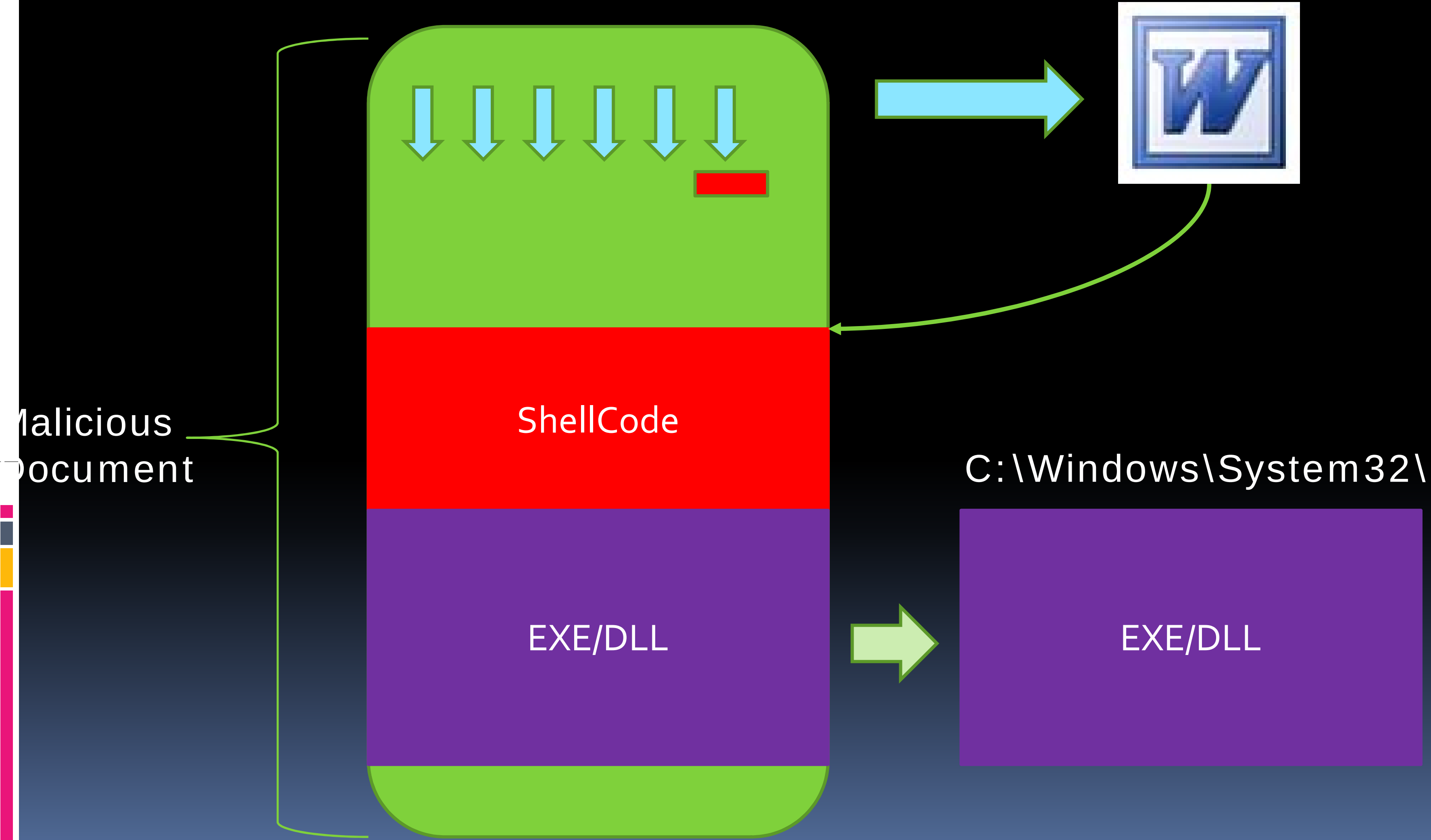
- HIT(Hacks In Taiwan)主辦人
- 網駭科技創辦人
- 資訊安全技術研究者，同時也是 Linux 愛好者。
- 專長於網路程式設計　網路滲透測試　駭客攻擊手法研究　惡意程式分析及嵌入式系統等。
- 著作
  - Linux C 函式庫詳解辭典 (旗標)
  - The Wargame 駭客訓練基地 - 決戰台灣版(旗標) (與曾信田、莊明躍、何弈甫等人合著)

什麼是惡意文件?

