Malicious Code
Lesson Introduction

- Reasons attackers use malware: automation, scalability, and deniability.
- Attackers release malicious programs on the **Internet** and let them **spread**
- Overview of **malware**

What is Malware? Quiz

What are the estimated yearly losses due to cybercrime worldwide?

- ◯ $100 million - $500 million
- ◯ $500 million - $1billion
- ◯ $100 billion - $500 billion

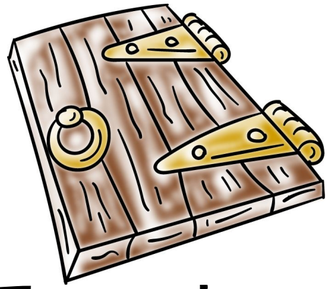
Types of Malicious Software (Malware)

- Needs host program

- Independent

Types of Malicious Software (Malware)

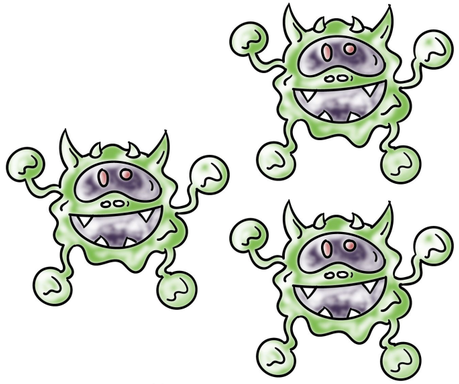
- Needs host program:



Trap doors

Logic bombs

Trojan horses

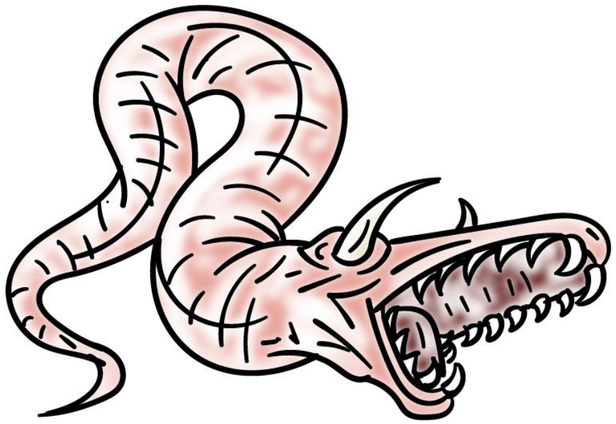


Viruses

Browser plug-ins,
extensions, scripts

Types of Malicious Software (Malware)

- Independent:



Worms

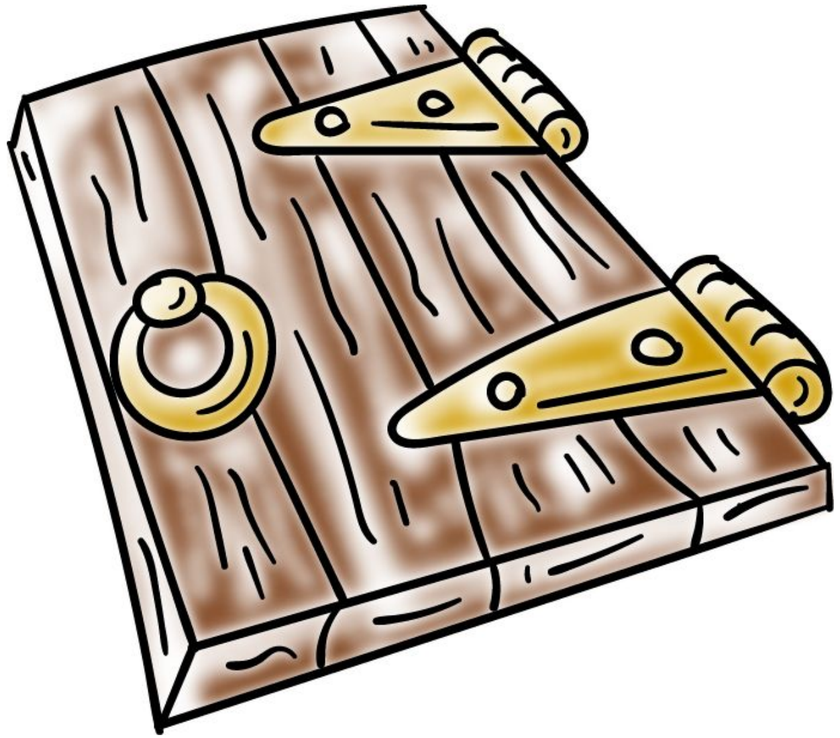
Botnet

APTs

Trap Doors

- A secret entry point to a program or system.

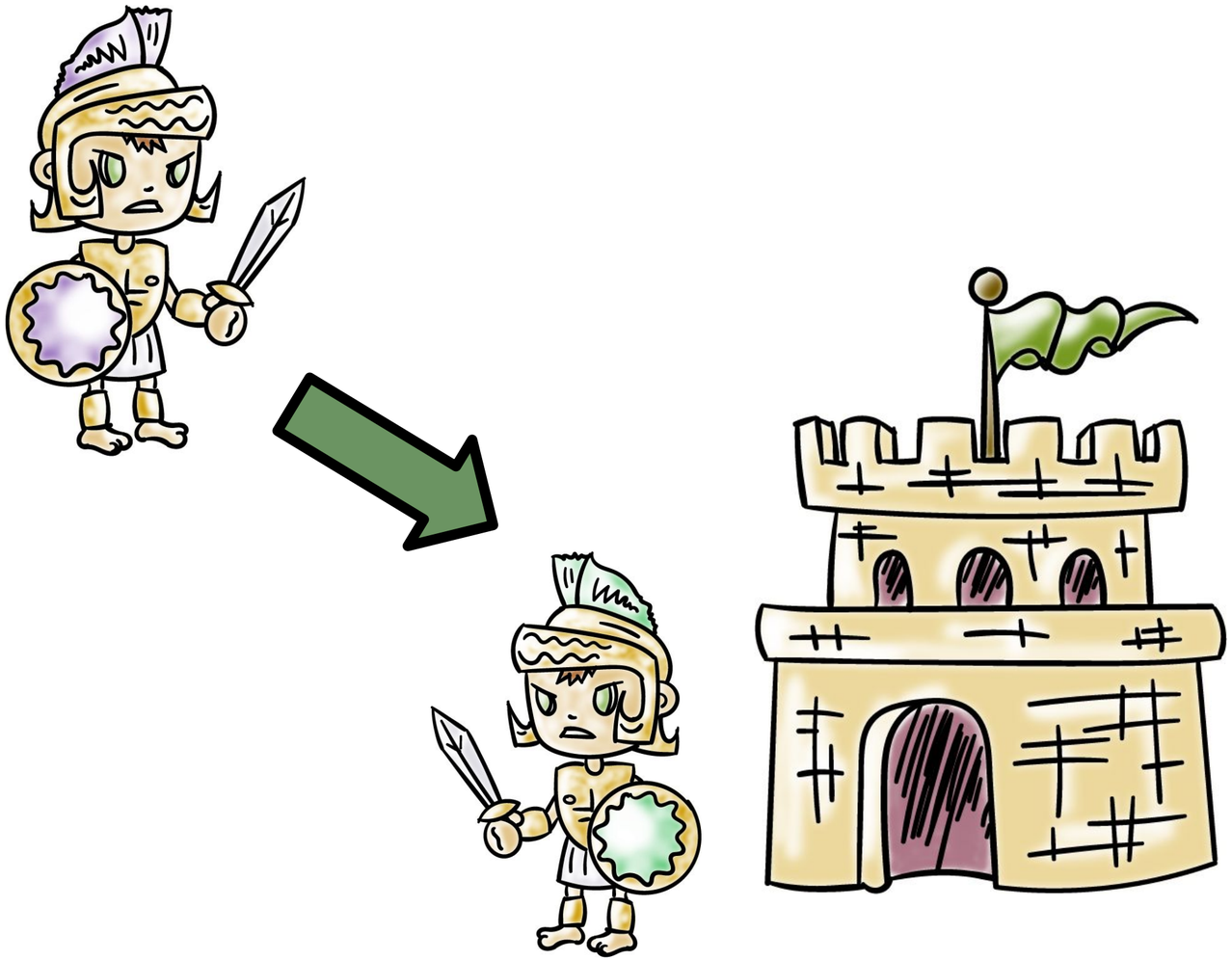
- Typically works by recognizing some special sequence of inputs or special user ID.



