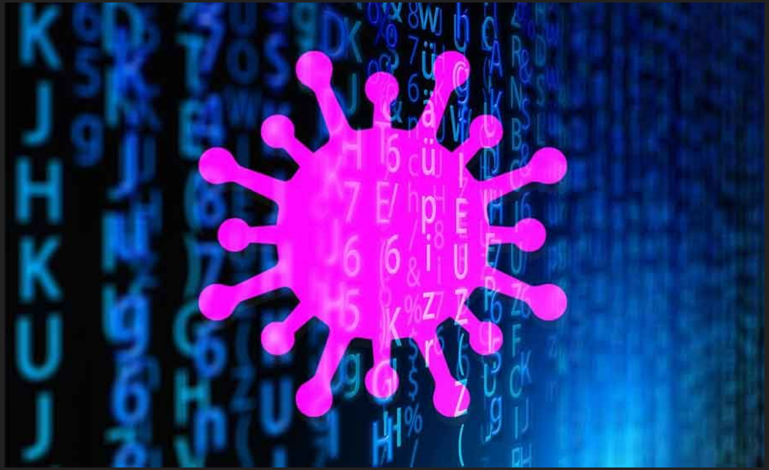
Viruses

Chandler Calkins & Gabriel Jones

Outline

1. Introduction / Recap of viruses
    a. What is a Virus?
    b. Parts of a Virus
    c. Brief History of Viruses
2. How to make a virus
3. How to make Anti-Virus software

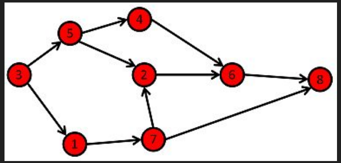


What is a Virus?

- A malicious program that overwrites other programs
- Can either completely replace, or carefully insert code into other programs
- Infected programs can be infected with code that makes them infect even more programs

Parts of a Virus

1. Infection Mechanism
    - How will the virus get into and spread through a system?



2. Payload
    - What will the virus do to the system in addition to spreading itself?

3. Trigger
    - When will the virus activate, and what will cause it to activate?

Brief History of Viruses

Very early viruses weren’t the smartest - but they were extremely effective

- Writing zeros to boot partitions/bios instructions
- Filling up a drive over time to be annoying
- Deleting random files

More modern viruses tend to incorporate other types of MALWARE

- Can be much more specifically targeted
- If attack is successful, result(s) can be catastrophic
  - Ransomware/Data encryption/Personal information digging
  - Phishing emails
  - Secrecy/Undetection (self encryption/mutations)

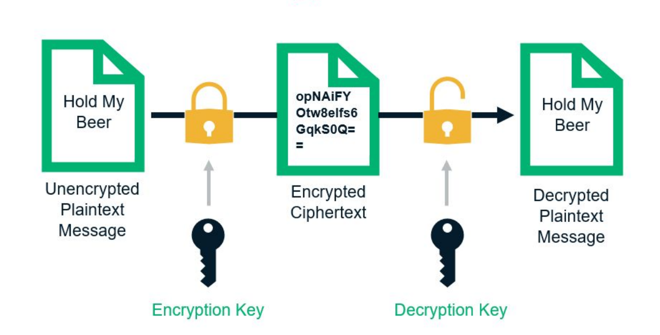
How to Make a Virus

How to make a Virus

- Step 1: Find which programs you want to infect
- Step 2: Determine where you want to place the payload in each file
- Step 3: Create the payload / infection mechanism
- Step 4: Write the payload to the files you want to infect

Polymorphism

- Same payload every time is easy to detect
- Lots of ways to randomize the payload
- Most popular way is using encryption:


Hold My Beer
Unencrypted Plaintext Message
opNAiFY Otw8elfs6 GqkS0Q= =
Encrypted Ciphertext
Hold My Beer
Decrypted Plaintext Message
Encryption Key
Decryption Key