惡意文件

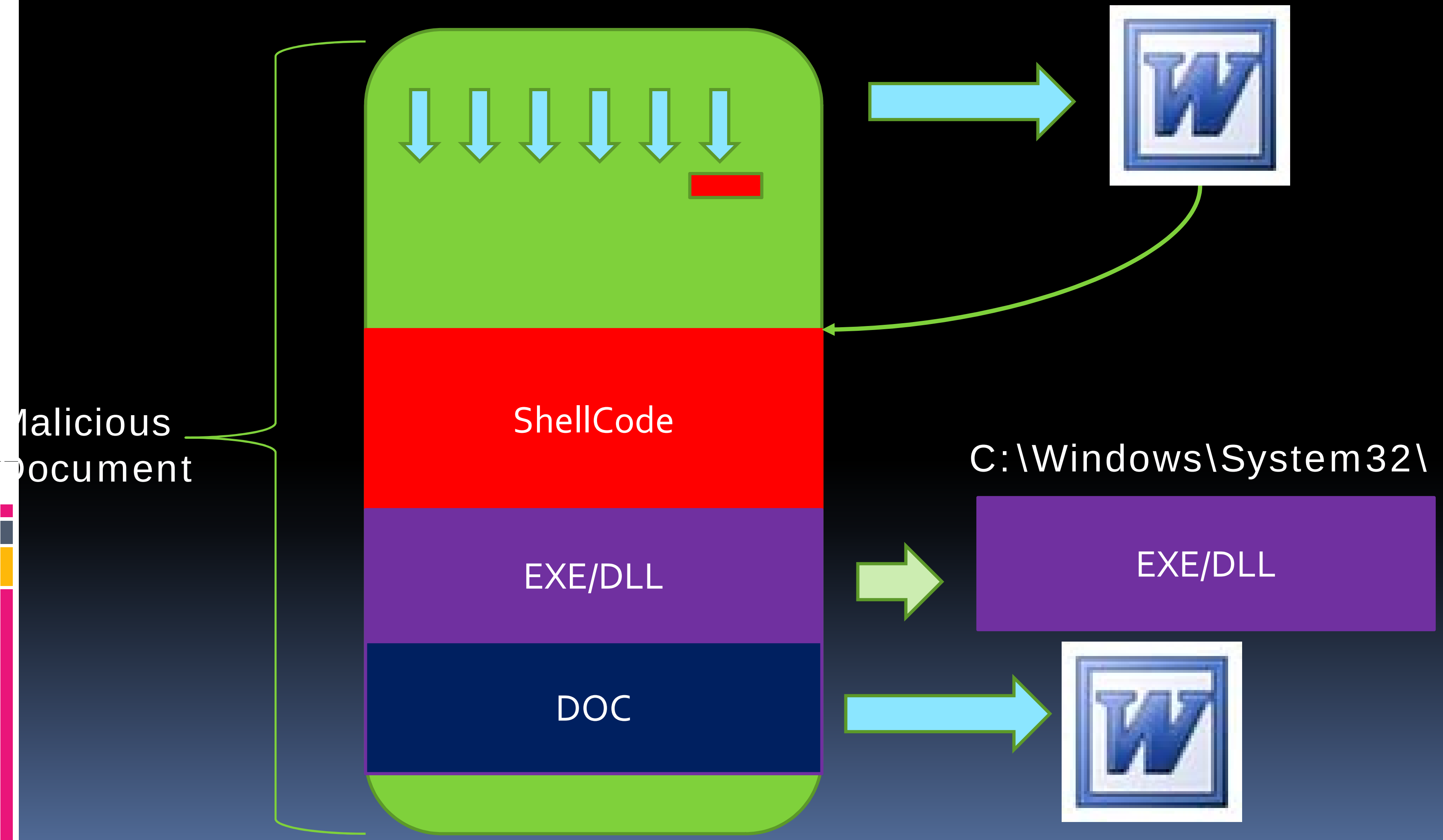
- 文件檔
  - 非可執行檔(.EXE、.DLL、.SYS)
  - 非純 Script 語言程式檔 (.BAT、.SH、.PL、.PY)
  - 非純文字 (.TXT)
  - 需要特定的程式解析並開啟 (DOC/XLS/PPT/PPS/MDB/CHM/PDF/RAR/ZIP/...)
- 惡意文件檔
  - 透過格式解析時錯誤所造成的弱點
  - 透過內嵌的 延伸功能或語言 (Macro/Javascript/ActionScript 等)

