Malware
Botnet and DDoS

Md. Safiqul Islam
Internetworking
2007-2008
Malware

• A set of instructions or a software to enter into a user computer without the users permission.
• Spyware, botnet, DDos, Crimeware, Badware, Trojans, Worms etc.
• It is not a bug or defect of a software program.
• Often comes with adware, freeware or music files, spam.
What it does?

- Change the system settings.
- Installs unauthorized dialer.
- Installs Keystroke logger.
- Captures personal information.
- Use the computer resources.
Botnet

- A Botnet is a network of trojanized computers, reporting to and commanded via a MasterServer.
- Group of computers compromised without owners permission.
- Controlled and upgraded via IRC or P2P.
- Operated under a single hacker - Botmaster

- Used as the platform for various Attacks:
  - DdoS (Distributed Denial of Service) attacks,
  - Social engineering and related e-mail spamming,
  - Remote exploits, or via keyloggers and network traffic sniffers.
Botmaster

• Control botnet in three ways:
  - Centralize:
    Advantage:
    - Most popular method.
    - Support larger number of bots
    Disadvantage:
    - Single point of failure

Peer to Peer
- Don't rely on single server.
- Smaller group of bots.

Random
- Not implemented in real world.

Command & Control server

Select

Initialization

Zombie machines

Figure: Centralize Method
Creation of Botnet and send spam Mail
Modern Bots

- Modern bots: Agobot (PhatBot, SDBot), GTBot.
- Agobots:
  - 20,000 lines of C/C++ code
  - IRC-based command and control
  - Capable of many DoS flooding types
How to Prevent

- Two Fold Protection
  - From the “inside” to be immune to:
    - Data exfiltration
  - From the “outside” to be immune to:
    - Intrusion
    - DoS attacks
Protecting from bots inside the corporate network

• Firewall rules should be appropriate.
  – Break communication to the master server
  – Default rule for both inbound and outbound connections: Deny
  – Allow important services for outbound connections (e.g.: HTTP, SMTP, SSH)
  – Enforce the use a HTTP proxy, so that port 80 is closed for users.
  – e.g. W32/Dumador.DH is a “full HTTP” bot
Protecting from bots inside the corporate network (Cont’d)

- Sniffing outbound traffic on the gateway for **keywords** used in Bot/Master communications:
  - .login
  - .scan
  - .status
  - .sysinfo

- Set up a **DNS redirection** to an in-house **honeypot** for blacklisted bot master servers => unveil the infected hosts

Figure 5: Network topology placing the IRC honeypot in the DMZ
Distributed Denial of Service (DDoS)

• Build a botnet of zombies
  – Multi-layer architecture: use some of the zombies as “masters” to control.
• Command zombies to stage a coordinated attack on the victim.
• Overwhelm victim with traffic arriving from thousands of different sources
DDoS Architecture

Attacker

Master machines

Zombie machines

Victim
Some Advices

– Do not click on pop-up advertisements.
– Do not open e-mails from unfamiliar or questionable sources.
– Do not propagate personal information, such as Social Security number, passwords, usernames.
– Download software programs that come from reputable sources.
– Install a good anti-virus product, with latest updates.
Discussion and Question !!