Malicious Software

Reese Hatfield

Malicious Software

- All form of bad actors we've discussed so far

- All gain some amount of information
  - Passwords, etc
- Through some manual intervention

Malicious Software

- But attackers rarely do things by hand
- That would simply take too much time
  - Or too much effort
  - Too many users

- Digital age ⇒ everything is software

Malicious Software

- Attacks will instead write malicious software to do their dirty work
- Software
  - Just some piece of code really
  - Interacts will existing software
    - Usually your operating system

Malicious Software

- Call this malicious software
  - “Malware”
- Probably mildly familiar with this
- Many famous examples of malware
- A few distinct categories
  - We’ll look at about a few

Ransomware

- Ransomware
- Hijacks your computer
    - Usually containing sensitive data
- Encrypts that data
- Does not give you the key
- If you pay money, they give you key

Ransomware

- WannaCrypt
- Famous example

- Want crypto currency

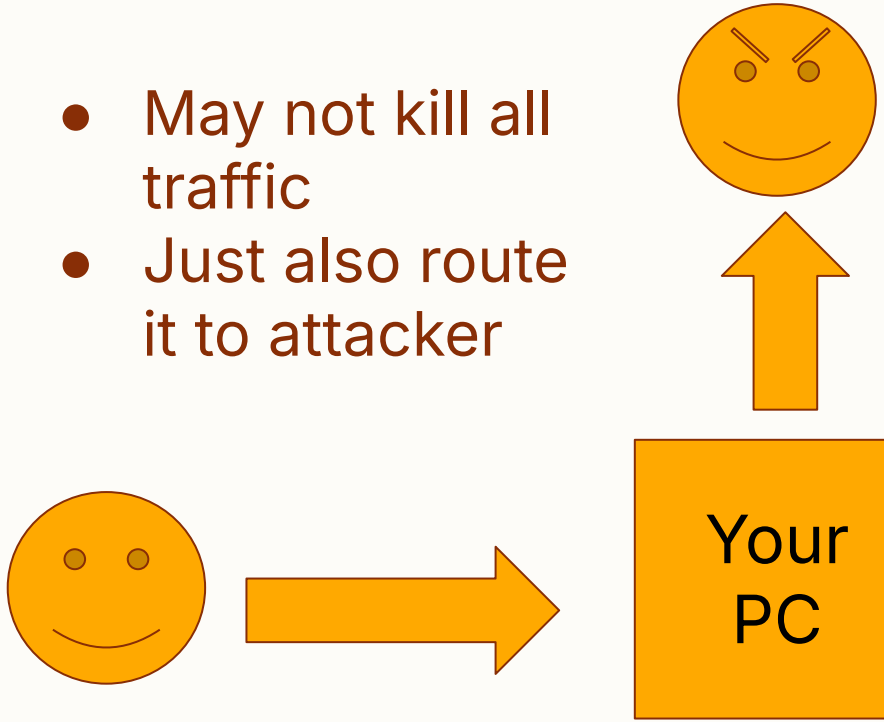
Spyware

- Spyware
- Doesn’t completely hijack
- Want to go unnoticed

- Secretly steal all sensitive data
