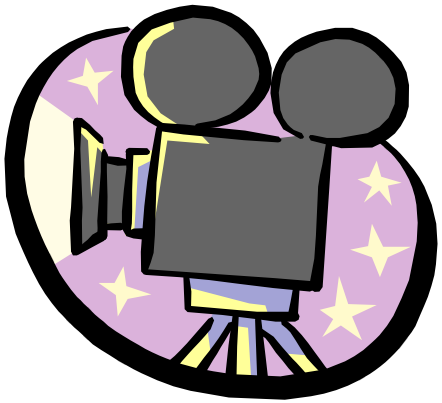
EMEA MSSD

# Bots and Botnets: Risks, Issues and Prevention

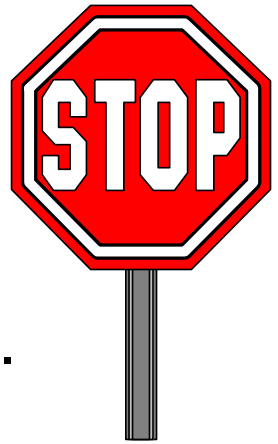
Martin Overton, IBM UK

# Agenda



- Definitions
- Size of the Problem
- Risks
- How They Work
- Solutions
- Conclusions
- Questions

# Disclaimer




- Products or services mentioned in this presentation are included for information only.
- Products and/or services listed, mentioned or referenced in any way do not constitute any form of recommendation or endorsement by IBM or the presenter.
- All trademarks and copyrights are acknowledged.

# Definitions:-

- ***Bot***

  'Bot' is a contracted (truncated or short) name for a software robot. A bot is a piece of software that allows a system to be remotely controlled without the owner's knowledge; it can also be used to automate common tasks such as on IRC aka drone or zombie.

- ***Botnet***

  A group ['Herd' or 'Network'] of Zombie systems controlled by the 'Bot Herder'. These botnets are told what to do by the botnet owner. This can be anything that the bot has been programmed to do....including updating itself or installing new malicious software.

- ***Bot Herder***

  The person [or group] which "own" and control a herd of bots. Also known as the Bot Master aka Zombie Master.

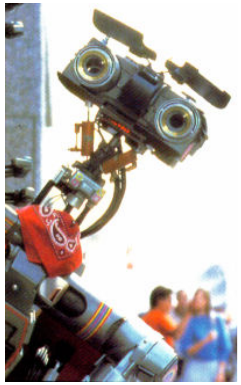
# Definitions:-

- ***DDoS [aka Distributed Denial of Service]***

  A distributed denial-of-service attack is an attack on a computer system or network from multiple co-ordinated systems connected to the same network which are performing a denial of service attack.

- ***IRC***

  “Internet Relay Chat (IRC) is a form of instant communication over the Internet. It is mainly designed for group (many-to-many) communication in discussion forums called channels, but also allows one-to-one communication.



# Size of the Problem

- The following are quite disturbing statistics for 2004[1]:
  - Britain has largest zombie PC population in the world
  - Over 1m connected computers are zombies
  - 30,000+ internet connected zombie networks in 2004
  - Estimated 25% of all infected PCs are under control of hackers
  - Broadband responsible for 93% increase in infected PCs in 2004

- The Honeynet project entitled: “Know your Enemy: Tracking Botnets”
  - Logged 226,585 unique IP addresses logging into one of the IRC botnet C&C channels.
  - Botnets ranged in size from several hundred ‘zombies’ to more than 50,000 ‘zombies’.
  - They observed 226 DDoS attacks against 99 unique targets.
  - Typical size of a botnet: 2000+ bots [‘zombies’].
  - **From this data they worked out that the number of bots required to successfully DDoS a typical company were just 13. This assumes that the company is on a T1 [1.544Mbit] and that each ‘zombie’ has a 128Kbit link [128Kbit x 13 = 1.664Mbit].**

[1] Source: http://news.bbc.co.uk/1/hi/technology/4579623.stm

# Size of the Problem… cont.

- In June 2004 a large European IRC service recorded between 200,000 and 600,000 connections from bots each and every day. Of these they confirmed between 150,000 and 400,000 unique ‘zombie’ systems per day.
- And more recently another group monitoring botnets used to send SPAM recorded that they had seen 1.5 Million compromised computers, with another 1 Million extra unconfirmed computers. They went on to estimate that it would take 5,763 man years to disinfect all of them and cost $600 Billion!
- In the first six months of 2005, Symantec identified an average of 10,352 bots per day, up from less than 5,000 per day in December 2004.
- Symantec also observed a dramatic increase in bot variants in the first half of 2005.

