

Anatomy of a Botnet

Ravishankar Borgaonkar

UniK/NTNU/TKK

Why to talk about Botnet?

“ Terrorists may be able to do more with a keyboard than with a bomb.

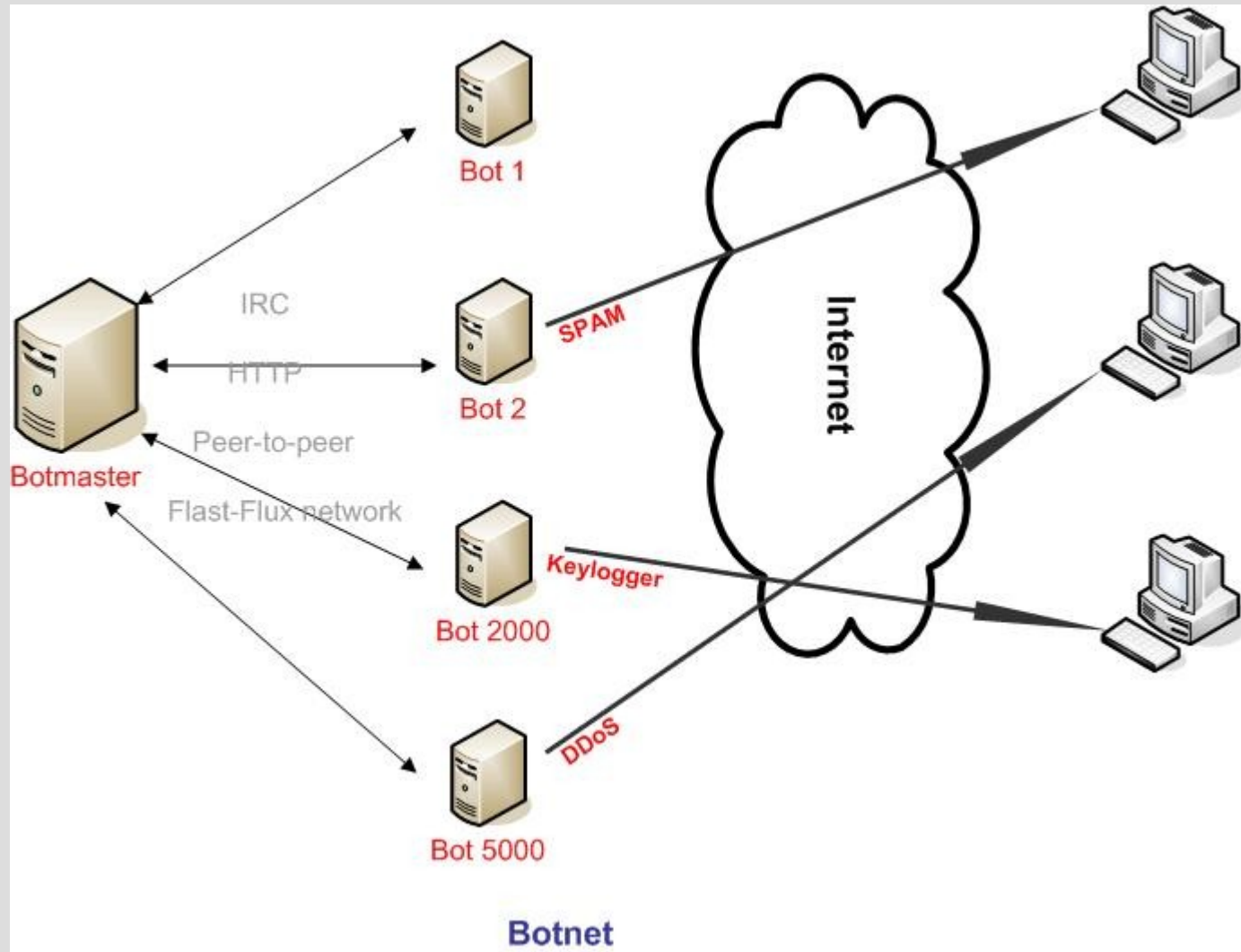
We understand the power of the bomb and the bullets but now we also have to understand 'cyber-terrorism' “ - IMPACT

- ♦ **“Botnet”** is a vehicle for cyber-terrorism & cyber-crime
- ♦ Recent attack on Estonia
- ♦ Attacks could be like disabling the banking networks, halting ATM machines and card payments OR could be worse than that
- ♦ **So we need to understand Botnet**

What is Botnet?