- Send it over to an attacker

Spyware

- May not kill all traffic
- Just also route it to attacker



- Steal as much info as possible
- Over the air

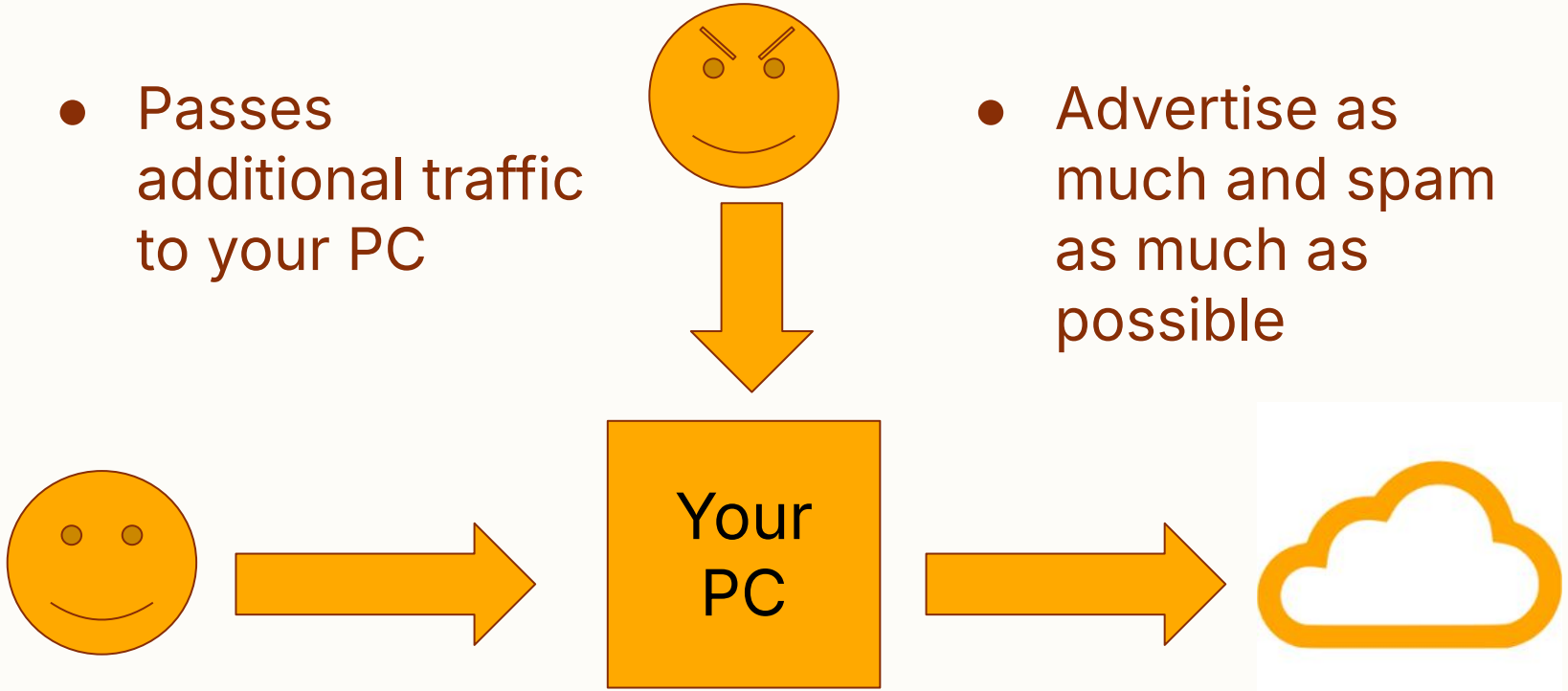
Adware

- Advertisement injection software
- Also usually “quiet”
- Quiet may be a misnomer

- Spam the user with advertisments

Adware

- Passes additional traffic to your PC



- Advertise as much and spam as much as possible

Adware


http://ads1.revenue.net - ExclusiveRewards - Microsoft Internet Explorer
CONGRATULATIONS!
You've been chosen to receive a
FREE Gateway Desktop Computer!
Intel Pentium 4 Processor 2.66 GHz
256MB DDR-SDRAM, 80GB HD, 48x CD-RW
19-inch Color CRT Monitor (18-inch viewable)
Click Here to Claim Your FREE Desktop Computer!
FREE!
Microsoft Internet Explorer
Click OK to download our free software while browsing the site
OK
Cancel
POKER ON-NET
Download
Getting Started
Features
Contact Us
Help
> Current Events
Finale
$5,000
Black Jack
Roulette
Slot Machine
Click Here!
Recycle Bin
start

Viruses

- Designed for pure harm*
- Often combined with other types of malware
- Attach themselves to a “host”
- Can replicate themselves
  - Upon human interaction
  - Opening an email, etc

