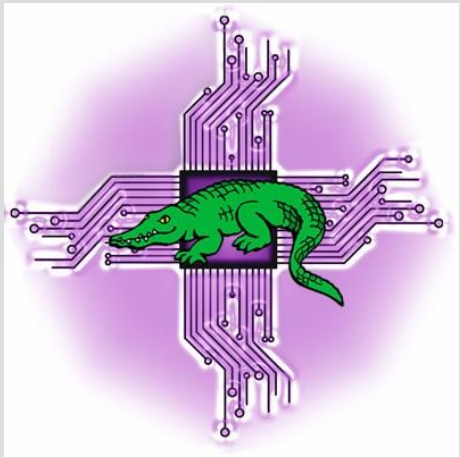
Storming the Castle: DDos and Active Network Defenses

Presentation to SecureCon, Thursday, Nov 8, 2007



Storming the Castle: DDos and Active Network Defenses

Medieval Castle Metaphor of Network Security

Buildings := Individual Hosts
Inner Keeps or Donjon := Secure Subnet
Outer Wall and Enceinte:= Network Border
Gatehouse := Router
Motte-and-bailey := Firewall

Storming the Castle: DDos and Active Network Defenses

Storming the Castle: DDos and Active Network Defenses

Secure Castles, Insecure Roads

Castles were built because the (a) roads were dangerous and (b) they provided a haven for rebels.

Gunpowder and cannon destroyed the era of the castle. However while they existed (and whilst we have private LANs) they were subject to siege warfare.

Storming the Castle: DDos and Active Network Defenses

Protect the Castle, Protect the Roads

The Southern Song Chinese used technological superiority to protect their castles from sieges.

Where technology, ability and morale are equivalent, warfare moves from Attrition Warfare to Maneuver Warfare

Storming the Castle: DDos and Active Network Defenses

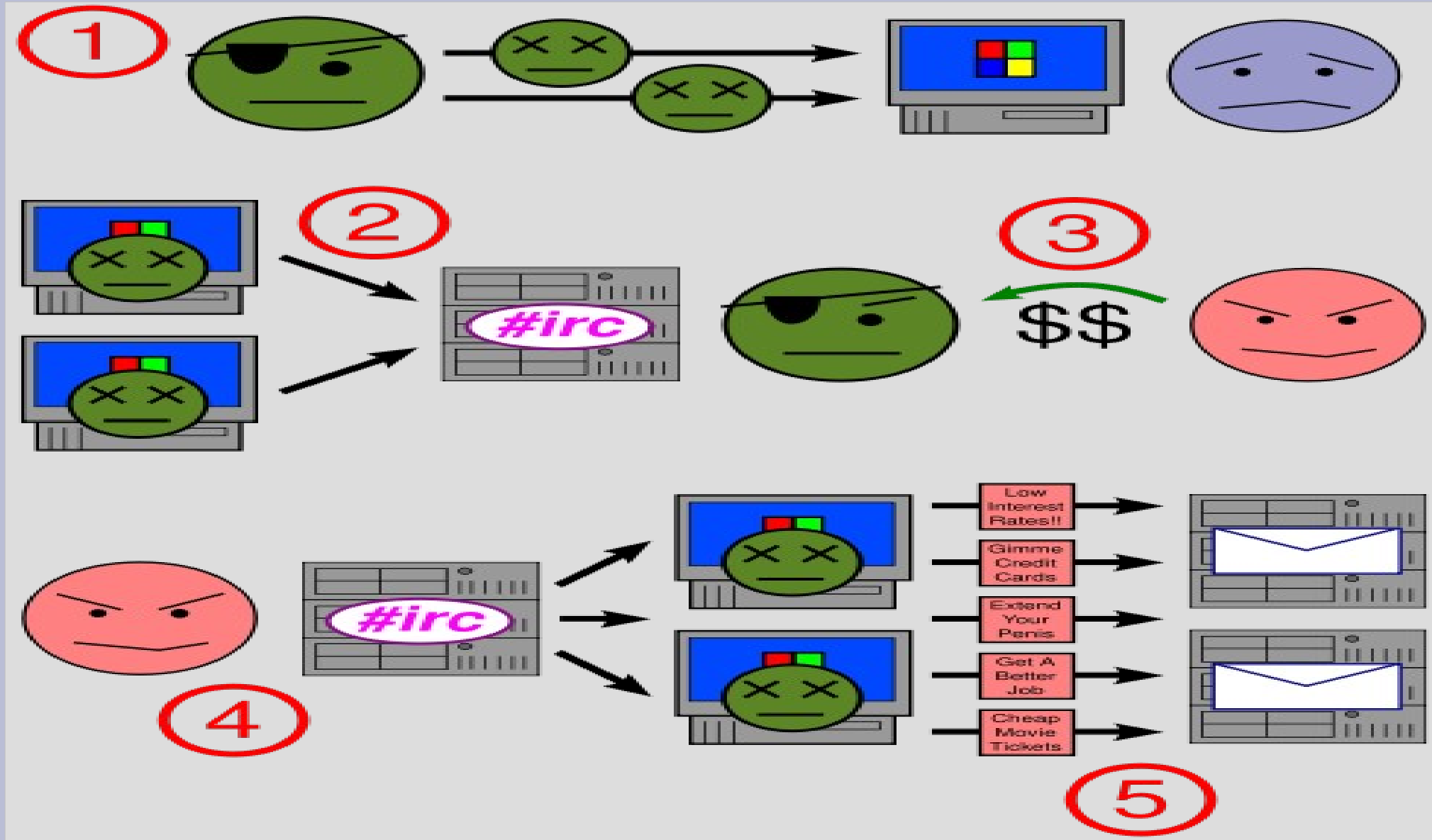
'Bots: The Enemy is Within!

Through infection of a vulnerable system a computer (or keep) has automatons (or zombies) under a common command (an evil wizard).

Typically used in conjunction with spammers (merchants) who pay the botnet controller to distribute junk mail.

Estimated that 25% of PCs are part of a 'botnet.

Storming the Castle: DDos and Active Network Defenses



Storming the Castle: DDos and Active Network Defenses

The Coming Storm

The Storm 'botnet is estimated to have infected 8% of all Windows systems (except 2003 Server).

It has sent 1.2 billion messages have been sent including a record 57 million on August 22 alone. Several thousand computers are dedicated in propagating the 'bot.

Protects itself and attacks anti-spam sites.

Storming the Castle: DDos and Active Network Defenses

Storm 'bot's internals

Process of infection:

 # Backdoor/downloader
 # SMTP Relay
 # Email Address Stealer
 # Email Virus Spreader
 # DdoS Attack Tool
 # Update Storm Worm dropper

At each stage connects to 'Botnet using FastFlux

Storming the Castle: DDos and Active Network Defenses

Active Defense Mechanisms

Enno David's Apache example

TCP/IP Stack Fingerprinting

Network Based Approaches (e.g., nullrouting)

Sally forth!