- Distributed network of a large number of hijacked computers under the control of single person via net-based command and control system
- Designed to accomplish some distributed tasks over the Internet
- It consists of
 - A Botnet creator and controller (Botnet herder)
 - Bots
 - Command and Control Server
- Evolution

Botnet



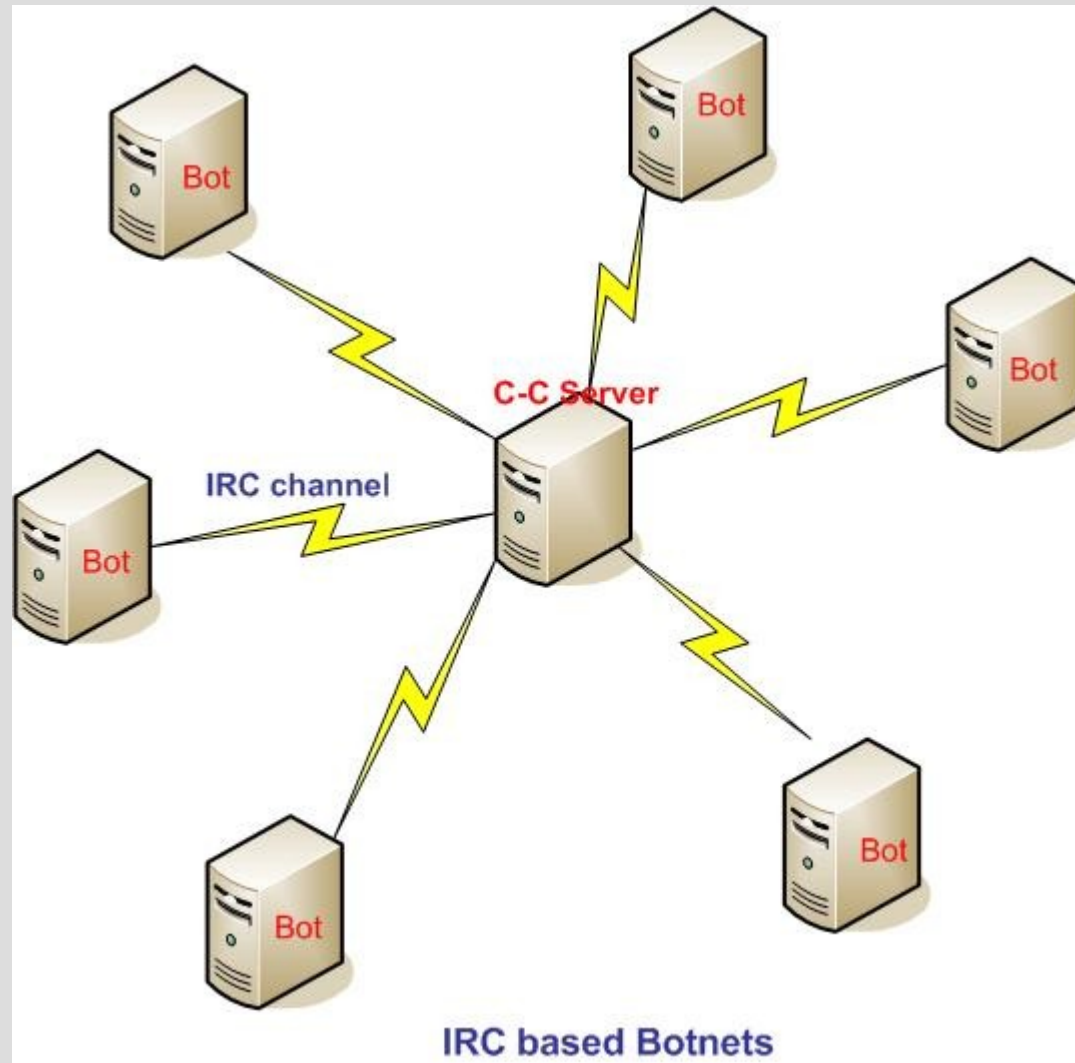
How does it spread?