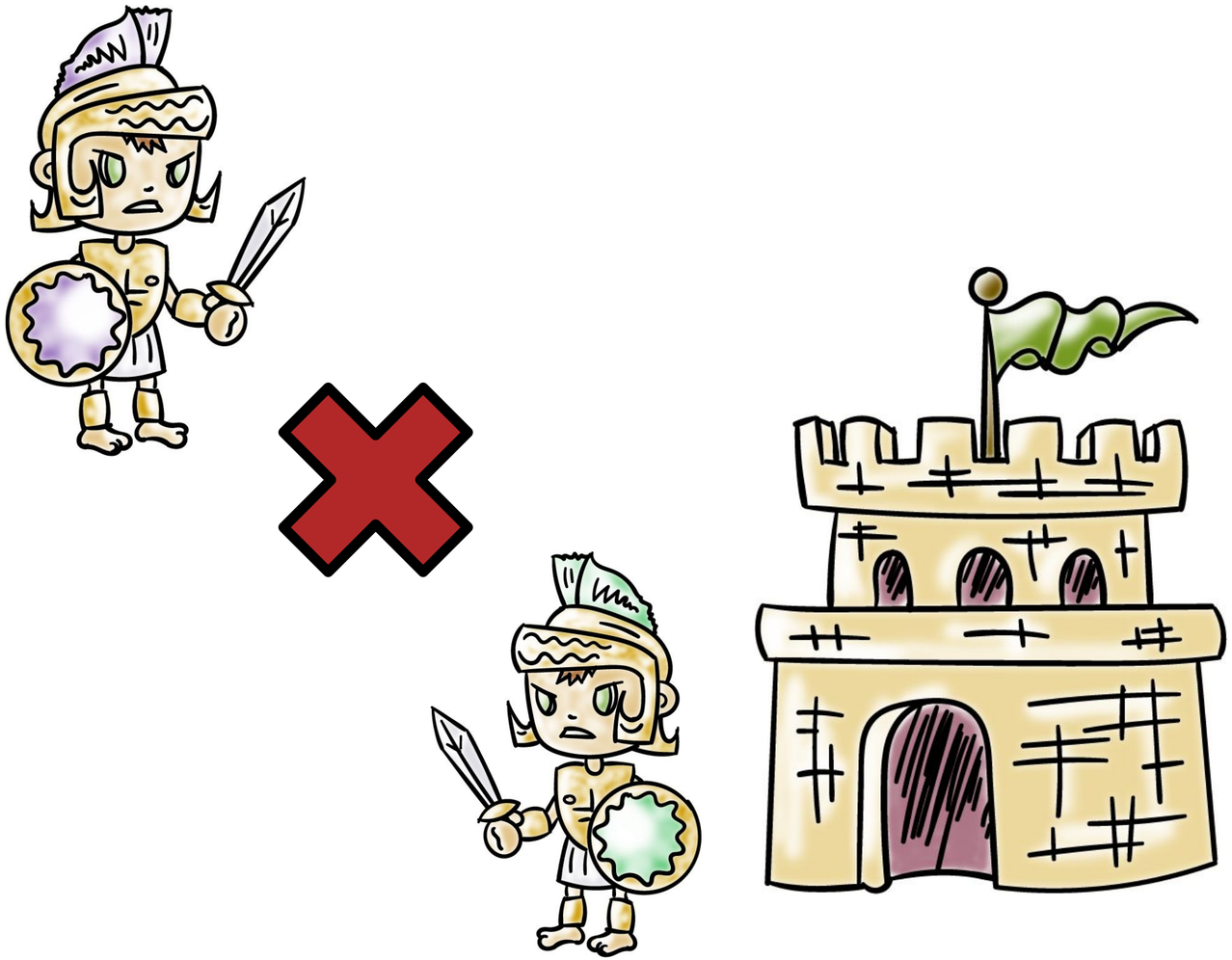
Logic Bombs

- Embedded in some legitimate program
- "Explode" or perform malicious activities when certain conditions are met.