惡意文件攻擊運作流程

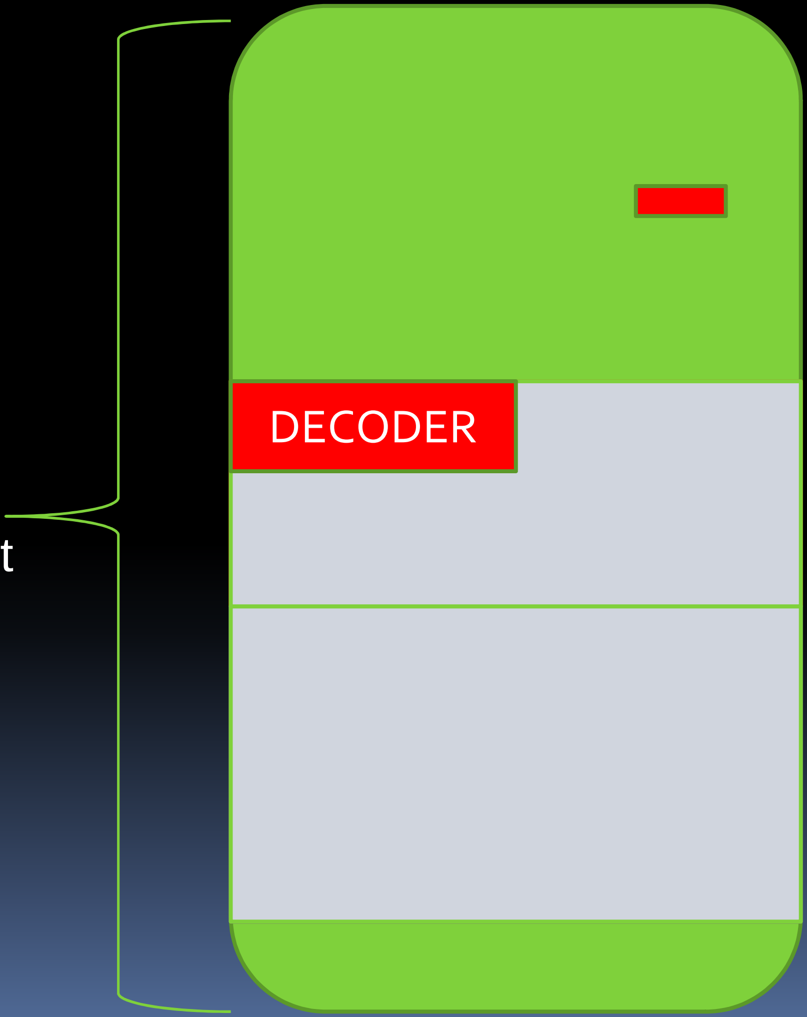


Malicious
Document
ShellCode
EXE/DLL
C:\Windows\System32\
EXE/DLL

惡意文件攻擊運作流程進化



利用編碼技術



Malicious
Document

DECODER

OLE Storage Access

- Libgsf
  - 'libgsf' is a simple i/o library that can read and write common file types and handle structured formats that **provide file-system-in-a-file** semantics. There are some additional utilities for document centric applications
- Source Archive: http://ftp.acc.umu.se/pub/GNOME/sources/libgsf/1.14/libgsf-1.14.4.tar.gz
- Licenses: LGPLv2.1

