AIM for Bot Coordination
Presented at VB2006

Lysa Myers
Virus Research Engineer
October 11, 2006
Early experiments with malicious bots

*Getting even…*
Expanding their reach

Birth of a Bot Master

Diagram showing the relationship between Bot Master, Bot Trojan, and Websites, with arrows indicating DDoS Command and DDoS.
Spreading commands

Automatic expansion
Truly automatic

Bot Master

Seed

Bot Worm

Spreading

Bot Worm

Bot Worm

Bot Worm

Bot Worm

Bot Worm
Equality in the eyes of the master

Bot Master

Bot Worm

Bot Worm

Bot Worm

Bot Worm

Bot Worm

Website

DDoS

Command
Moving up in the world

Bot Master

DDoS Command

Bot Worm

Bot Worm

Bot Worm

Bot Worm

Website

DDoS
As the world turns...

- Initially for DDoS power
- Power + Control = $$$!!
- Bot “Industries” created
- Evolving to protect investment
Mitigation techniques

Protocol Filtering

C&C Detected

Bot Master

Bot Worm

Bot Worm

Bot Worm

Bot Worm

Bot Worm

Bot Worm

Cleaned
Evading cleaning

- Polymorphism
- Run-time packers
- Minor variants
- Self-updating
- Application Vulnerabilities
- Changing file-types
- Disabling security apps
- Rootkits
Evading port/protocol filtering

- Encryption
- Web-based C&Cs
- Using alternate ports

*Not readily available for home users!*
Evading C&C shutdown

- Dynamic DNS
- “Friendly” ISPs
- Smaller botnets
- Lieutenants
- Peer to Peer networks
Legal troubles

► Proxies
► Paypal/eGold
► Bureaucracy
► International law

Arrests unlikely to impact bot net threat, say experts

By Tom Espiner, ZDNet UK
04 Jul 2006

Police in London, acting in conjunction with Finnish law enforcement authorities, arrested three suspected virus writers last month.

A 63-year-old man in Suffolk, a 28-year-old man in Scotland, and a 19-year-old man in Finland were arrested in connection with "an international conspiracy to infect computers using viruses attached to unsolicited commercial e-mail," a representative for the Metropolitan Police said.

Dutch Police Crush Big 'Botnet,' Arrest Trio

A huge network of 100,000 PCs was used to conduct a denial-of-service attack against an unidentified U.S. company in an extortion attempt, and for many other nefarious deeds, according to Dutch police.

By Gregg Keizer
TechWeb News
Oct 10, 2005 02:42 PM

Dutch police arrested three men for creating a botnet of more than 100,000 compromised PCs in the Netherlands said Friday. They allege the botnet was used in an attempt to extort a U.S. company, steal PayPal and eBay accounts, and to install adware and spyware.

The pinch is among the biggest botnet scores ever for law enforcement. Dutch authorities said 100,000 infected computers, the dismantled botnet is one of the largest ever seen," the Public Service (Openbaar Ministerie, or OM) said in a statement. The network of hijacked PCs and se
Lessons learned

► Smaller
► Mobility
► Camouflage
► Vulnerabilities
Remaining issues

► Central C&C
► Self-healing
The future?

Bot

Worm

Bot

Master

Bot

Worm

Bot

Worm

Bot

Worm

Bot

Worm

Bot

Worm

Bot

Worm

Bot

Worm

Bot

Worm

Bot

Worm

Bot

Worm

Bot

Worm

Bot

Worm
Early Development

► Phatbot
  ● WASTE-based, no encryption
  ● Gnutella
  ● Non-standard port
  ● Username/Password

► Nugache
  ● WASTE-based, encrypted traffic
  ● Long list of IPs
  ● Gnutella
  ● Smaller file size
Problems

► Phatbot
  ● Unencrypted, easily filtered
  ● Accepts few connections
  ● Central C&C

► Nugache
  ● Unusual port
  ● Accepts few connections
  ● Hard-coded addresses
Solution? IM!

- >70 Million users
- All interconnected
- Businesses/Home users
Why AIM?

► Already familiar
► Up to 500 “buddies”
► Multiple sessions
► “Away” messages
Hurdles

► Still going through a server
► SPIM filtering
No problem!

► Vertical structure
► Personalized messages
► Randomization
► Garbage
► Encryption
► Dedicated IDs
Conclusions

► Defense – More of the same
  ● Software solutions
  ● User Education, early and often
  ● Security Companies, ISPs, LEOs, IM providers
  ● Adware companies held accountable

► Updated laws and processes