# Size of the Problem… cont.

| Rank Jan–June 2005 | Rank July–Dec 2004 | Rank Jan–June 2004 | Country | Percent of events Jan–June 2005 | Percent of events July–Dec 2004 | Percent of events Jan–June 2004 |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | United States | 33% | 30% | 37% |
| 2 | 3 | 5 | Germany | 7% | 8% | 5% |
| 3 | 6 | 6 | United Kingdom | 7% | 4% | 4% |
| 4 | 2 | 2 | China | 6% | 8% | 6% |
| 5 | 7 | 7 | France | 5% | 3% | 4% |
| 6 | 9 | 8 | Spain | 5% | 3% | 3% |
| 7 | 5 | 3 | Canada | 4% | 4% | 6% |
| 8 | 8 | 12 | Japan | 4% | 3% | 1% |
| 9 | 4 | 9 | South Korea | 3% | 4% | 3% |
| 10 | 10 | 11 | Italy | 3% | 2% | 2% |

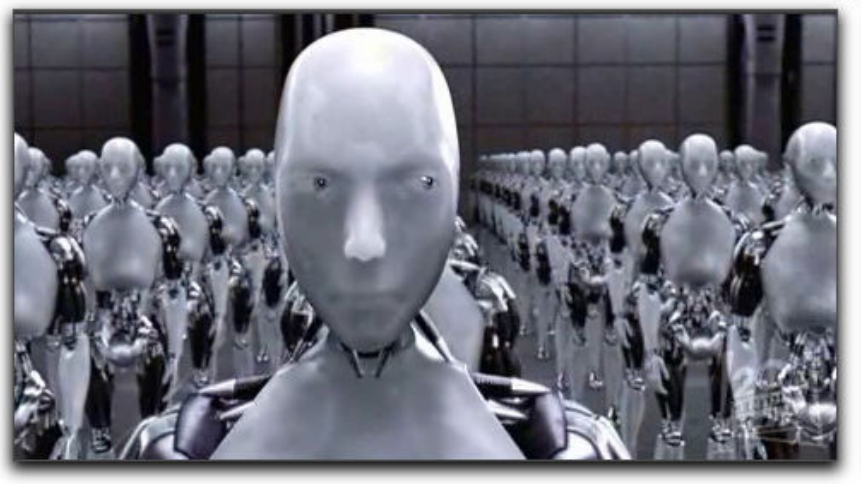
**Table 4. Top originating countries**
*Source: Symantec Corporation*

| Rank Jan–June 2005 | Rank July–Dec 2004 | Country | Percent of bot-infected computers Jan–June 2005 | Percent of bot-infected computers July–Dec 2004 |
|---|---|---|---|---|
| 1 | 1 | United Kingdom | 32% | 25% |
| 2 | 2 | United States | 19% | 25% |
| 3 | 3 | China | 7% | 8% |
| 4 | 4 | Canada | 5% | 5% |
| 5 | 6 | France | 4% | 4% |
| 6 | 9 | South Korea | 4% | 3% |
| 7 | 7 | Germany | 4% | 4% |
| 8 | 10 | Japan | 3% | 3% |
| 9 | 5 | Spain | 3% | 4% |
| 10 | 8 | Taiwan | 2% | 3% |

**Table 3. Top countries by percentage of bot-infected computers**
*Source: Symantec Corporation*

# Size of the Problem… cont.

| Family | Number of Variants | Source | Notes |
|---|---|---|---|
| **Sdbot** | ~12,800 | McAfee | Last count, as McAfee no longer counts individual variants. Includes Forbot, Rbot, Wootbot and IRCbot. |
| **Agobot** | 3,821 | McAfee | + 396 Non-viable. Includes Phatbot. |
| **Spybot** | 2,116 | McAfee | + 69 Non-viable |
| **Polybot** | 106 | McAfee | + 8 Non-viable |
| **Mytob** | 228 | TREND | |