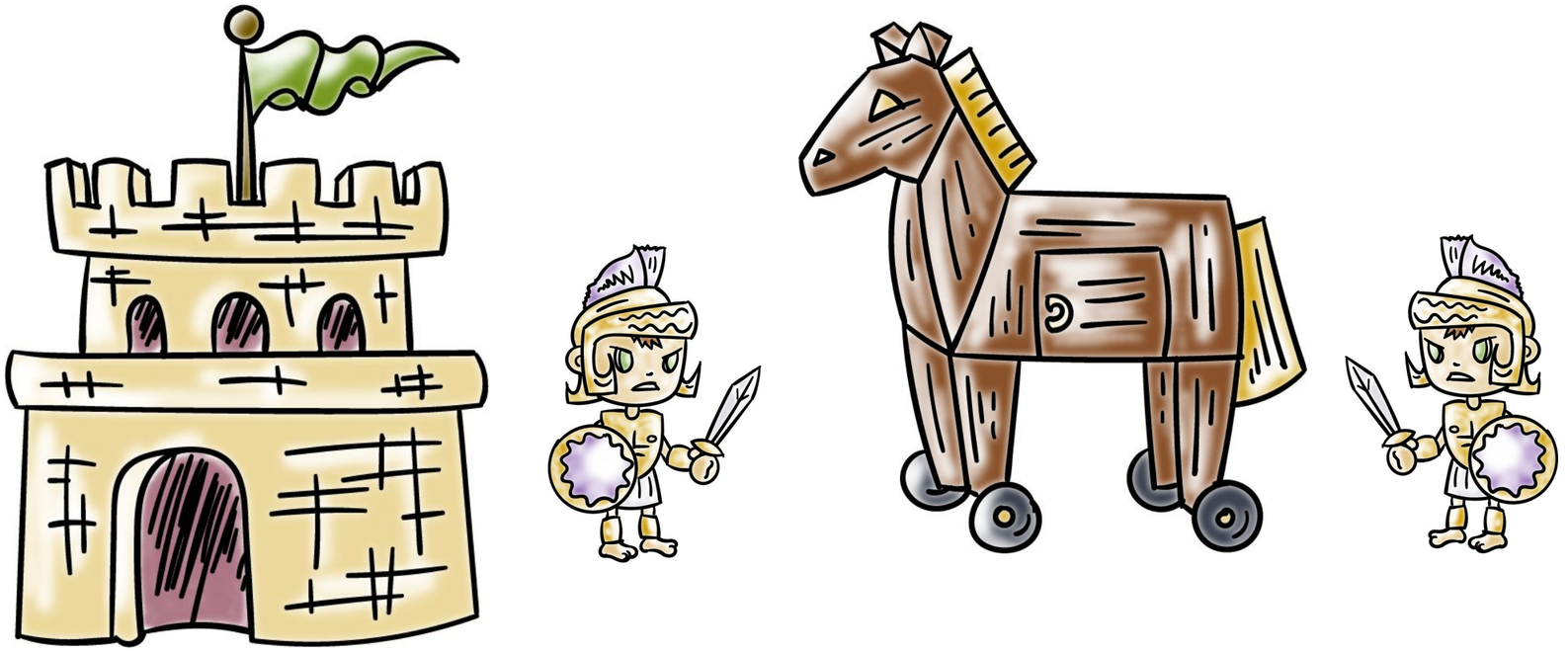
Trojan Horses



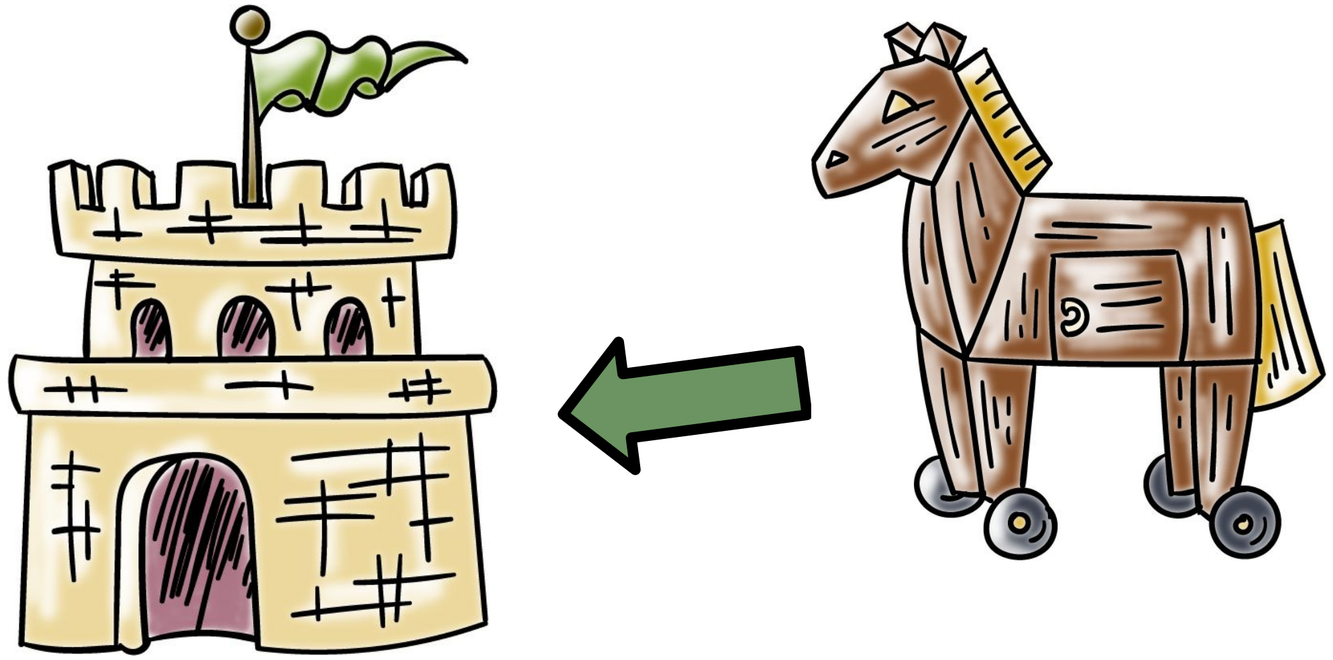
Trojan Horses



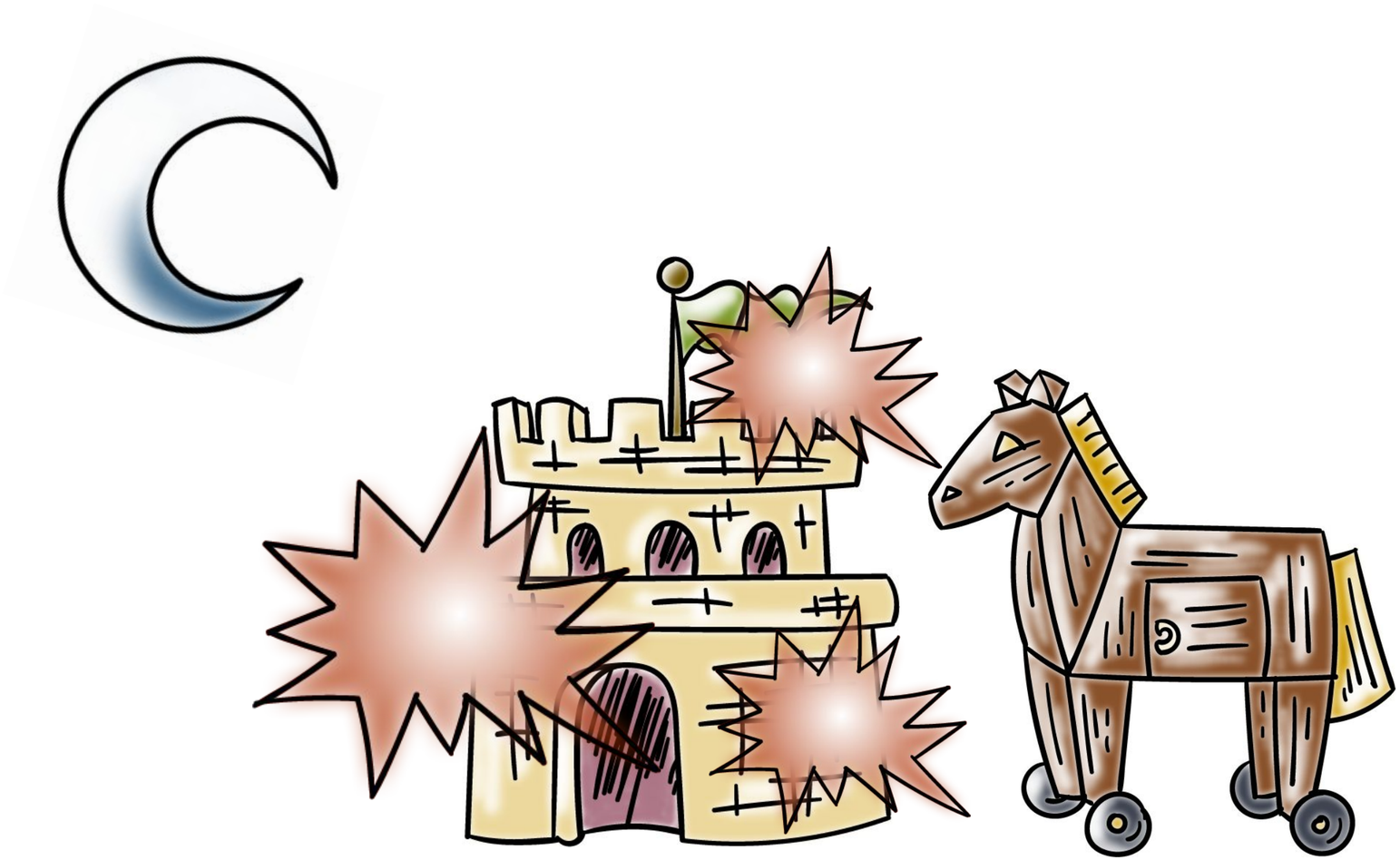
Trojan Horses



Trojan Horses



Trojan Horses



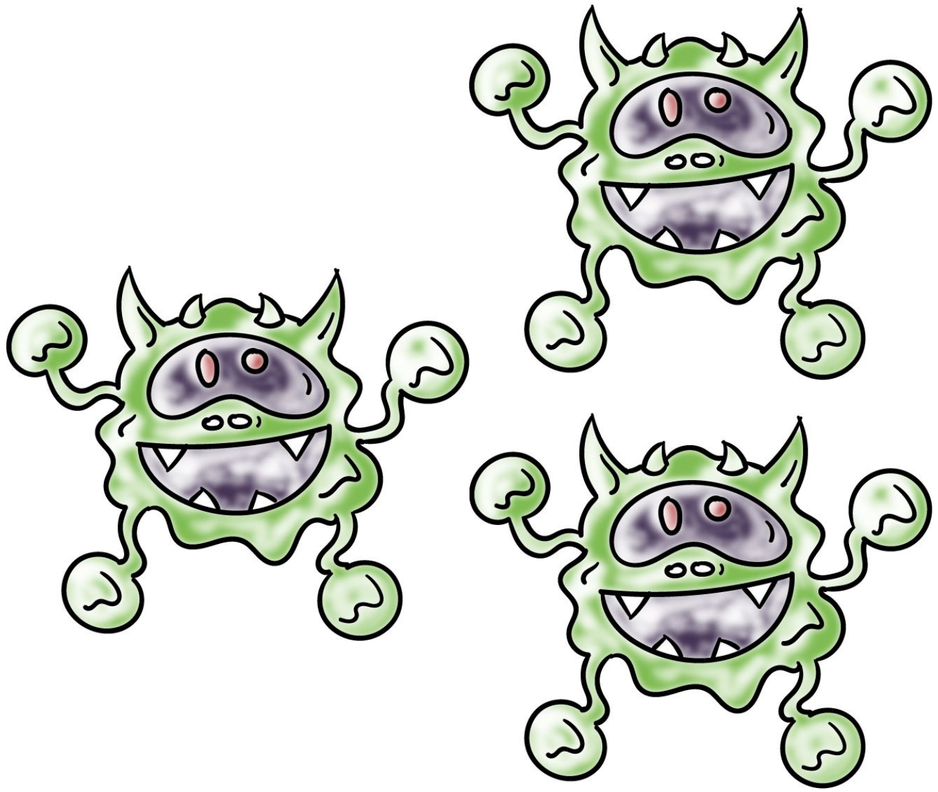
Trojan Horses

Trojan Horses

- Hidden in an apparently useful host program

- Performs some unwanted/harmful function when the host program is executed

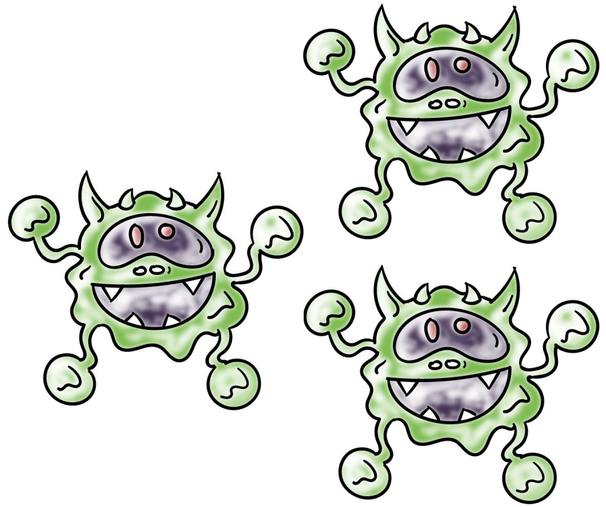
Viruses



- Infect a program by modifying it
- Self-copy into the program to spread

Viruses

Four Stages of Viruses



Dormant Phase

Propagation Phase

- E.g. attachment to email

Triggering Phase

Execution Phase

Host-Required Malware Quiz #1

Determine which category each of these belongs to:

☐ An email attachment that when being opened will send itself to all people in the user's address book.

☐ A customized keyboard app that logs user input and sends it to a server on the Internet.

☐ Part of a program will only run if the computer is at the user's home, and it will upload all MS Word docs to a web site.

☐ A login program with an undocumented option (e.g., DEBUG) that would allow an attacker to supply any username and password to gain access to the computer.

