New Threats evolution
David Sancho
TrendLabs Av-EMEA
Old enemies
New enemies

Jay R. Echouafni

Jeremy D. Janes

Andrew Schwarmkoff
Threats in 2005

• Bot worms
• Trojans
• Spyware/Grayware
• Phishing
• Pharming
• Zombies: Infected PCs sleep until the attacker wakes them up

• Botnet: a network made up of zombies
What’s the purpose of bot worms?

- Get Money:
  - Selling botnet to spammers
  - Uploading spyware/adware
  - Sending DoS to websites

Recent examples include:
SDBOT, AGOBOT and MYTOB
• Trojans can’t replicate by themselves.

• Downloaded by the user from some webpage
• Trojan cycle…
• Spyware/Grayware: non-malicious threats - security breaches

• Spyware comes downloaded from the web
Phishing

- Emails seem to come from a bank, asking to validate your login
- They redirect you to a fake website
- You give login data, they steal the money
Phishing

Banks never contact their customers via email!!!

Phishing: Online Banking Fraud
Attacker pretends to be your bank and asks for your personal details.

- Never click on links from emails
- Never log in directly from an email
• DNS Server attack

• Can redirect to fake websites

• Can redirect to spyware sites
Any Question?