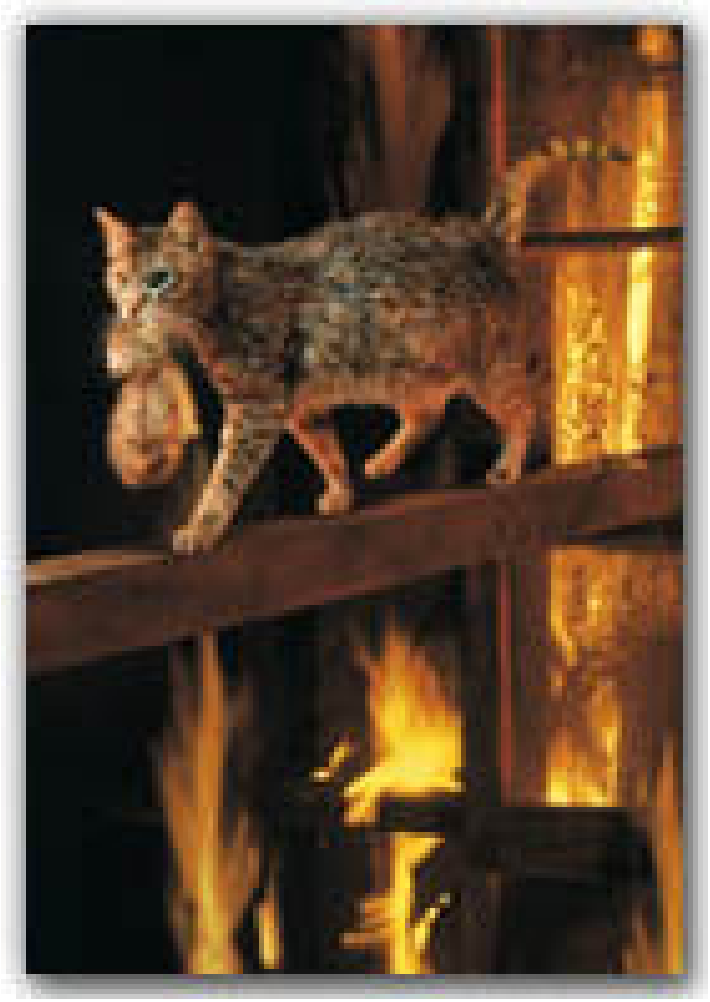


# Risks

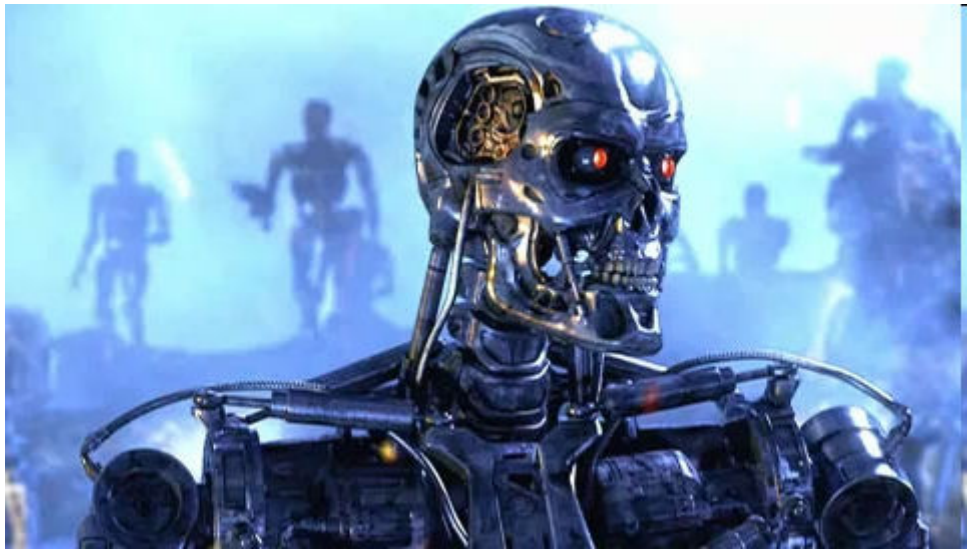
- DDoS
  - Syn flood
  - UDP flood
  - ICMP Flood
  - Cyber-Extortion
- On average, the number of DoS attacks grew from 119 to 927 per day, an increase of 679% over the