ripOLE

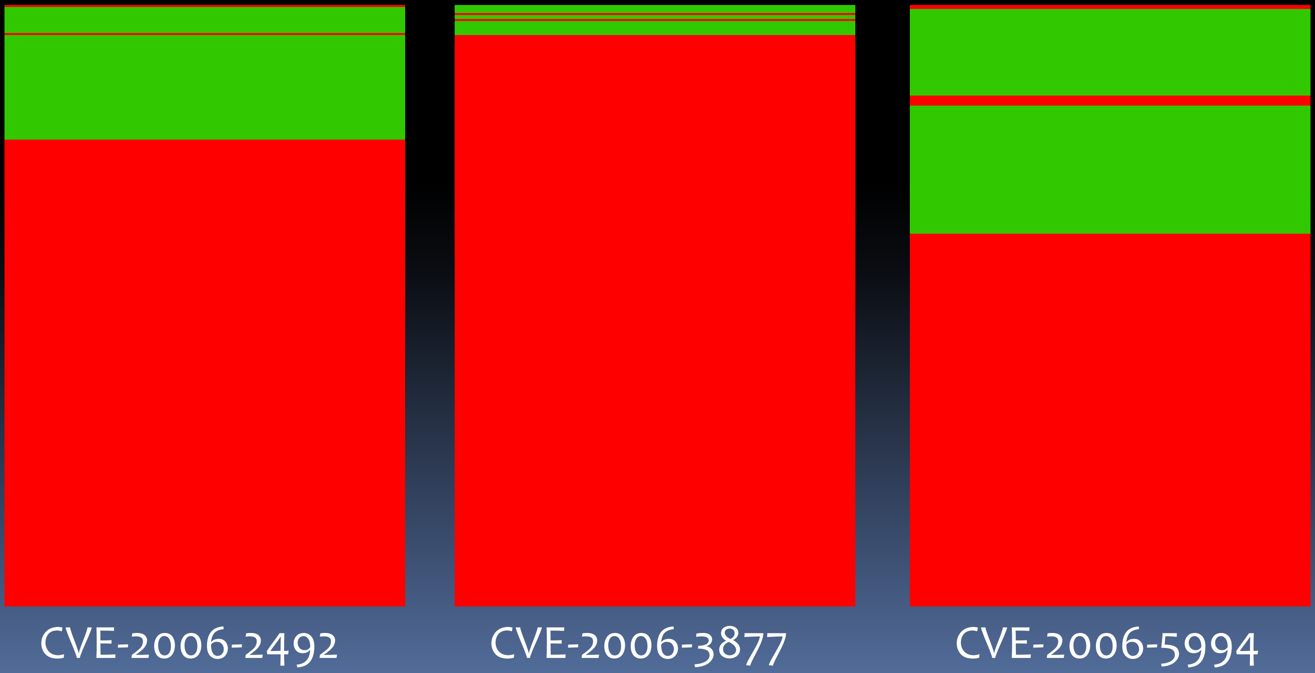
- http://www.pldaniels.com/ripole/
- ripOLE is a small program/library designed to pull out attachments from OLE2 data files (ie, MS Office documents).
- Licenses: BSD licenced

LAOLA

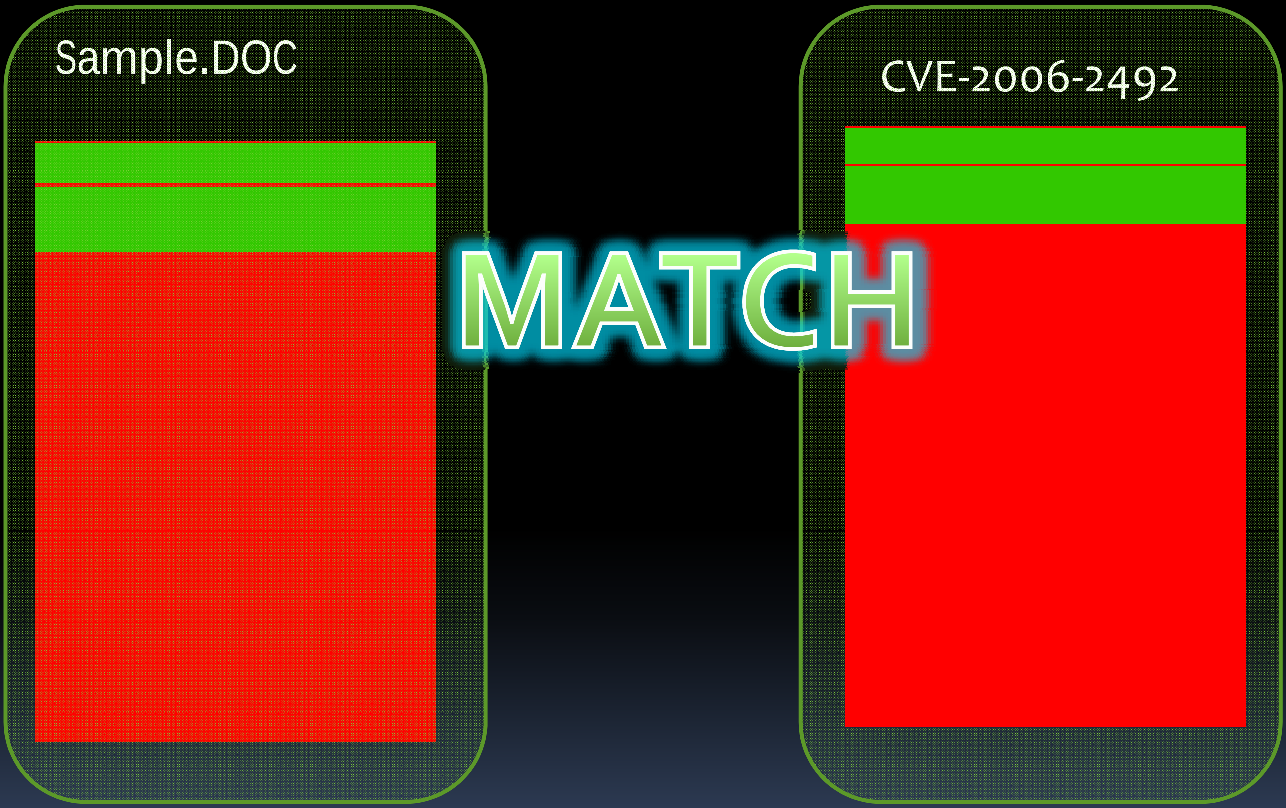
- http://www.cs.tu-berlin.de/~schwartz/pmh/laola.html
- LAOLA is a collection of documentations and perl programs dealing with binary file formats of Windows program documents.
- Licenses: GPLv2