T = trapdoor, L = logic bomb, H = trojan horse, V = virus

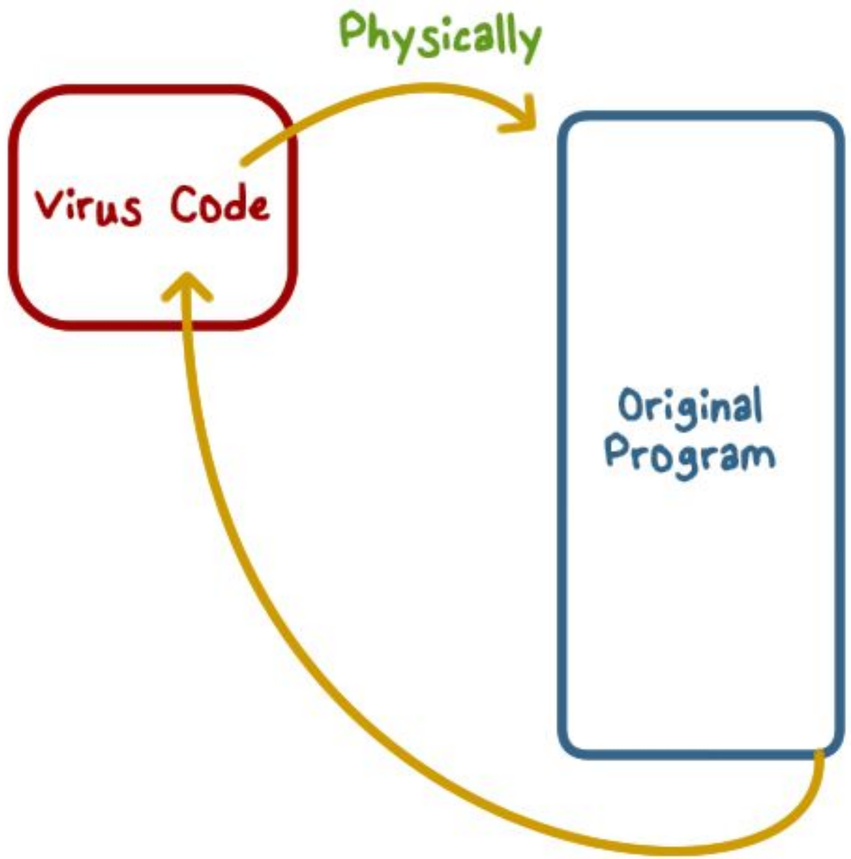
Host-Required Malware Quiz #2

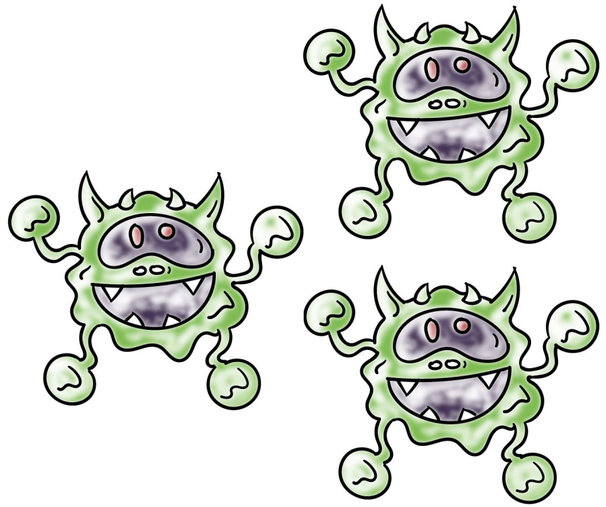
Which type of malware would be best for each of the given tasks?

- ☐ spy on employees of a specific company
- ☐ cripple an organization's computers
- ☐ quickly spread information and drive traffic to a specific website

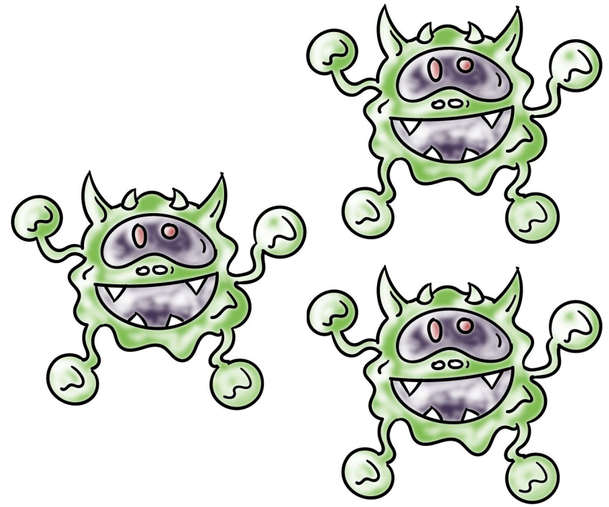
T = trapdoor, L = logic bomb, H = trojan horse, V = virus

Virus Structure



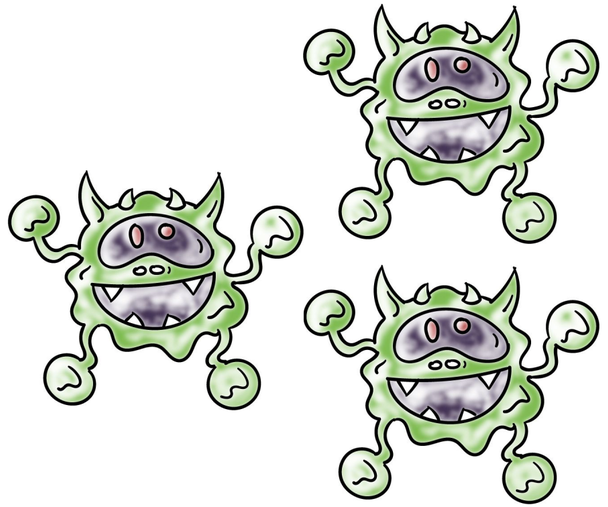


Virus Structure



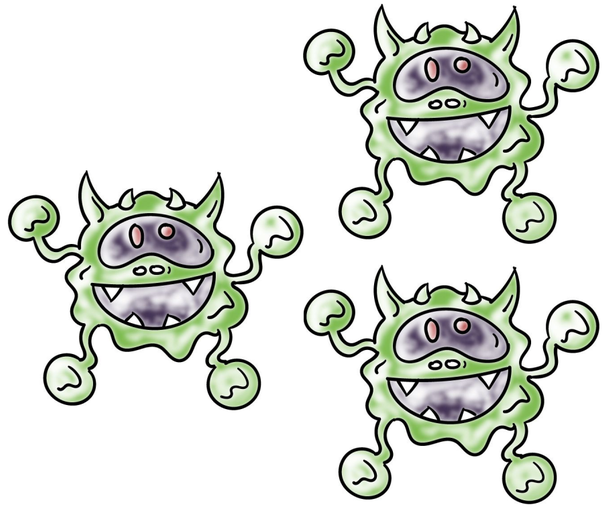
- First line: go to "main" of virus program
- Second line: a special flag (infected or not)
- Main:
    - Find uninfected programs - infect them
    - Do something damaging to the system
    - "Go to" first line of the host program - do normal work
- Avoid detection by looking at size of program
    - Compress/decompress the host program