previous reporting period – source Symantec
- Privacy
  - Identity Theft
- Intellectual Capital
- Loss of Confidence
- Network Stability

# Risks

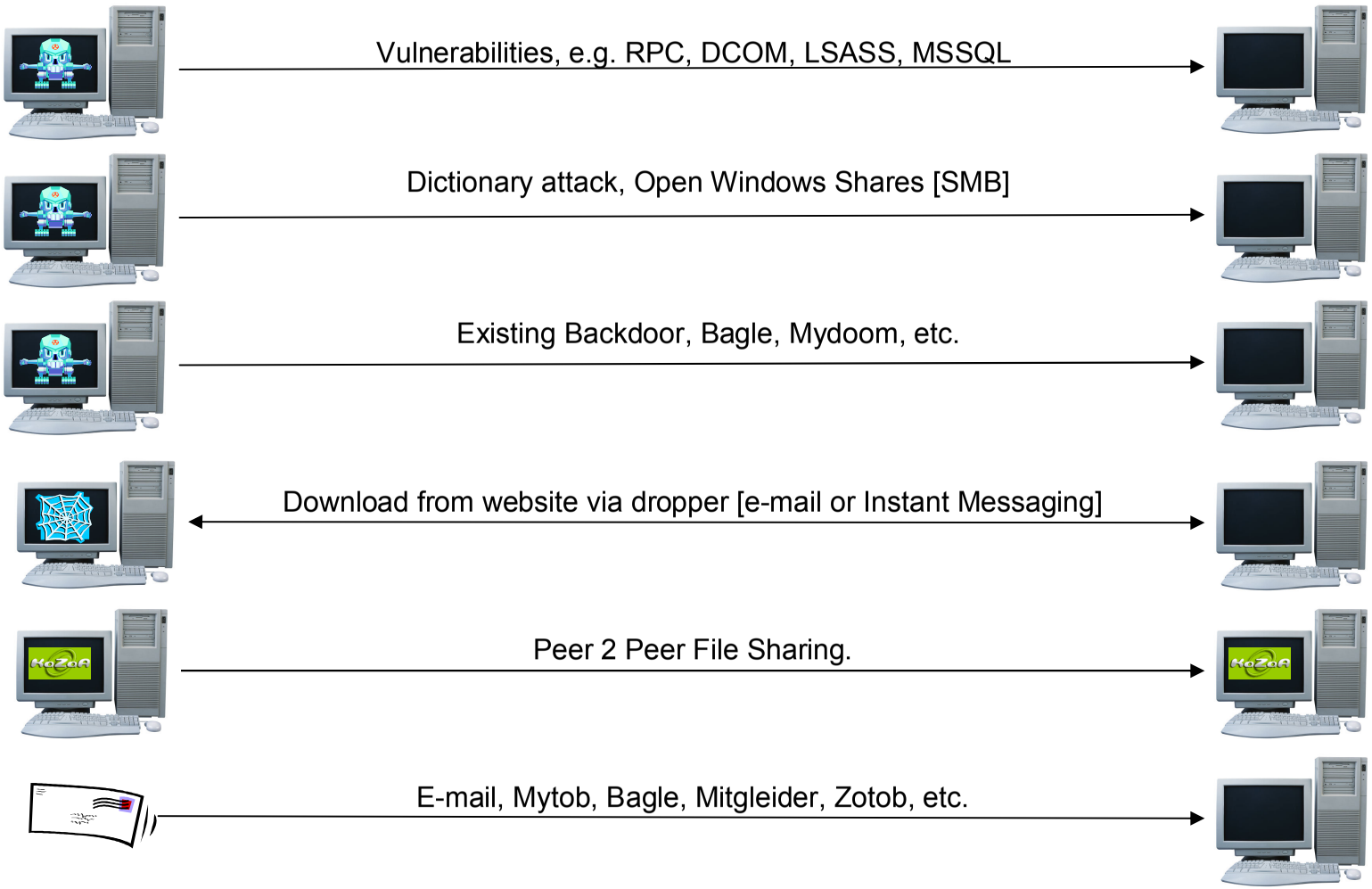
- Proxy
  - SPAM
  - Malware
  - Phishing
- Web Server
- Mule
- Other Tricks