OLE Storage Fingerprint

- OLE Storage offset and size
- Draw the diagram with MDScan
- Green: OLE   Red: Data or Unknow

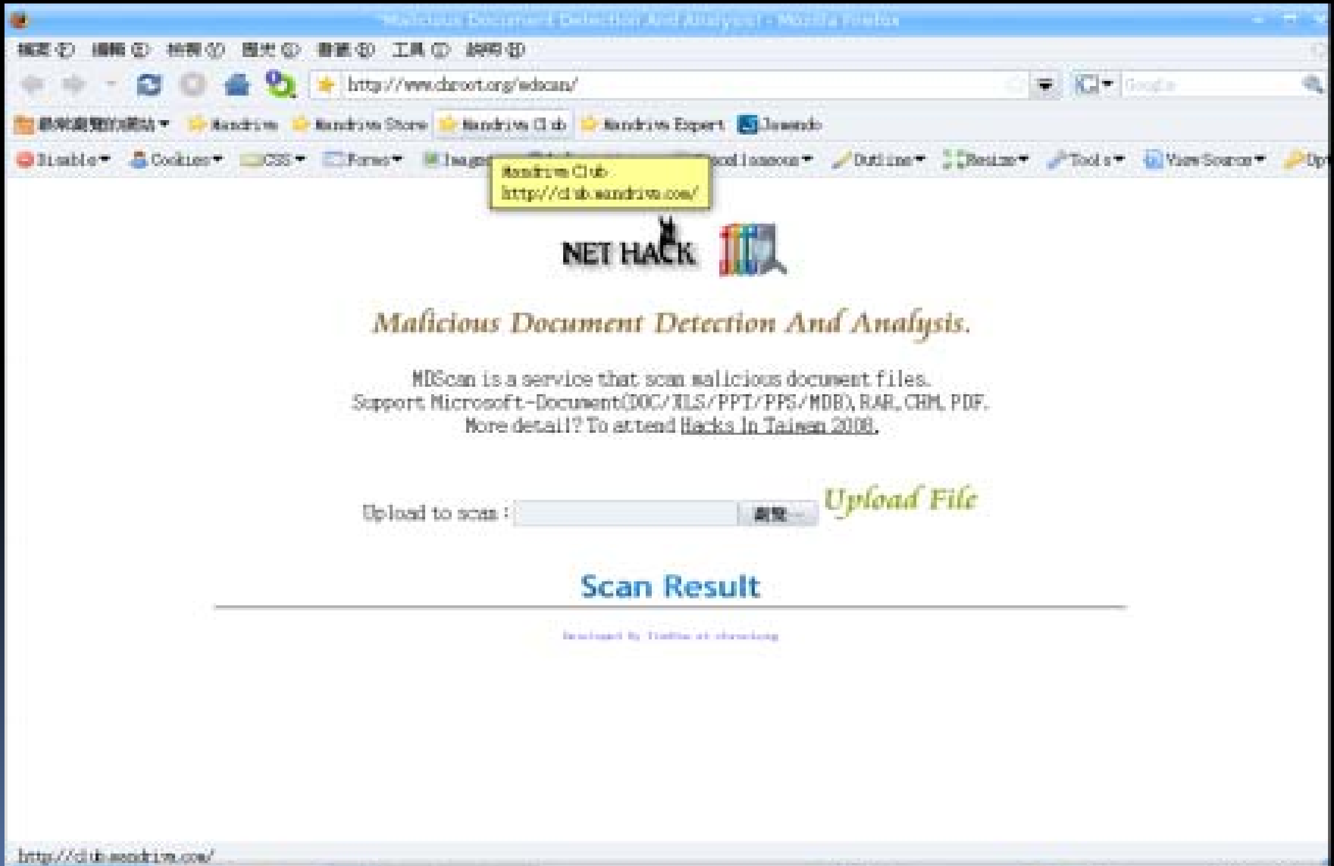