- **Operating system vulnerabilities**
 - mostly in Windows environment
- **Client-side attacks using social engineering**
 - sending spams to download interesting stuff
 - directing client to the malicious website
 - using hacked website

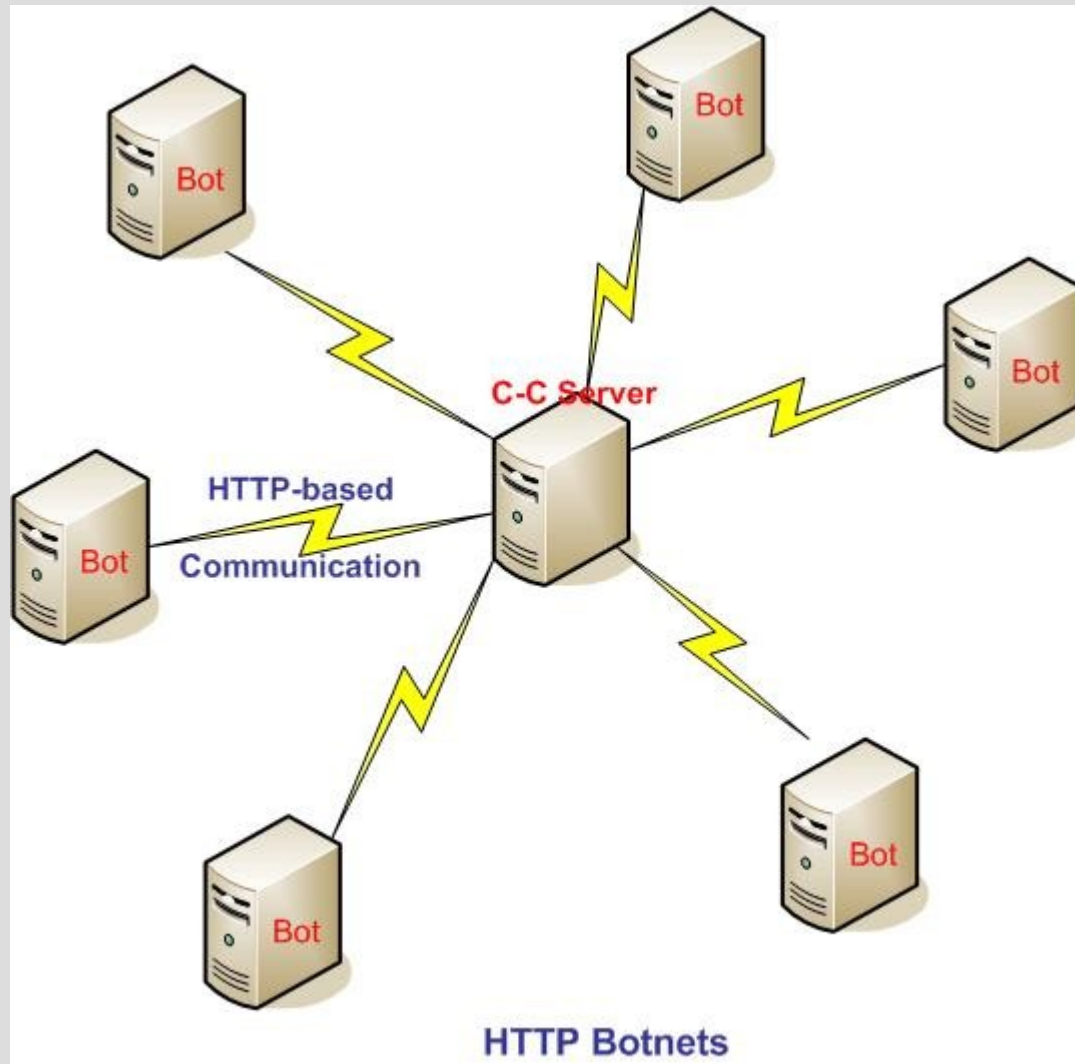
Types of Botnet

1. IRC based botnets
2. HTTP based botnets
3. Peer-to-peer network based botnets
4. Fast flux network based botnets

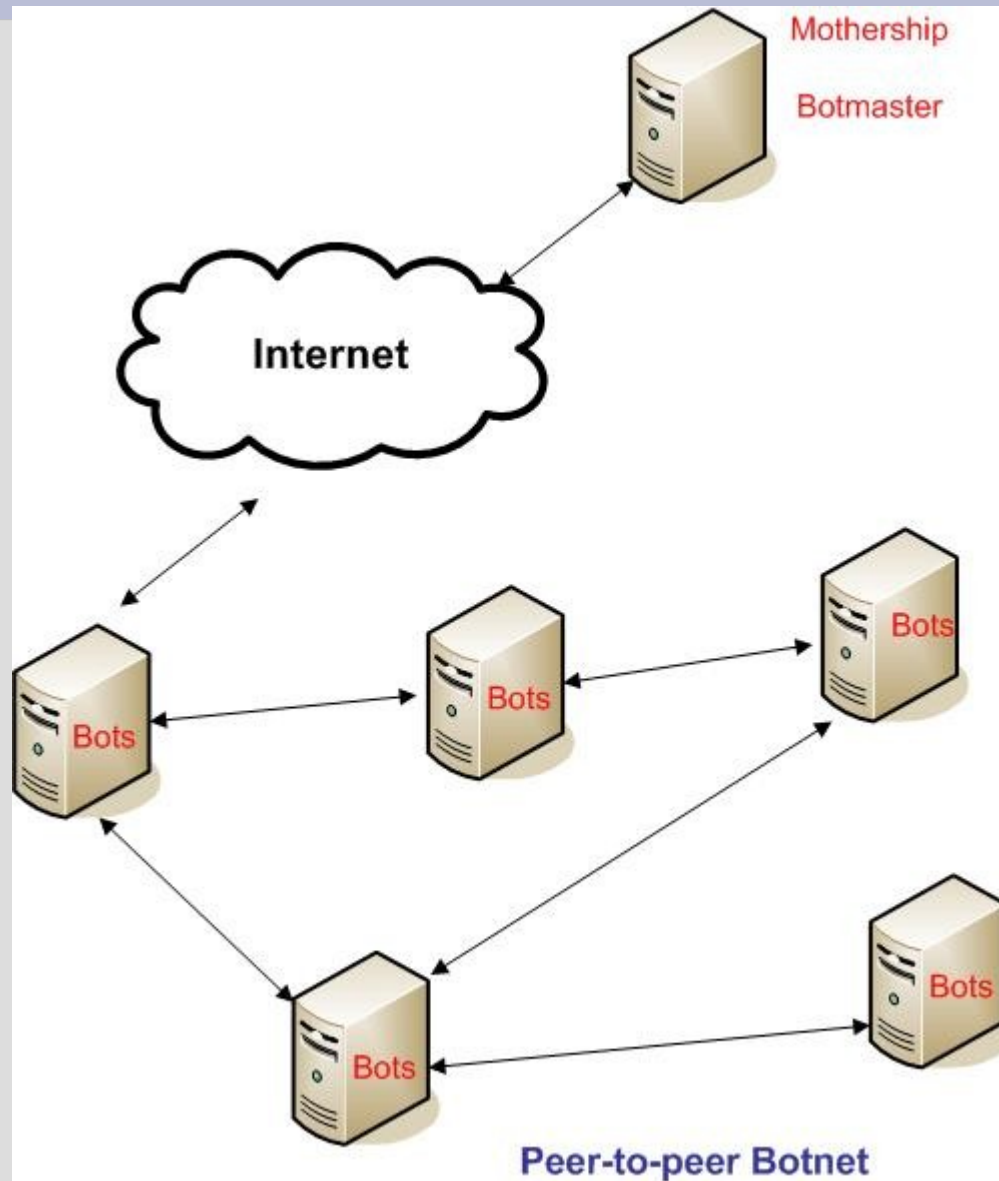
IRC Botnet



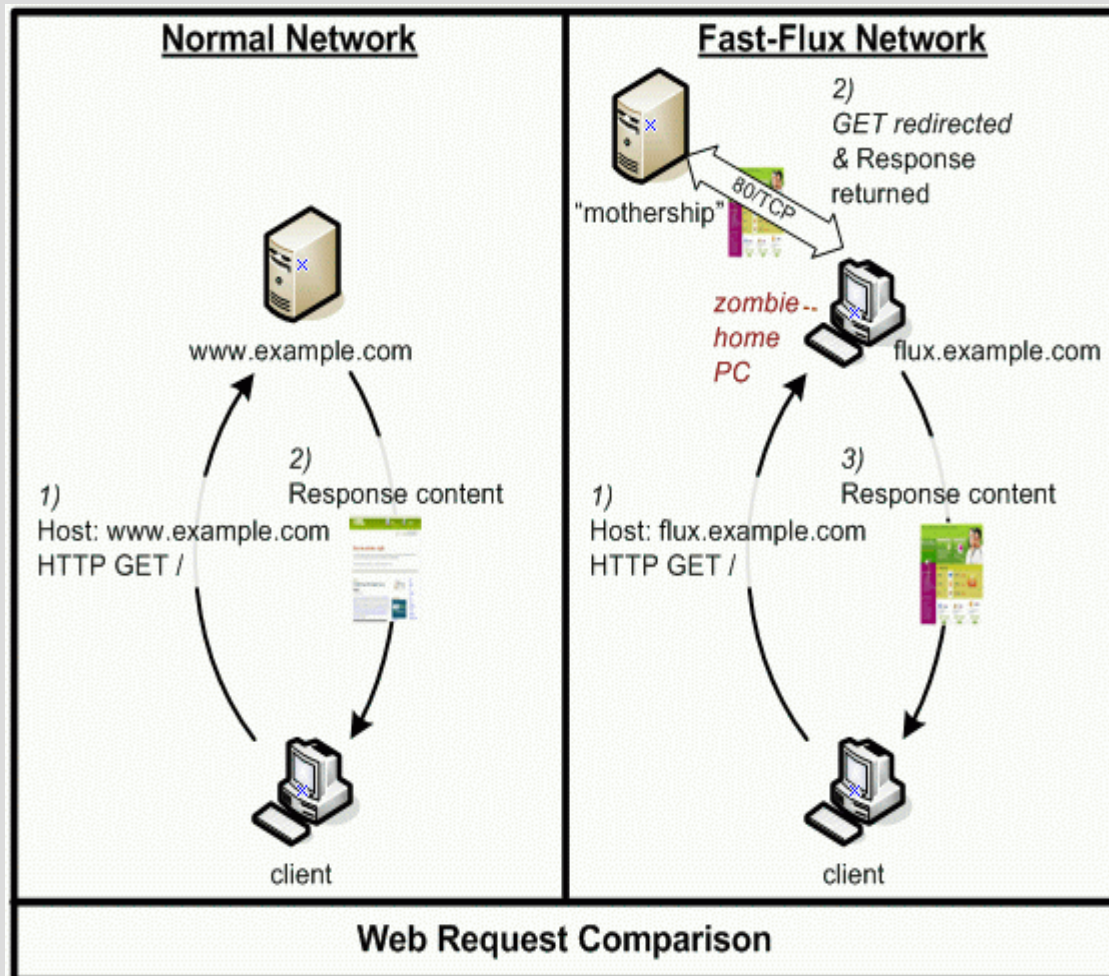
HTTP Botnet



Peer-to-Peer Botnet



Fast-flux network Botnet



Construction of a Botnet

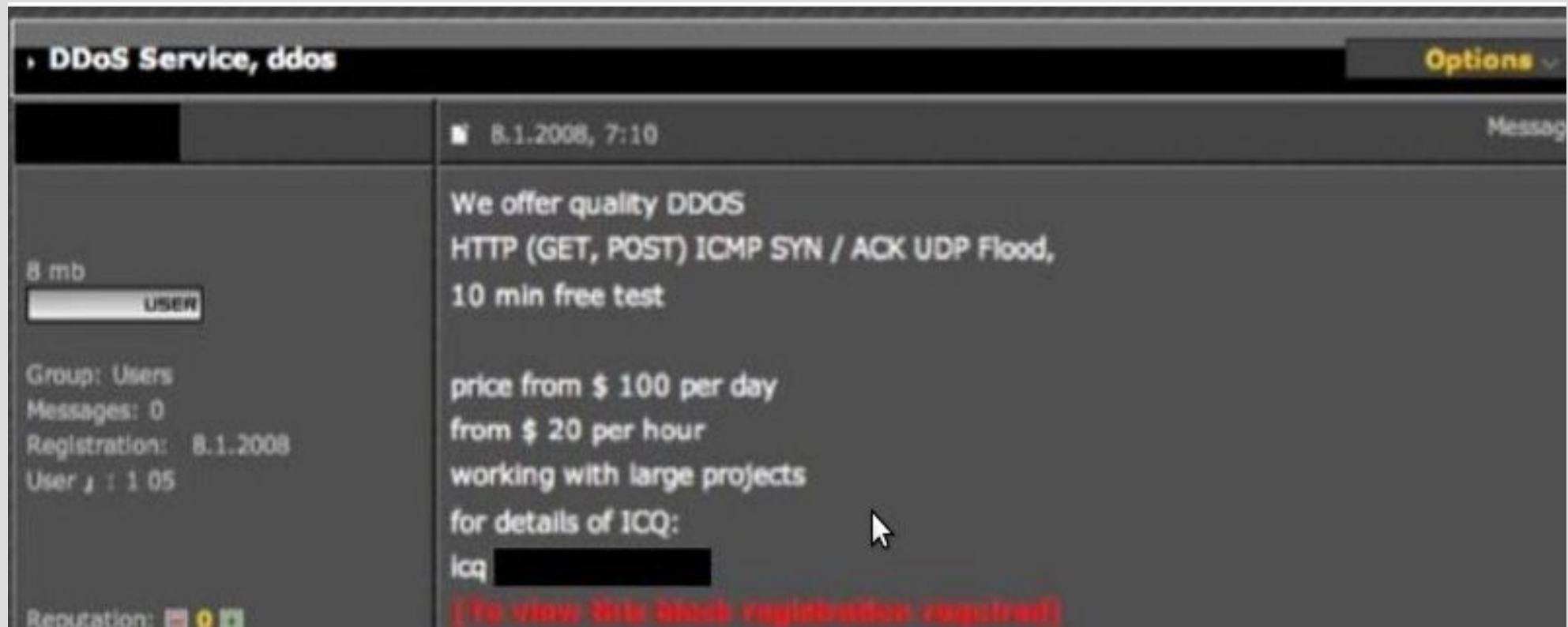
- First stage, exploit vulnerabilities(operating system's/browser's)