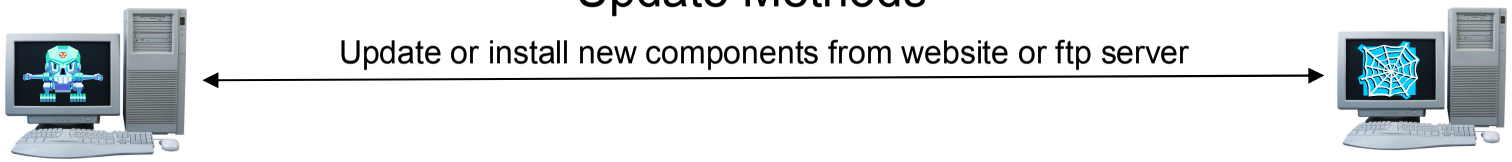
# How They Work

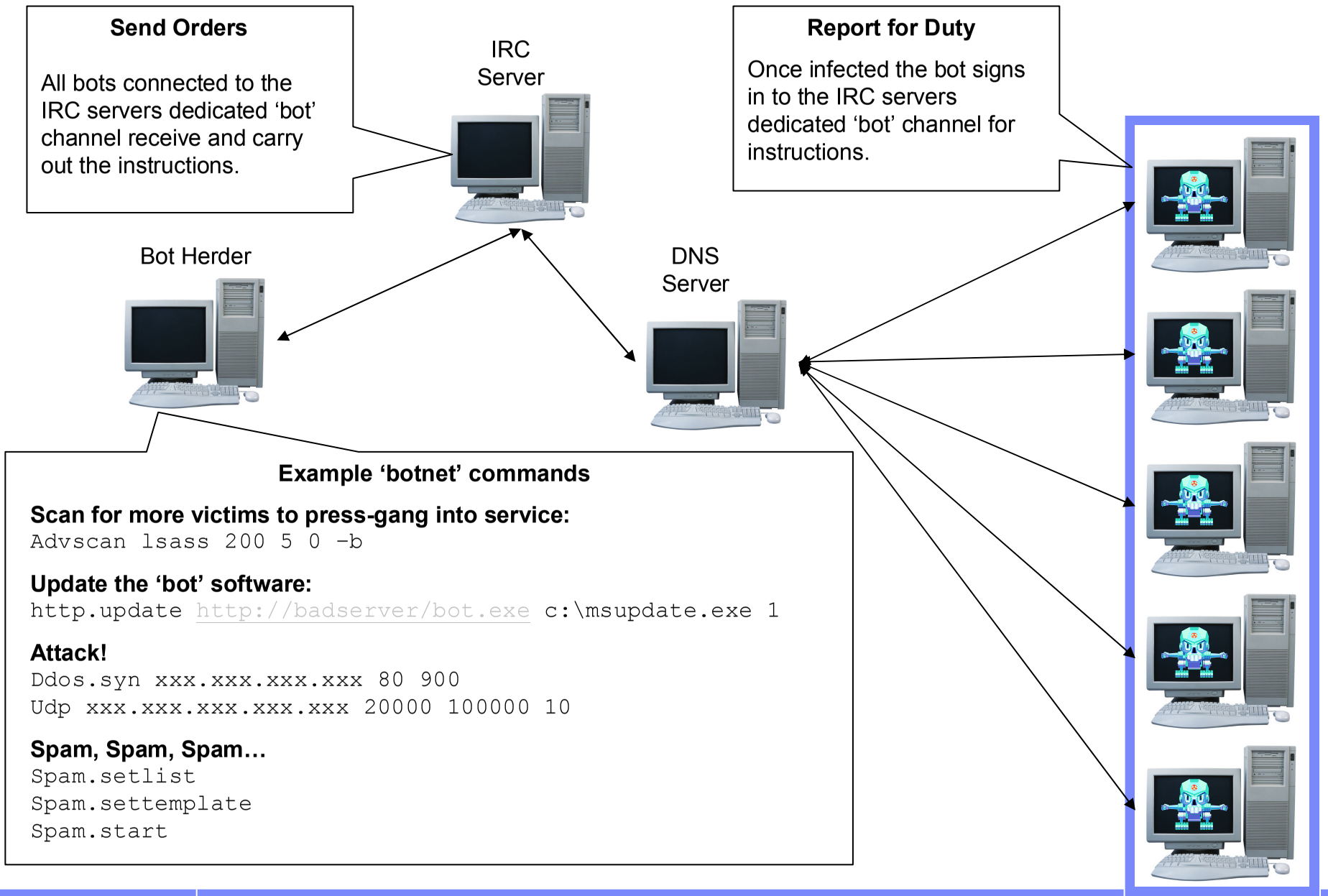


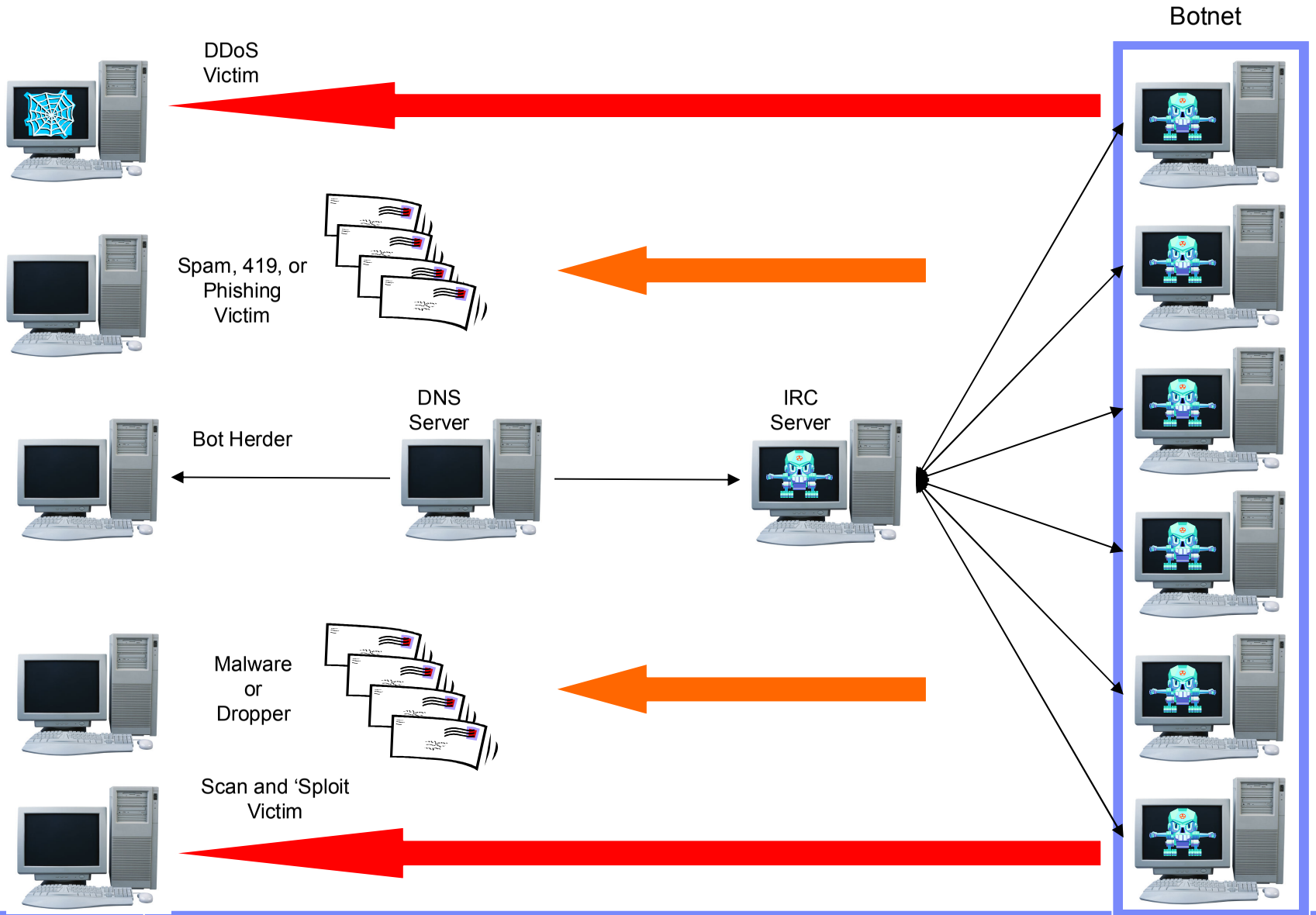
# Infection/Propagation Methods



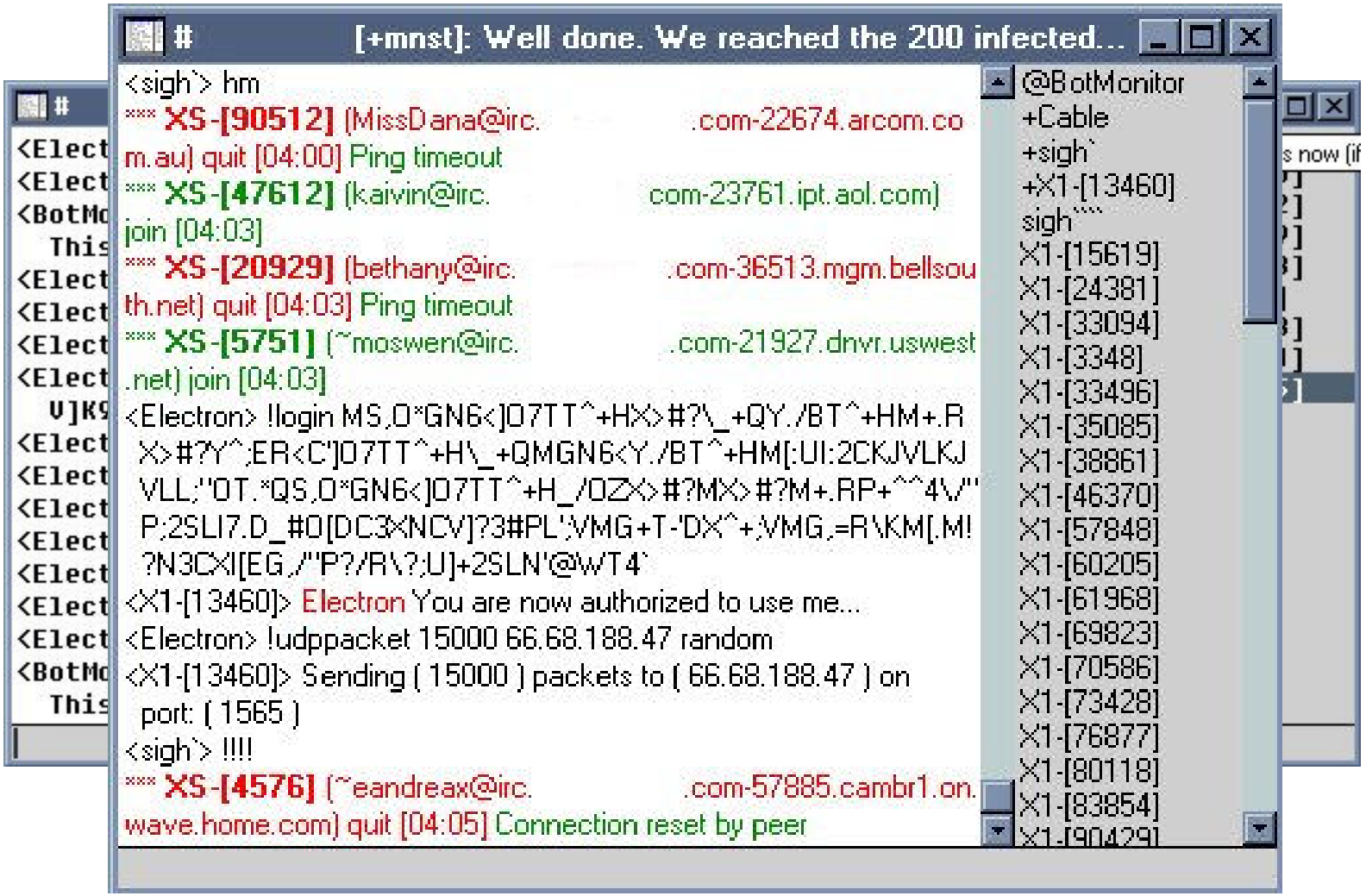

# Update Methods







# Examples



# Solutions - Generic

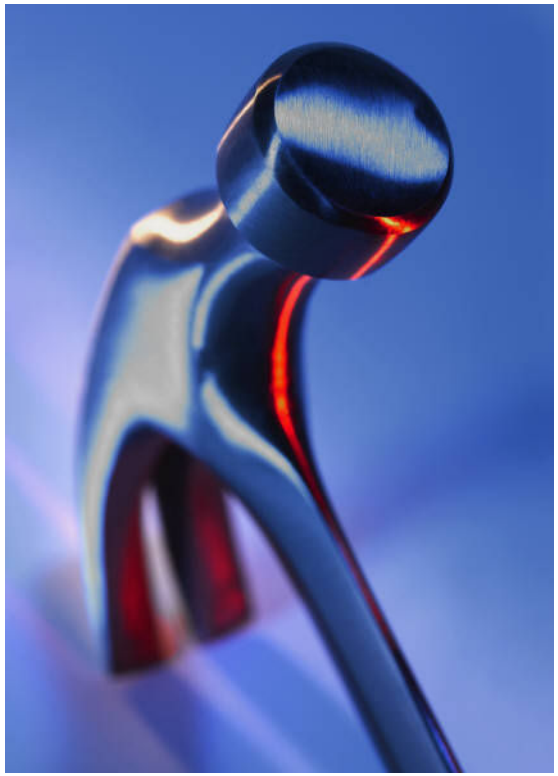
- Policies and Procedures
- Passwords
- Education

# Solutions – Generic cont.

- IRC
  - Main botnet command and control system
- IM
  - Mytob
- Vulnerability Scanning
  - Nessus [http://www.nessus.org/]
  - InternetScanner – ISS [http://www.iss.net/]
  - Nmap [http://www.insecure.org/nmap/]
  - SAINT [http://www.saintcorporation.com/]
  - Microsoft Baseline Security Analyzer (MBSA)

# Solutions – Tools and Technologies

- Firewalls
  - Perimeter
  - Intra-network
- Proxies
  - Socks
  - Application



# Solutions – Tools and Technologies

- IDS and IPS