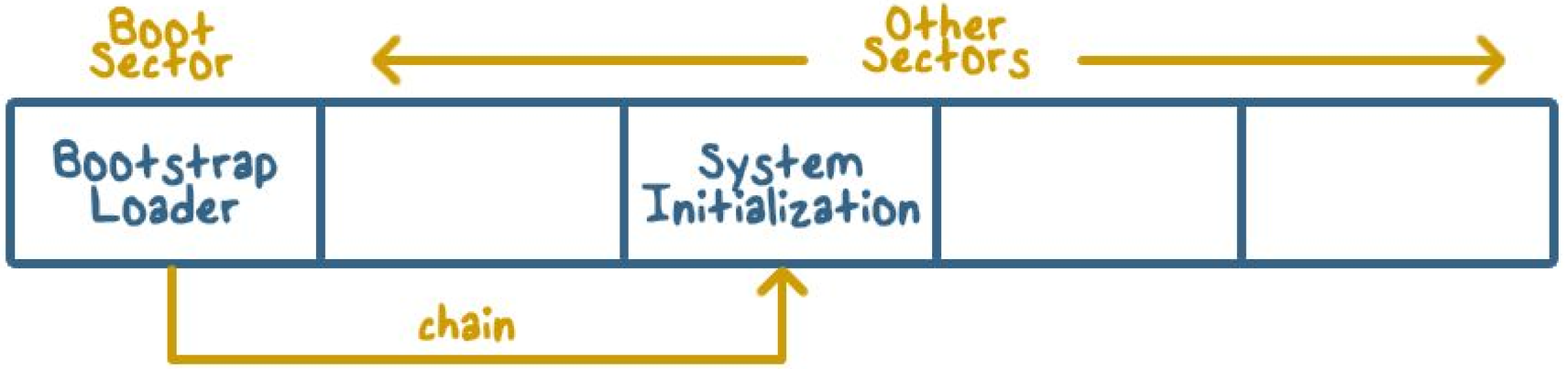
Types of Viruses



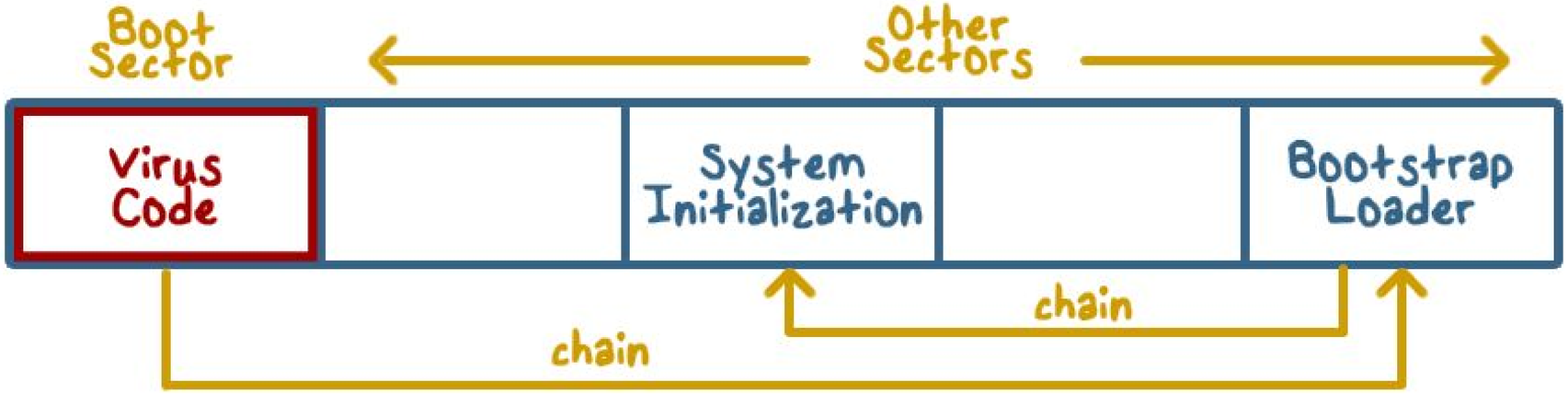
- Parasitic virus: scan/infect programs
- Memory-resident virus: infect running programs
- Macro virus: embedded in documents, run/spread when opened
- Boot sector virus: run/spread whenever the system is booted
- Polymorphic virus: encrypt part of the virus program using a randomly generated key

Boot Sector Virus





(a) Before infection



(b) After infection

Types of Viruses Quiz

Which type of virus begins on the operating system level?

- ◯ Macro virus
- ◯ Boot sector virus
- ◯ Memory-resident virus

Macro Viruses

Macro:

- An executable program (e.g. instructions opening a file, starting an application) embedded in a word processing document, e.g. MS Word

Macro Viruses

A common technique for spreading:

- A virus macro is attached to a Word Document
- Document is loaded and opened in the host system
- When the macro executes, it copies itself to the global macro file
- The global macro can be activated/spread when new documents are opened

Rootkit

- Resides in operating systems
  - Modifies OS code and data structure
- Helps user-level malware
  - E.g., hide it from user (not listed in "ls" or "ps" command)

