Botnets

- A collection of compromised machines
- Under control of a single person
- Organized using distributed system techniques
- Used to perform various forms of attacks
  - Usually those requiring lots of power

What Are Botnets Used For?

- Spam (90% of all email is spam)
- Distributed denial of service attacks
- Hosting of pirated content
- Hosting of phishing sites
- Harvesting of valuable data
  - From the infected machines
- Much of their time spent on spreading

Botnet Software

- Each bot runs some special software
  - Often built from a toolkit
- Used to control that machine
- Generally allows downloading of new attack code
  - And upgrades of control software
- Incorporates some communication method
  - To deliver commands to the bots

Botnet Communications

- Originally very unsophisticated
  - All bots connected to an IRC channel
  - Commands issued into the channel
- Most sophisticated ones use peer technologies
  - Similar to some file sharing systems
  - Peers, superpeers, resiliency mechanisms
  - Conficker's botnet uses peer techniques
- Stronger botnet security becoming common
  - Passwords and encryption of traffic

Botnet Spreading

- Originally via worms and direct break-in attempts
- Then through phishing and Trojan Horses
  - Increasing trend to rely on user mistakes
- Conficker uses multiple vectors
  - Buffer overflow, through peer networks, password guessing
- Regardless of details, almost always automated

Characterizing Botnets

- Most commonly based on size
  - Estimates for Conficker over 5 million
  - Zeus-based botnets got 3.6 million machines in US alone
  - Trend Micro estimates 100 million machines are members of botnets
- Controlling software also important
- Other characteristics less examined

Why Are Botnets Hard to Handle?

- Scale
- Anonymity
- Legal and international issues
- Fundamentally, if a node is known to be a bot, what then?
  - How are we to handle huge numbers of infected nodes?

Approaches to Handling Botnets

- Clean up the nodes
  - Can't force people to do it
- Interfere with botnet operations
  - Difficult and possibly illegal
  - But some recent successes
- Shun bot nodes
  - But much of their activity is legitimate
  - And no good techniques for doing so

Spyware

- Software installed on a computer that is meant to gather information
- On activities of computer's owner
- Reported back to owner of spyware
- Probably violating privacy of the machine's owner
- Stealthy behavior critical for spyware
- Usually designed to be hard to remove

What Is Done With Spyware?

- Gathering of sensitive data
  - Passwords, credit card numbers, etc.
- Observations of normal user activities
  - Allowing targeted advertising
  - And possibly more nefarious activities

Where Does Spyware Come From?

- Usually installed by computer owner
  - Generally unintentionally
  - Certainly without knowledge of the full impact
  - Via vulnerability or deception
- Can be part of payload of worms
  - Or installed on botnet nodes

Malware Components

- Malware is becoming sufficiently sophisticated that it has generic components
- Two examples:
  - Droppers
  - Rootkits

Droppers

- Very simple piece of code
- Runs on new victim's machine
- Fetches more complex piece of malware from somewhere else
- Can fetch many different payloads
- Small, simple, hard to detect

Rootkits

- Software designed to maintain illicit access to a computer
- Installed after attacker has gained very privileged access on the system
- Goal is to ensure continued privileged access
  - By hiding presence of malware
  - By defending against removal

Use of Rootkits

- Often installed by worms or viruses
  - E.g., the Pandex botnet
  - But Sony installed rootkits on people's machines via music CDs
- Generally replaces system components with compromised versions
  - OS components
  - Libraries
  - Drivers

Ongoing Rootkit Behavior

- Generally offer trapdoors to their owners
- Usually try hard to conceal themselves
  - And their other nefarious activities
  - Conceal files, registry entries, network connections, etc.
- Also try to make it hard to remove them
- Sometimes removes others' rootkits
  - Another trick of the Pandex botnet