  - HIDS
  - NIDS
  - HIPS
  - NIPS


alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg: "BLEEDING-EDGE VIRUS Agobot/Phatbot Infection Successful"; flow: established; dsize: 40; content:"221 Goodbye, have a good infection |3a 29 2e 0d 0a|"; reference: url,www.lurhq.com/phatbot.html; classtype: trojan-activity; sid: 2000014; rev:2; )

# Solutions – Tools and Technologies

- SMTP

  Only allow ‘Official’ SMTP servers to be used

  Extension blocking inbound and outbound

  Content filtering

| | |
|---|---|
| ade | Access Project Extension |
| adp | Access Project file |
| bas | BASIC program |
| bat | DOS batch file script |
| chm | Compiled HTML file |
| cmd | 1st Reader External Command Menu |
| com | Command file (program) |
| cpl | Control Panel Module |
| crt | Certificate file |
| eml | Outlook Express message |
| exe | Executable file (program) |
| hlp | Windows help file |
| hta | HTML file |
| inf | Package information file |
| ins | Install script |
| js | Javascript |
| lnk | Shortcut file (Windows) |
| mdb | Access database |
| mde | Access file |
| msc | Common console document (Windows 2000) |
| msi | Installer program |
| msp | Windows Installer patch file |
| mst | Windows Installer transform |
| pif | Program information file (Win 3.1) |
| rar | RAR compressed file format |
| reg | Registration file |
| scr | Screen saver |
| sct | FoxPro forms |
| shs | Shell scrap file |
| url | Internet shortcut file (Universal Resource Locator) |
| vbs | Visual Basic program |
| vbe | Visual Basic related |
| wsh | Windows Shell |
| zip | ZIP file |

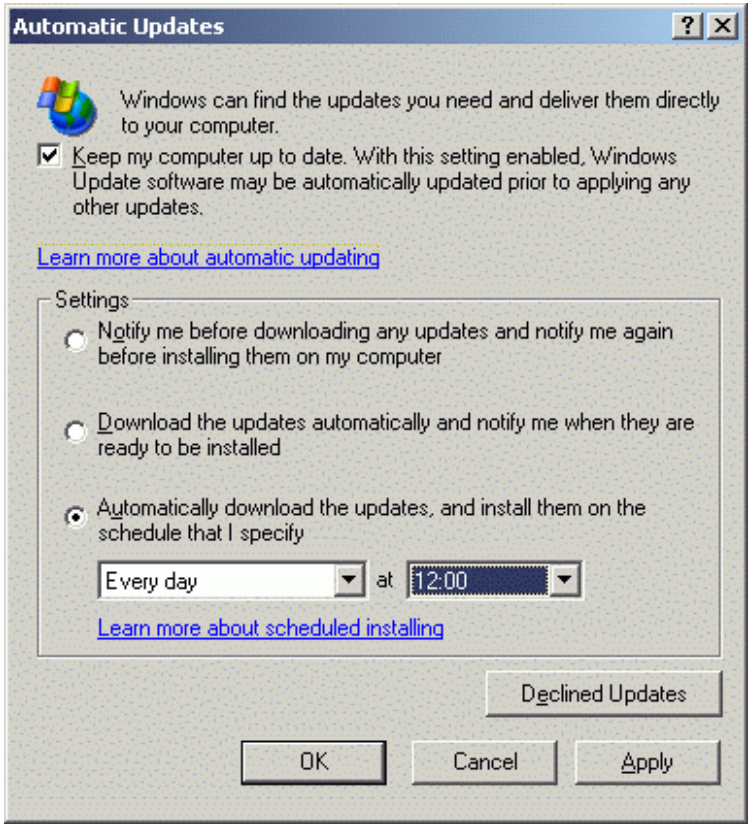
# Solutions – Tools and Technologies

- Patch Management

  Windows Update

  SUS [Software Update Server]

