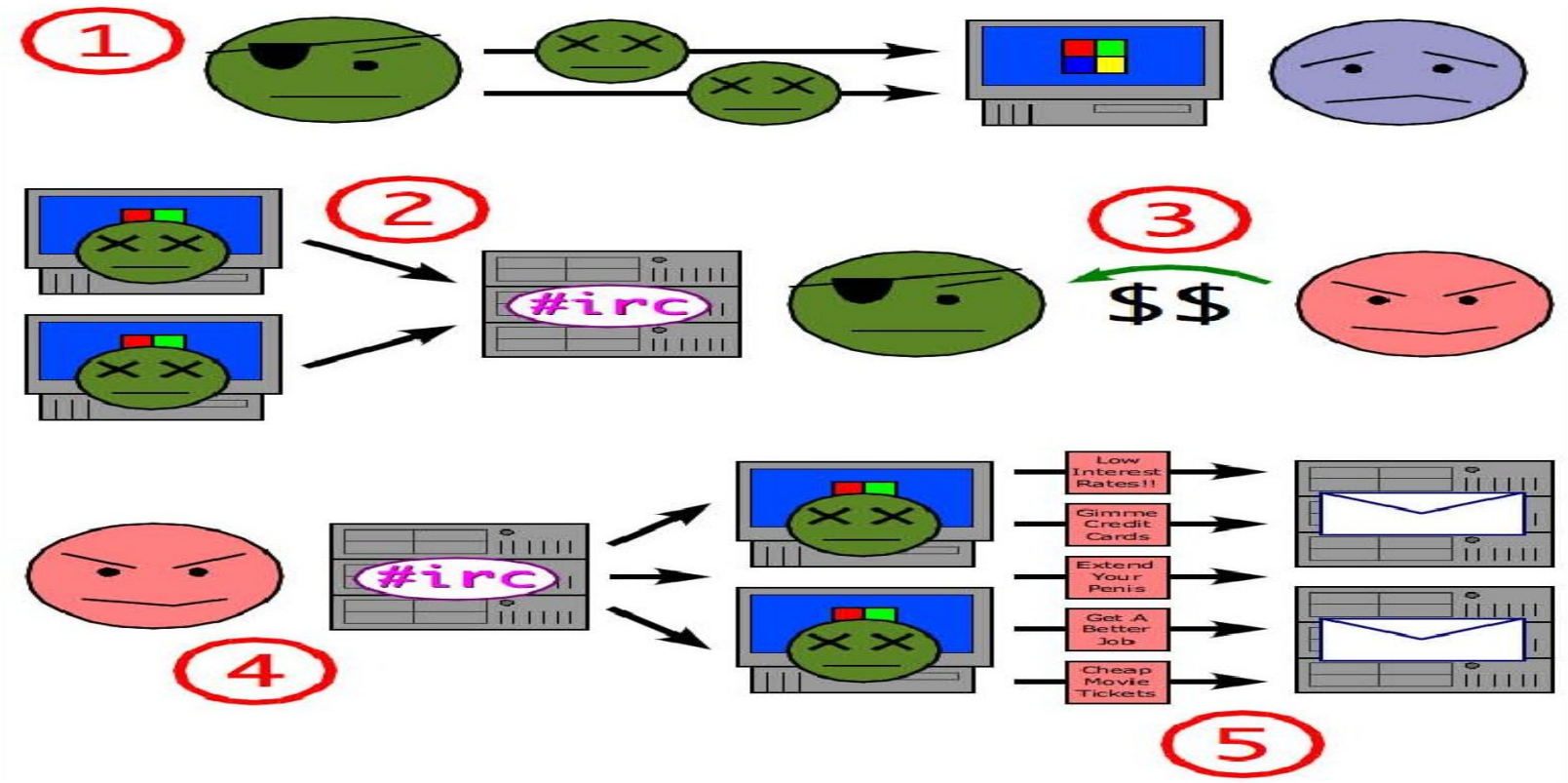
Botnets

Philippe Owezarski
LAAS-CNRS, Toulouse, France
owe@laas.fr

Botnet

- A distributed computer network consisting of computers (also called bots or zombies) remotely controlled without their owner's knowledge
  - In general home and small office machines infected by trojan horses
- Objective: hackers aim at making money out of the botnets they own
  - Sending SPAM
  - Launching DoS or DDoS attacks
  - Cyberwar
  - …