Identify CVE



MDScan

- http://www.chroot.org/mdscan



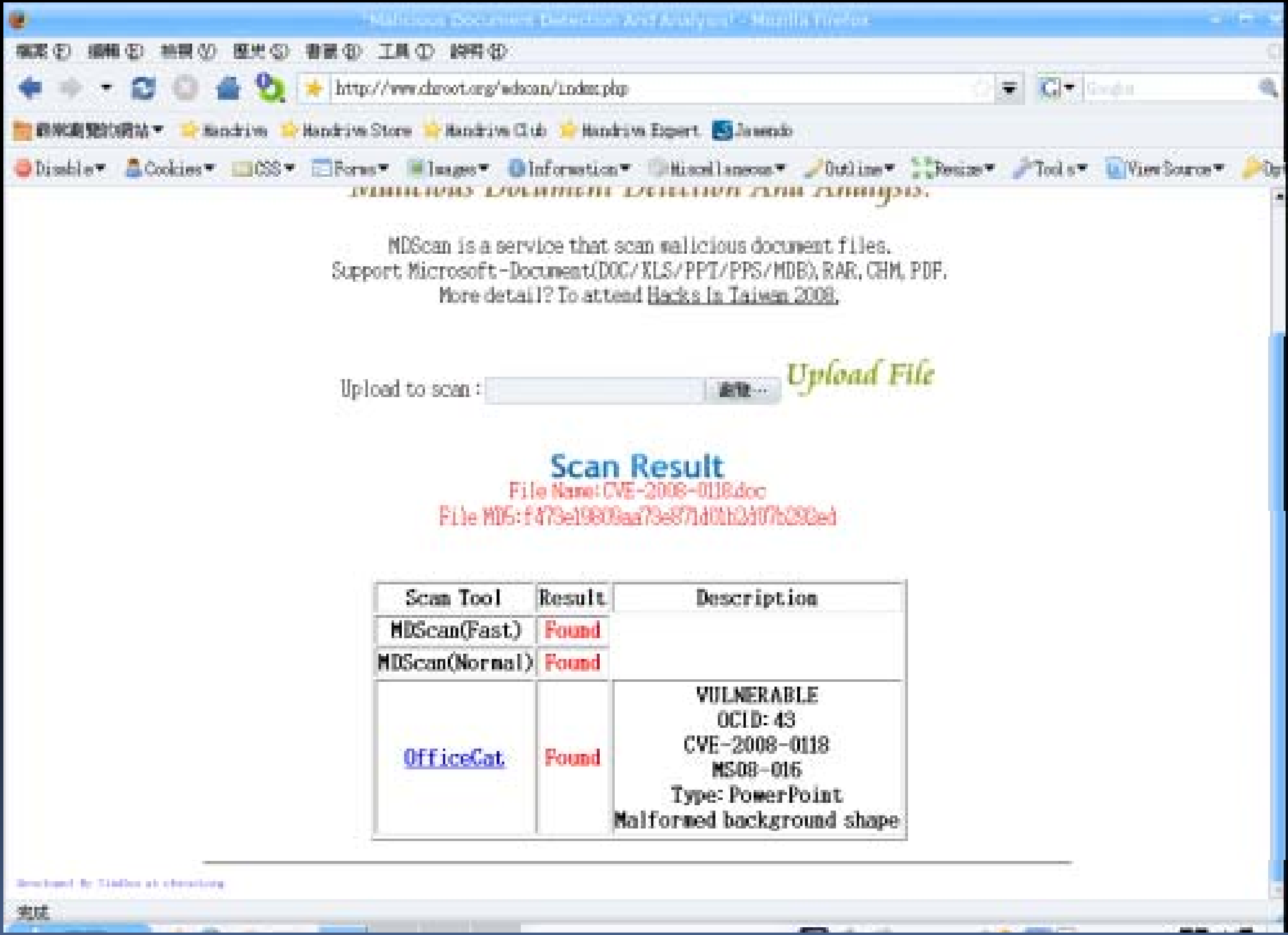
Malicious Document Detection And Analysis.