  3rd Party Solutions



# Solutions – Tools and Technologies cont.

- DNS

**Zone entry in named.conf**

```
Zone "blackcarder.net" {
  Type master;
  File "blackcarder.zone";
};
```

**Contents of blackcarder.zone file**

```
$TTL 2592000
@ IN SOA blackcarder.net.
  root (
     46
     3H
     15M
     1W
     1D )
  IN NS your.dns.server.name
  IN A  10.109.37.123
```

# Solutions – Tools and Technologies cont.

- Anti-Virus
  - Too many to list
- Anti-Rootkit Tools
  - ChkRootkit [*NIX - http://chkrootkit.org/]
  - Rootkit Hunter [*NIX - http://www.rootkit.nl/projects/rootkit_hunter.html]
  - RootkitRevealer [Wintel - http://www.sysinternals.com/ntw2k/freeware/rootkitreveal.shtml]
  - UnHackme [Wintel - http://greatis.com/unhackme/]
  - Blacklight [Wintel - http://www.f-secure.com/blacklight/]
- Personal Firewalls
  - Too many to list
  - Can block internet access to untrusted executables – assuming the malware hasn't already disabled it!

# Solutions – Tools and Technologies cont.

- **Anti-DDoS Products**
- Network
  - Arbor Networks [http://www.arbornetworks.com/]
  - Captus Networks [http://www.captusnetworks.com/]
  - Cisco Systems [http://www.cisco.com
  - Lanscope [http://www.lancope.com/]
  - Mazu Networks [http://www.mazunetworks.com/]
  - Top Layer [http://www.toplayer.com/]
  - IntruShield [http://www.mcafee.com/]
- Host
  - Entercept [http://www.mcafee.com/]
  - Tripwire [http://www.tripwire.com/]
  - AIDE [http://sourceforge.net/projects/aide]
- **Anti-DDoS Strategies**
  - Akamai
  - ISP
  - Quick and Dirty

"*On any day there are in excess of a million compromised systems just waiting to be used in DDoS like this, any business is vulnerable, and there is no 100% protection.*"

***Johannes Ullrich, CTO - SANS Institute's Internet Storm Center***.

# Solutions – Tools and Technologies cont.

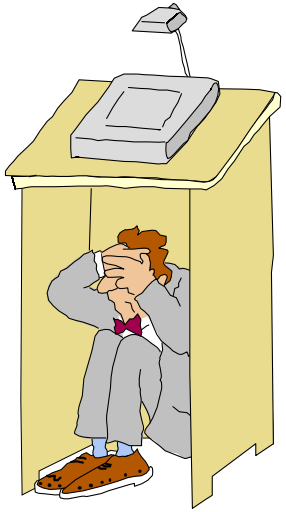
- Industry Initiatives
  - Fingerprint Sharing Alliance
- SMB-Lure and WormCharmer
  - Early Warning
  - Catches many bots


- Companies involved in this initiative include:
  - Asia Netcom
  - British Telecom
  - Broadwing
  - Cisco Systems
  - Earthlink
  - Energis
  - Internet2
  - ITC^DeltaCom
  - MCI
  - Merit Network
  - NTT Communications
  - University of Pennsylvania
  - The Planet
  - Rackspace Managed Hosting
  - Utah Educational Networks
  - Verizon Dominicana
  - WilTel Communications
  - XO Communications

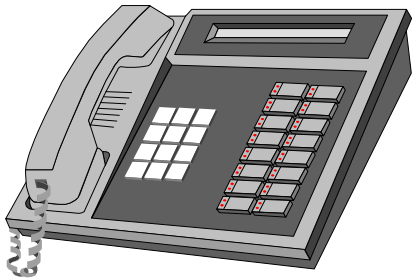
# Conclusions

- Bots have grown from simple tools to automate tasks on IRC to a major threat to the Internet and those that use it.
- DDoS attacks are a growing threat to businesses.
- We seem to be currently witnessing the birth of a new threat; the super-bot. This is a multi-component and multi-stage creation.
- We will see bots using other command and control networks other than IRC.
- The war for control of your PC has started and so far the ‘enemy’ has infiltrated and captured many systems; using them as bases for attack, storage, mis-information, mis-direction, theft and spying…..are you going to let them win?

# Questions?



# Contact Details



**Telephone:** **+44 (0) 2932 563442**

**WWW:** **http://www.ibm.com/uk**

**Email:** **overtonm@uk.ibm.com**

**Thank You For Your Attention**

**Personal Web Server: http://arachnid.homeip.net**