1. Take your payload and turn it into a string

2. Get a random key and encrypt your payload

3. Make it so infected files decrypt that string back into code, and then execute it

Parts of this Virus

- Infection mechanism:
  - Just the root virus program infecting as many python files as it can
- Payload:
  - Makes the keyboard unusable + slightly lags the computer
- Trigger:
  - Running any infected program

How to Make an Anti-Virus

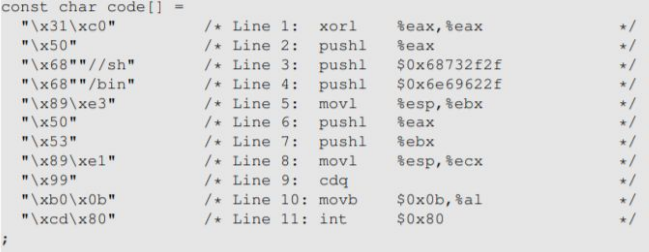
How to make Anti-virus software

Which is more effective?

Why?

Generally 2 main ways

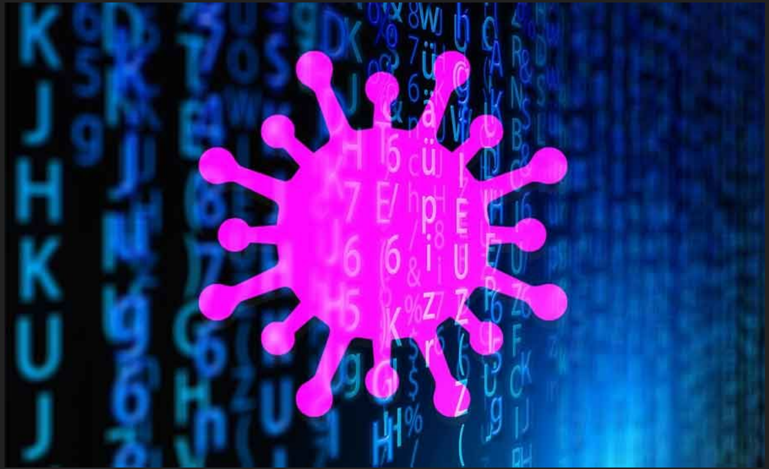
- Behavioral/Pattern/Action Recognition
  - Several files all running the exact same code? Changing by the same length?
  - One program scrubbing large amounts of files?
- Payload (key terms/code) Searching
  - Recall our buffer overflow lab
  - We took advantage of a vulnerability to run this malicious shellcode ---------------------------->
  - These known payloads can be stored in a remote server and added to when more are found



```
const char code[] =
  "\x31\xc0"          /* Line 1:  xorl    %eax,%eax          */
  "\x50"              /* Line 2:  pushl   %eax               */
  "\x68""//sh"        /* Line 3:  pushl   $0x68732f2f        */
  "\x68""/bin"        /* Line 4:  pushl   $0x6e69622f        */
  "\x89\xe3"          /* Line 5:  movl    %esp,%ebx          */
  "\x50"              /* Line 6:  pushl   %eax               */
  "\x53"              /* Line 7:  pushl   %ebx               */
  "\x89\xe1"          /* Line 8:  movl    %esp,%ecx          */
  "\x99"              /* Line 9:  cdq                        */
  "\xb0\x0b"          /* Line 10: movb    $0x0b,%al          */
  "\xcd\x80"          /* Line 11: int     $0x80              */
;
```

Outline

1. Introduction / Recap of viruses
    a. What is a Virus?
    b. Parts of a Virus
    c. Brief History of Viruses
2. How to make a virus
3. How to make Anti-Virus software



Sources + Questions?

- http://etutorials.org/Misc/computer+book/Part+2+Dangerous+Threats+on+the+Internet/Chapter+7+Viruses+and+Worms/HOW+VIRUSES+AVOID+DETECTION/
- https://www.youtube.com/watch?v=2Ra1CCG8Guo
- https://www.youtube.com/watch?v=-TSWzErSxC4

calk9614@vandals.uidaho.edu

jone1291@vandals.uidaho.edu