Rootkit

Inspect all files

```
FindFirstFile()
{ checkfile
  FindNextFile()
  repeat
```

Windows API

NTQueryDirectoryObject

kernel Native Interface

Device driver functions

Drivers

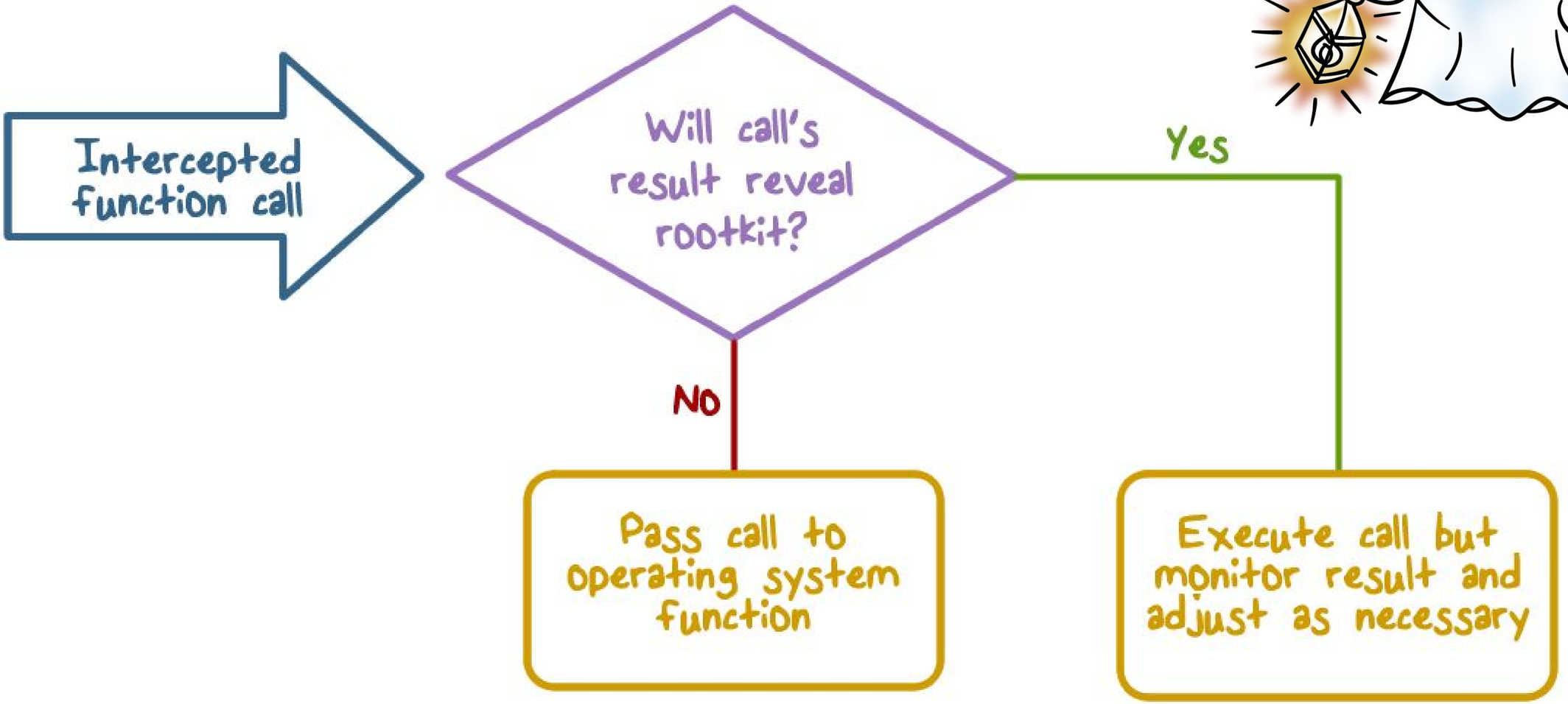
Rootkit

```
Volume in drive C has no label.
 Volume Serial Number is E4C5-A911

 Directory of C:\WINNT\APPS

01-09-10   13:34    <DIR>          .
01-09-10   13:34    <DIR>          ..
24-07-02   15:00            82,944 CLOCK.AVI
24-07-02   15:00            17,062 Coffee Bean.bmp
24-07-02   15:00                80 EXPLORER.SCF
24-07-08   15:00           256,192 mal_code.exe
22-08-04   01:00           373,744 PTDOS.EXE
21-02-04   01:00               766 PTDOS.ICO
19-06-03   15:05            73,488 regedit.exe
24-07-02   15:00            35,600 TASKMAN.EXE
14-10-02   17:23           126,976 UNINST32.EXE
               9 File(s)        966,852 bytes
               2 Dir(s) 13,852,132,800 bytes free
```

Rootkit


Intercepted function call
Will call's result reveal rootkit?
Yes
No
Pass call to operating system function
Execute call but monitor result and adjust as necessary

Rootkit

Inspect all files

```
FindFirstFile()
{ checkfile
  FindNextFile()
  repeat
```

Windows API

NTQueryDirectoryObject

kernel Native Interface

Rootkit filters call and results

Device driver functions

Drivers

Rootkit

```
Volume in drive C has no label.
 Volume Serial Number is E4C5-A911

 Directory of C:\WINNT\APPS

01-09-10   13:29       <DIR>          .
01-09-10   13:29       <DIR>          ..
24-07-02   15:00            82,944 CLOCK.AVI
24-07-02   15:00            17,062 Coffee Bean.bmp
24-07-02   15:00                80 EXPLORER.SCF
22-08-04   01:00           373,744 PTDOS.EXE
21-02-04   01:00               766 PTDOS.ICO
19-06-03   15:05            73,488 regedit.exe
24-07-02   15:00            35,600 TASKMAN.EXE
14-10-02   17:23           126,976 UNINST32.EXE
               8 File(s)        710,660 bytes
               2 Dir(s) 13,853,472,768 bytes free
```

Rootkit Quiz

Which operating systems can be affected by Rootkit?

- ◯ Linux
- ◯ iOS
- ◯ Windows
- ◯ Android

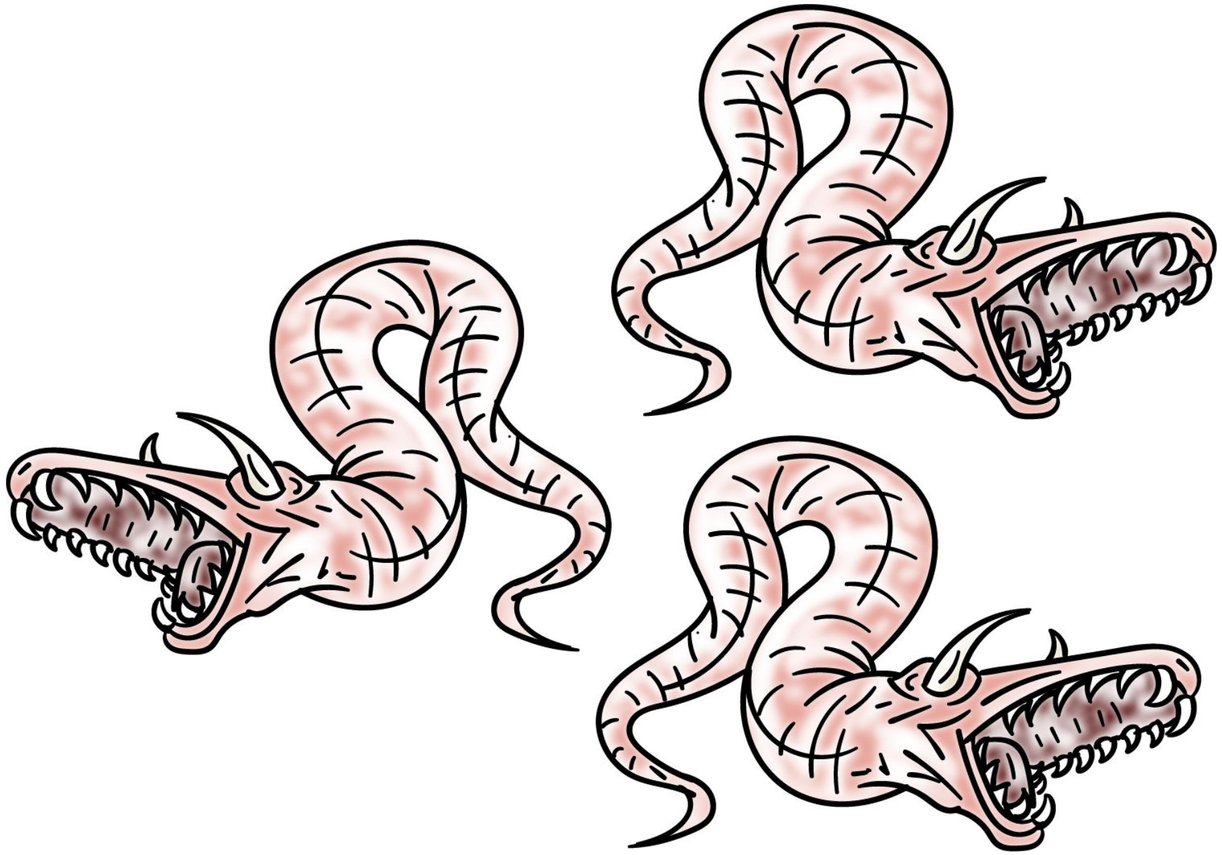
Truth and Misconceptions about Malicious Software Quiz

Put a 'T' in the box for any statement you think is true and an 'F' for any statement you think is false.

