Large Botnets and Distributed Denial of Service Attacks

CS 161/194-1
Anthony D. Joseph
October 28, 2005

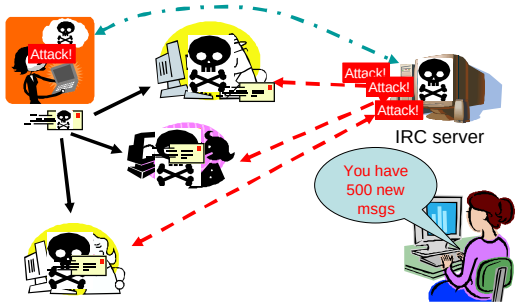
Outline

- What is a botnet?
- How to create and use a botnet
- The money trail…
- Distributed Denial of Service Attacks
- Examples

What is a Botnet?

- A network of compromised machines
  - See last lecture for compromise techniques
- Zombies connect to server(s)
  - Typically one or more IRC servers running on zombies
  - Some botnets use custom encrypted protocols
- Zombies await commands or perform pre-determined actions (e.g., send spam)
  - Some botnets require authenticated commands
  - Commands can be scripts or executables

Creating and Using a Botnet



Botnets

- Typically rented to “users”
  - Cost depends on metrics of botnet
- Important metrics (“bragging rights”)
  - Number of machines (1,000’s – 100,000’s)
  - Aggregate bandwidth (gigabits – terabits)
- Can be rented for campaign or for time

Uses for Botnets

- Send spam, spyware, adware, and phishing e-mail
  - Also, hosting phishing websites
- Click-for-pay fraud
- Distributed programming
  - Example: password cracking
  - Distributed servers to control the botnet
- Distributed Denial of Service (DDoS) attacks
  - Overwhelm server and/or network links
  - Political msgs, fame/bragging
  - Extortion (“pay or your site and business die”)

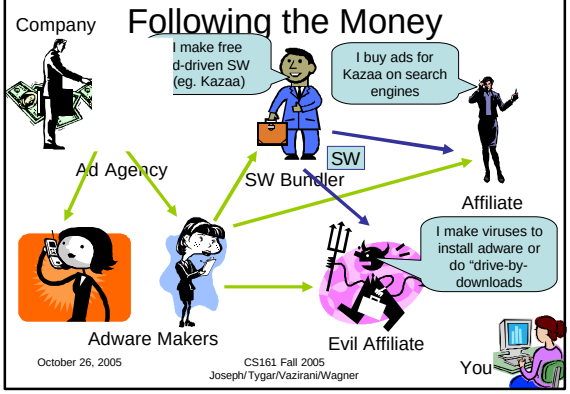
Outline

- What is a botnet?
- How to create and use a botnet
- The money trail…
- Distributed Denial of Service Attacks
- Examples

The Money Trail…

- Popup ads start appearing on Joe's PC
  - For well-known brands (Chrysler, Expedia, Microsoft, Priceline, and Travelocity)
  - Each has border saying it is from "Aurora"
- Aurora is adware from Direct Revenue
  - But, Joe doesn't remember installing it…
- The adware industry has a $200 million to $2 billion a year revenue stream
- How does the ad go from Priceline to Joe?

Following the Money



Malicious Affiliates

- Most adware/spyware vendors claim they prohibit drive-by-download and virus-based installs
- But, there's a strong profit incentive, since they get paid based on the number of "eyeballs"…
- Some even sue adware/spyware detection companies for labeling thing as such!!

Outline

- What is a botnet?
- How to create and use a botnet
- The money trail…
- Distributed Denial of Service Attacks
- Examples

DDoS Attacks

- Overwhelm server and/or network links
  - Typical target is web server(s)
  - Try to consume all resources (BW, disk space, CPU)
- Simple: same req. for large images/complex action
  - Might be able to create packet filter to block
  - Might also be able to block source subnets
  - Have to put filters into the network (at upstream ISPs)
- Complex: Vary requests, rate, zombie set
  - Harder to create packet filter (esp. if requests look "real")
  - Rotating set makes source subnet blocks hard
  - Only choice may be to add more and more HW and BW

Toxbot Trojan (Oct 10, 2005)

- Three Dutch crackers (19, 22, and 27)
- Used Toxbot Trojan (aka Codbot) to infect machines
  - Installed adware and spyware on user' machines
  - Conducted DDoS attack against a US company for extortion (pay or crash your site)
  - Conducted phishing attacks to hijack PaPal and eBay accounts, then bought goods with accounts
- Estimated network size of 100K
- Investigators later discovered true size (>1.5M!)

Microsoft Decoy Zombie

- Intentionally infected a machine with zombie code
- Within 20 days:
  - PC received > 5 million connections!
  - Tried to send 18 million spam e-mails containing ads for 13,000 unique domains!
- October 27, 2005: filed 13 "John Doe" lawsuits against spammers
  - Enables them to subpoena ISPs and domain registrars for identities