Viruses

- ILOVEYOU
- 2000
- Famous Email Virus

45 Million devices Infected in 24 hours

Viruses

- Corrupted all your files
- Sent itself to ALL of your email contacts

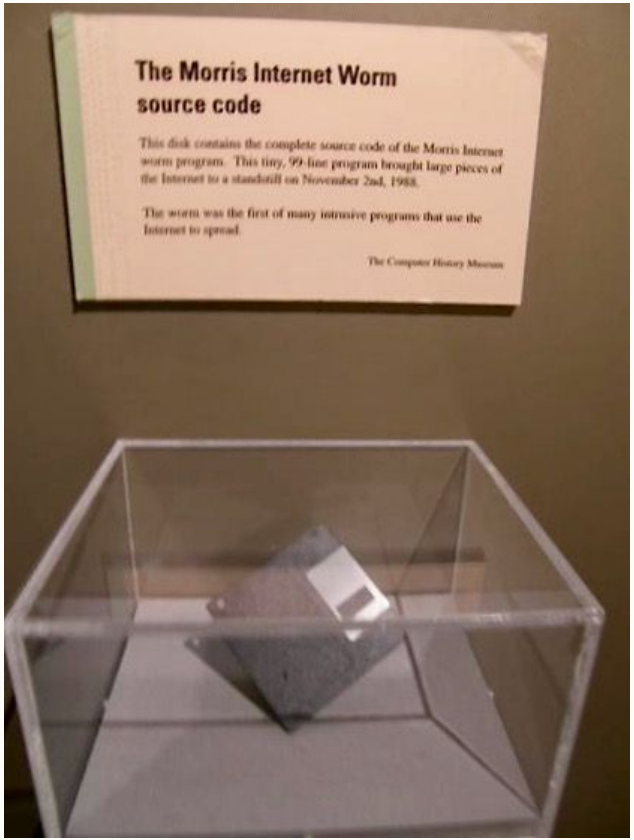
Worms

- Self-Replicating
- Unlike Viruses, worms require NO manual intervention to spread

- Super dangerous
- Rely on vulnerabilities in existing technologies

Worms

- Morris Worm
- 1988
- Spread via the internet
- Left files intact, but slowed system dramatically
- Cripled the early internet



Trojans

- Usually* don’t self replicate
- Sneak on to your computer

- Disguise itself as legitimate software
- Maybe a fake download link
- software.wright.edu
- software.wrihgt.edu

Trojans

- Zeus
- Late 2000s

- Logged your keyboard input
- Stole bank account information
- Made itself hard to detect

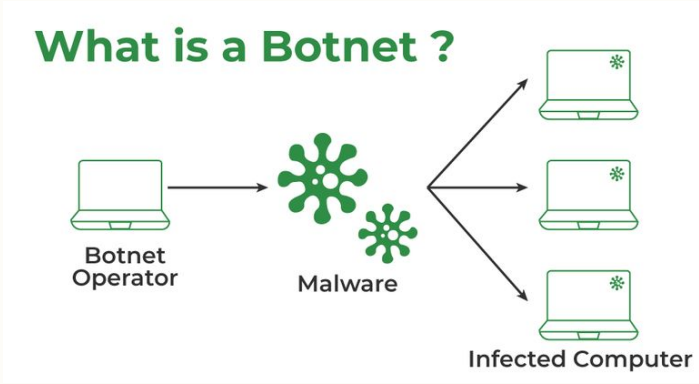
Botnets

- Sneak onto your device through some existing means
- Run some program on your computer
- Maybe not make it entirely unusable

- Maybe just a bit slower

Botnets

- Split this program up across MANY infected devices
- All connect to some remote device
- Steal computer power for other tasks



Malware

- Malware used to target end users a lot more

- See early 2000s “virus” examples
- I’m sure you have some stories

Malware

- Modern malware often targets companies and corporations

- Large businesses
  - Have a lot of data
  - As opposed to a single user

Malware

- Global scale attacks
- Government warfare
- Modern ideas of defense
- Locally
  - Kettering Health

Malware

- Defense and Military
- Cybersecurity is even more important
- SCIFs

Malware

- We covered a bunch of distinct categories
- But these are really just properties of malware

- They are almost always combined into a larger malicious program

Malware

- Your modern browser is very secure

- You can configure your firewall
  - Network access configator
- To block suspicious traffic