Botnet creation and use



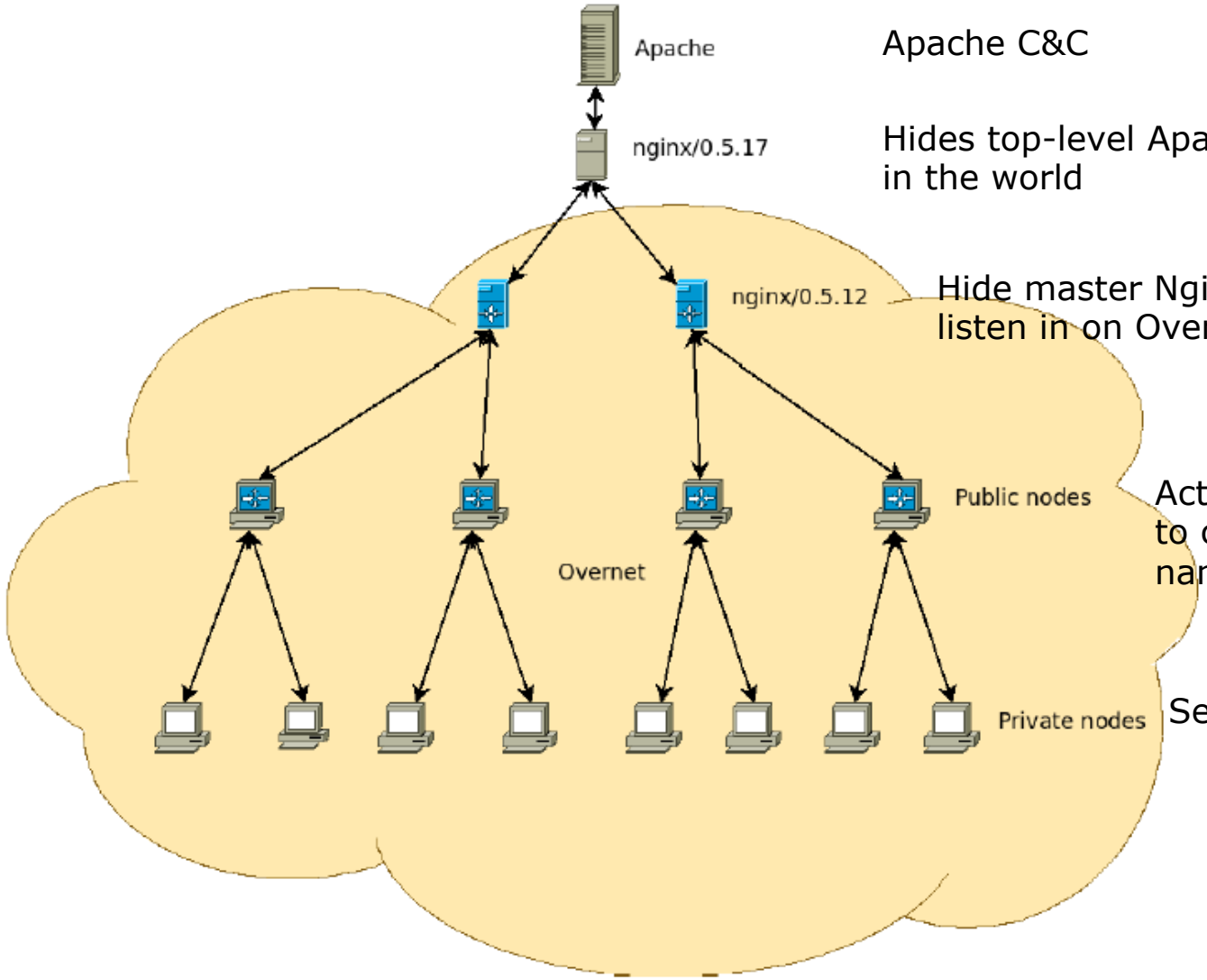
Examples of botnets

- Srizbi (or Cbepblay, or Exchanger)
  - Sends around 60% of the SPAMs in the world (60 billions SPAMs per day)
  - Maybe the largest botnet in the world (debate with Kraken
  - Machines are infected by the Srizbi trojan
- Mariposa
  - 13 millions of infected machines / worldwide distribution (190 countries)
  - Machines are infected by Conficker via MSN
- Storm
  - Between 1 and 50 millions of infected machines
  - Machines are infected by the Storm trojan by e-mail spam, false blog, infected legitimate sites
  - Can block the Internet connectivity of countries
  - More powerful than the most powerful super-computers in the world

Storm Botnet

- Migration from an IRC to a P2P based control system (Kademlia's DHT implementation – MD4 hash)
- Many vectors for replacing lost zombies
- Storm botnet consists of:
  - Male hosts in charge of finding 1000 to 2000 females ready to accept the genetic code of the trojan (or rootkit)
  - Females are connected to at least 3 males for a tight and fast connectivity
  - Females attempt to propagate empty envelopes to 1000 or 2000 other machines
- The packing code changes every 10 minutes
- Observed attacks from the storm botnet were only targeting researchers in security who wanted to track or dismantle the botnet
- Storm can boot the system for disactivating tools as security software, antivirus, IDS, …

Storm Architecture



Apache C&C

Hides top-level Apache server somewhere in the world

Hide master Nginx host, listen in on Overnet traffic

Act as reverse HTTP proxies to controller, fast-flux name servers

Send spam or DDoS packets

Storm's private overnet

- Overnet is filled with poison peers, nosy botnet researchers ☺
- Storm's answer – keep the protocol, but encrypt the packets
  - Creates a new network – only Storm nodes can talk to each other
  - Encryption is simple XOR by embedded key
  - Could be used to segment botnets in case Storm author feels like selling turn-key spam system

That’s all folks !