- Next stage to download bot software , C&C instructions
- Once the bot software is executed and connected to C&C server
 - Bots connect to channel of C&C (IRC or HTTP)
 - password protected channel
 - encryption layer between bot and C&C

Use of a Botnet

- DDoS attacks
- ID theft
- Phishing
- Spamming
- Privacy Issues- installing keylogger, spywares
- Renting web proxies for illegal purposes
- many more

In short- “ **TO EARN MONEY**”

Bot-Economics



The screenshot shows an ICQ chat window with the following details:

- Window Title:** DDoS Service, ddos
- Options:** A dropdown menu is visible in the top right corner.
- Message Header:** 8.1.2008, 7:10
- Message Content:**

We offer quality DDOS
HTTP (GET, POST) ICMP SYN / ACK UDP Flood,
10 min free test

price from \$ 100 per day
from \$ 20 per hour
working with large projects
for details of ICQ:
lcq [REDACTED]

[To view this block registration required]
- Left Panel:**
 - 8 mb
 - USER
 - Group: Users
 - Messages: 0
 - Registration: 8.1.2008
 - User J : 1 05
 - Reputation: [Icons]

Bot-Economics

- a paper from VB conference 2006 by Lovet
- A credit card business-
 - buying 40 valid CC - \$200
 - hiring 10 drops to collect purchased things- \$800 (\$20 per package)
 - drops to cyber criminal delivery - \$800
 - Selling on eBay - \$16,000 (like Laptop,mobiles,clothes)

Total cost, monthly- \$1800

Total profit - \$17,800

Net profit : \$16,000

Productivity index (Profit/Costs): 8.9

Protection against Botnets

For individual users:

- Use updated OS and legal softwares
- Anti virus software
- Firewall
- Don't open Spam e-mails
- Check your logs

For Corporate networks:

- Use strict firewall rules
- Deploy honeypots and set-up DNS redirection to to it
- Sniff outbound connection by using keywords used by bot herders

Summary

- Overall, It's a kind of **management problem**
- Great tool for illegal activities
- Not easy to root out, hacker's are one step ahead
- **User Awareness** is important!

Thank You.

Questions?