Foundstone
A division of McAfee

Analyzing Malware with REMnux

Glenn P. Edwards Jr.
Senior Consultant
Incident Response & Digital Forensic Practice
Foundstone Professional Services

whoami

Glenn P. Edwards Jr.

id

uid=0(Senior Consultant) gid=0(Foundstone) groups=0(IR Practice)

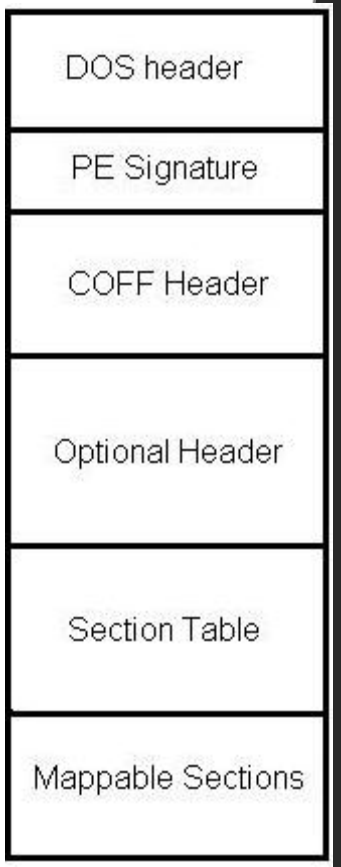
- Have some fancy letters after my name
  - M.S. in Digital Forensics, University of Central Florida
  - B.S. in Information Security & Privacy, High Point University
  - GREM, GCIH, GCFA (yada yada…)
- started to come out of the shadows…
  - @hiddenillusion
  - hiddenillusion.blogspot.com
  - blog.opensecurityresearch.com

… you get the point

PE file

$ xxd file | head

```
0000000: 4d5a 9000 0300 0000 0400 0000 ffff 0000  MZ..............
0000010: b800 0000 0000 0000 4000 0000 0000 0000  ........@.......
0000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000030: 0000 0000 0000 0000 0000 0000 e800 0000  ................
0000040: 0e1f ba0e 00b4 09cd 21b8 014c cd21 5468  ........!..L.!Th
0000050: 6973 2070 726f 6772 616d 2063 616e 6e6f  is program canno
0000060: 7420 6265 2072 756e 2069 6e20 444f 5320  t be run in DOS
0000070: 6d6f 6465 2e0d 0d0a 2400 0000 0000 0000  mode....$.......
0000080: 7ff2 bb9b 3b93 d5c8 3b93 d5c8 3b93 d5c8  ....;...;...;...
0000090: f89c 88c8 3793 d5c8 3b93 d4c8 3493 d5c8  ....7...;...4...
```



REMnux

$ man REMnux

- Around since 2010
- VM based or ISO
- Current v3 is based on Ubuntu 11.10
- Full of goodies ☺
  - ~remnux/.bash_aliases
  - /usr/local/bin/
  - /usr/bin/

http://zeltser.com/remnux/

http://zeltser.com/remnux/remnux-malware-analysis-tips.html

REMnux

$ sudo find / -group goodies –exec basename {} \;

wireshark
honeyd
fakedns
fakemail
iietsim
netcat
NetworkMiner
tcpdump
trid
file
7z
clamscan
pescanner
pyew

upx
packerid
volatility
strings
hachoir-metadata
hachoir-subfile
jd-gui
js-beautify
pdnstool
swf_mastah
flashbug
pdfextract

pdfid
pdf-parser
pdfxray_lite
peepdfvbindiff
ssdeep
md5deep
hashdeep
sha1sum
bytehist
pyew
radare
icat
ils

sorter
swfdump
swfextract
srch_strings
yara
rhino
burpsuite
Xorsearch
origami

REMnux

- File Identification
  - file
  - TRiD
  - 7zip
  - hachoir-metadata

REMnux

- File Analysis
  - strings
  - srch_strings
  - hachoir-subfile
  - pyew
  - pescanner

YARA

$ cat /usr/local/etc/capabilities.yara | grep oohyeah

```
1  rule embedded_exe
2  {
3      meta:
4      description = "Detects embedded executables"
5
6      strings:
7      $a = "This program cannot be run in DOS mode"
8
9      condition:
10     $a in (1024..filesize)
11 }
12
13 rule mz_executable // from YARA user's manual
14 {
15     condition:
16     // MZ signature at offset 0 and ...
17     uint16(0) == 0x5A4D and
18     // ... PE signature at offset stored in MZ header at 0x3C
19     uint32(uint32(0x3C)) == 0x00004550
20 }
```

REMnux

$ man INetSIM

- INetSIM
  - /etc/inetsim/inetsim.conf
    - #service_bind_address 10.10.10.1
    - #dns_default_ip 10.10.10.1
  - Sample of services …
    - HTTP / HTTPS
    - SMTP / SMTPS
    - POP3 / POP3S
    - DNS
    - FTP / FTPS
    - TFTP
    - IRC
    - NTP
    - Ident
    - Finger
    - Syslog

Foundstone Professional Services
A DIVISION OF McAfee

Questions?