MDScan is a service that scan malicious document files.
Support Microsoft-Document(DOC/XLS/PPT/PPS/MDB), RAR, CHM, PDF.
More detail? To attend Hacks In Taiwan 2008.

Upload to scan : 瀏覽... *Upload File*

Scan Result

http://www.chroot.org/mdscan



Malicious Document Detection And Analysis.

MDScan is a service that scan malicious document files.
Support Microsoft-Document(DOC/XLS/PPT/PPS/MDB),RAR,CHM,PDF.
More detail? To attend Hacks In Taiwan 2008.

Upload to scan : 瀏覽...

Upload File

Scan Result

File Name:CVE-2008-0118.doc
File MD5:f473e19808aa73e871d0b2d07b292ed

Scan Tool	Result	Description
MDScan(Fast)	Found	
MDScan(Normal)	Found	
OfficeCat	Found	VULNERABLE OCID:43 CVE-2008-0118 MS08-016 Type:PowerPoint Malformed background shape

CHM/RAR/PDF

- CHM(compiled html help)
  - Extract it
  - Any PE/MZ Executed file?
- RAR
  - WinRAR "lzh.fmt" LHA Archive Processing Client-Side Buffer Overflow Vulnerability
  - CVE-2006-3845
  - .RAR but LHA magic?
- PDF
  - Adobe Products JavaScript Method Code Execution Vulnerability
  - Embed Javacript?

RARCheck.sh

```
#!/bin/sh
if [ "$1" == "" ]; then
    echo Usage: $0 [rar]
    exit 0;
fi
#file $1 | grep "RAR" > /dev/null 2>&1
echo $1 | grep -iE '\.rar$' > /dev/null 2>&1
if [ "$?" == "1" ]; then
echo Sorry! Not RAR file.
exit;
fi
file $1 | grep -i "lha" > /dev/null 2>&1
if [ "$?" == "0" ];then
    echo Warnning: $1 maybe not be safe!
    exit 1;
else
    echo $1 is safe.
    exit 0;
fi
```

PDFCheck.sh

```
#!/bin/sh
if [ "$1" == "" ]; then
    echo Usage: $0 [pdf]
    exit 0;
fi
file $1 | grep "PDF document" > /dev/null 2>&1
if [ "$?" == "1" ]; then
echo Sorry! Not PDF file.
exit 0;
fi
pdfsize=`pdfinfo $1 | grep "File size" | awk '{print $3}'`
pdftotext -raw $1 /tmp/pdf_test.txt
pdftxtsize=`stat -c %s /tmp/pdf_test.txt`
if [ $pdftxtsize == 1 ];then
    echo Warnning: $1 maybe not be safe!
    exit 1;
else
    echo $1 is safe.
    exit 0;
fi
```

Reference

- Exploit Modify Tips & oday – Nanika
  - HIT 2006 (http://www.hitcon.org/oldweb/sch.htm)
- Understanding Windows Shellcode
  - http://www.hick.org/code/skape/papers/win32-shellcode.pdf
- Windows Memory Layout, User-Kernel Address Spaces
  - http://www.openrce.org/reference_library/files/reference/Windows%20Memory%20Layout,%20User-Kernel%20Address%20Spaces.pdf
- Dynamic analysis of malicious code
  - http://www.cs.ucsb.edu/~chris/research/doc/virology06_dynamic.pdf
- OfficeCat
  - http://www.snort.org/vrt/tools/officecat.html

Question?