- [ ] Can only infect Microsoft Windows
- [ ] Can modify hidden and read-only files
- [ ] Spread only on disks or in email
- [ ] Cannot remain in memory after reboot
- [ ] Cannot infect hardware
- [ ] Can be malevolent, benign, or benevolent

Worms

- Use network connections to spread from system to system

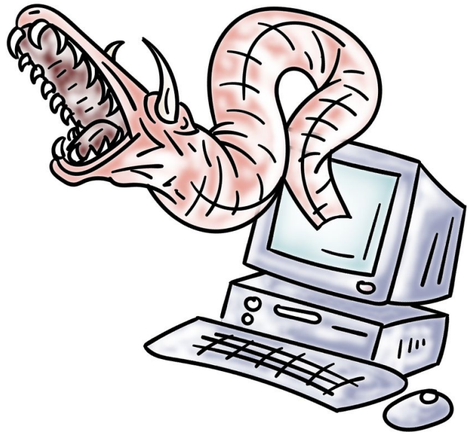


The Internet Worm

What it did:

- Determine where it could spread
- Spread its infection
- Remain undiscovered and undiscoverable

The Internet Worm

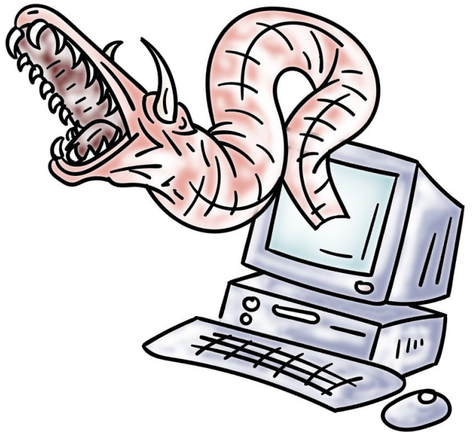


Effect:

Resource exhaustion - repeated infection due to programming bug

- Servers are disconnected from the Internet by system admin to stop the infection

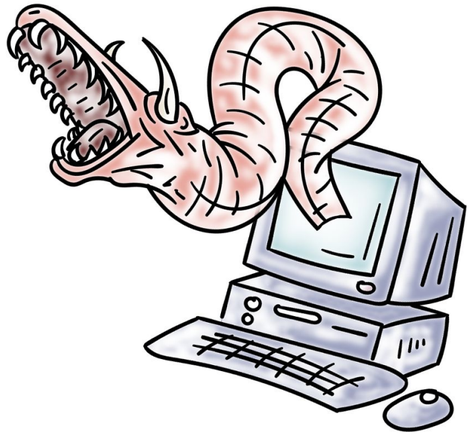
The Internet Worm



- Exploit security flaws
  - Guess password (encrypted passwd file readable)
  - fingerd: buffer overflow
  - sendmail: trapdoor (accepts shell commands)

- Spread
  - Bootstrap loader to target machine, then fetch
  - rest of code (password authenticated)

The Internet Worm

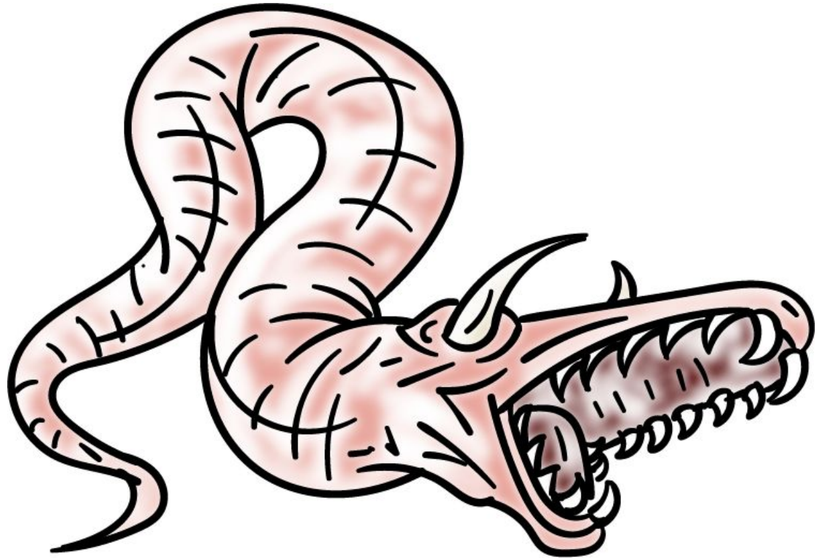


- Remain un-discoverable
  - Load code in memory, encrypt, remove file
  - Periodically changed name and process ID

- What we learned:
  - Security scanning and patching
  - Computer Emergency Response Team

Worm Quiz

Which of the following methods can be used to spread a worm? Check all that apply:



- [ ] email
- [ ] instant messaging
- [ ] downloading files
- [ ] watching a video on netflix
- [ ] clicking on a popup
- [ ] using facebook

Malware Prevention & Detection Approaches

- **Prevention:** Limit contact to outside world
- Detection and Identification
- Removal

Malware Prevention & Detection Approaches

4 Generations of antivirus software:

- Simple scanners: Use "signatures" of known viruses
- Heuristic scanners: Integrity checking: checksum, encrypted has
- Activity traps
- Full-featured analysis: Host-based, network-based, sandboxing-based

Malware Prevention & Detection Quiz

Given that signature-based anti-virus solutions are not always effective, why do we still use them?
Check all that apply:

- [ ] they are very efficient
- [ ] effective against known malware good
- [ ] "first-line" defense

The Most Expensive Worm Quiz

Which of the worms described below caused the greatest financial damage?

- ILOVEYOU: Sent by email with the subject "ILOVEYOU" It had an attachment that, when executed, deleted all files on the host computer.
- CODE RED: a worm that took advantage of a buffer overflow vulnerability in Microsoft servers. Infected machines would launch 'denial of service' on IP addresses.
- Morris Worm: 99 lines of code that Robert Morris, a Cornell student launched to find out the size of the internet.

Malicious Code
Lesson Summary

Host-dependent malware:

- trap doors
- logic bombs
- trojan horses and
- viruses

Host-independent malware:

- Worms
