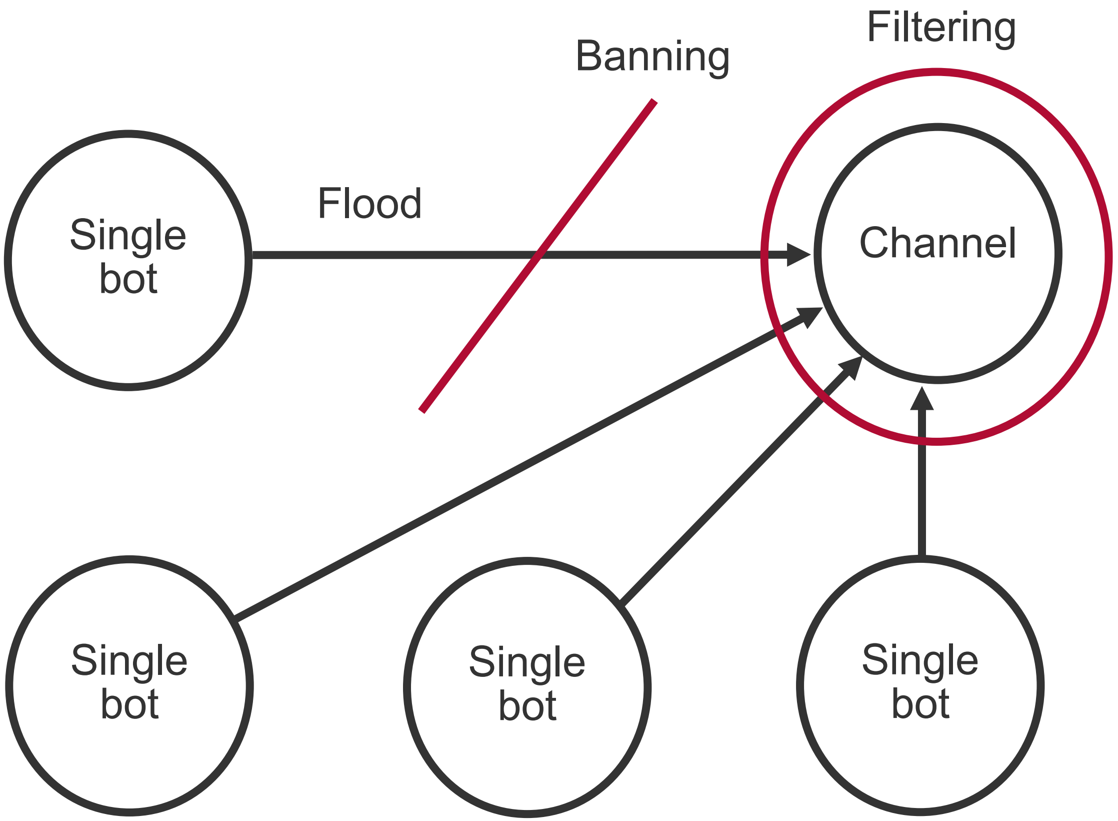
AIM for Bot Coordination

Presented at VB2006

Lysa Myers
Virus Research Engineer
October 11, 2006

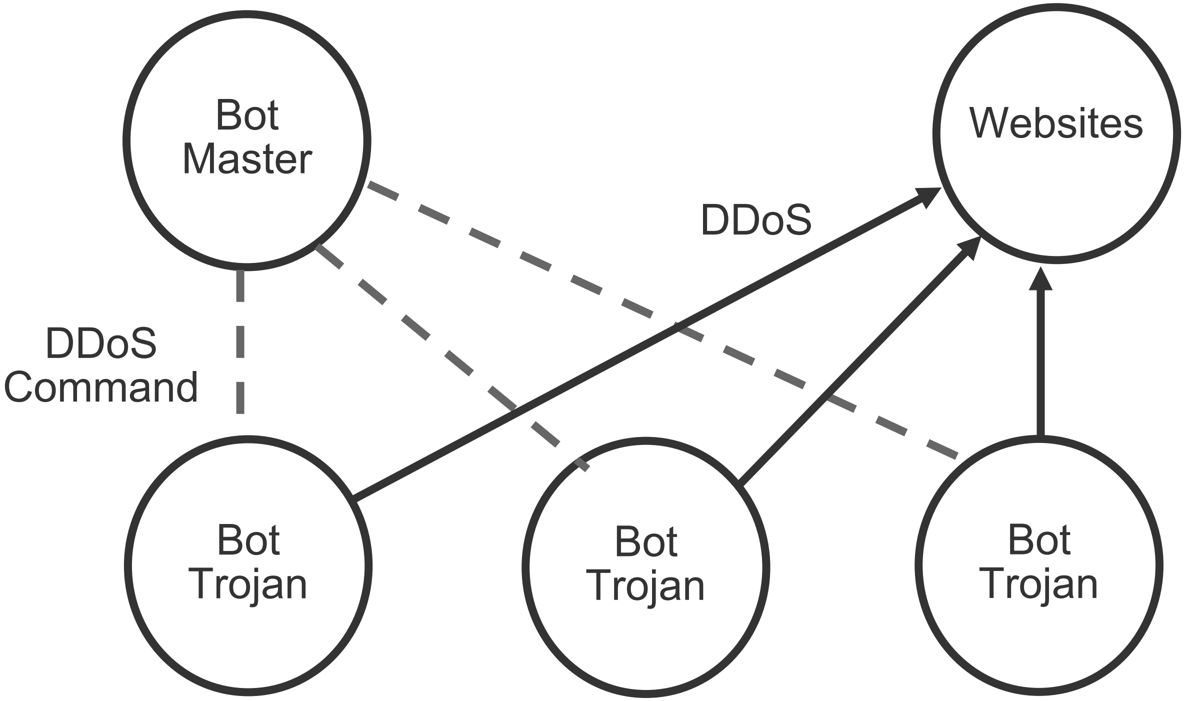
Early experiments with malicious bots

Getting even…



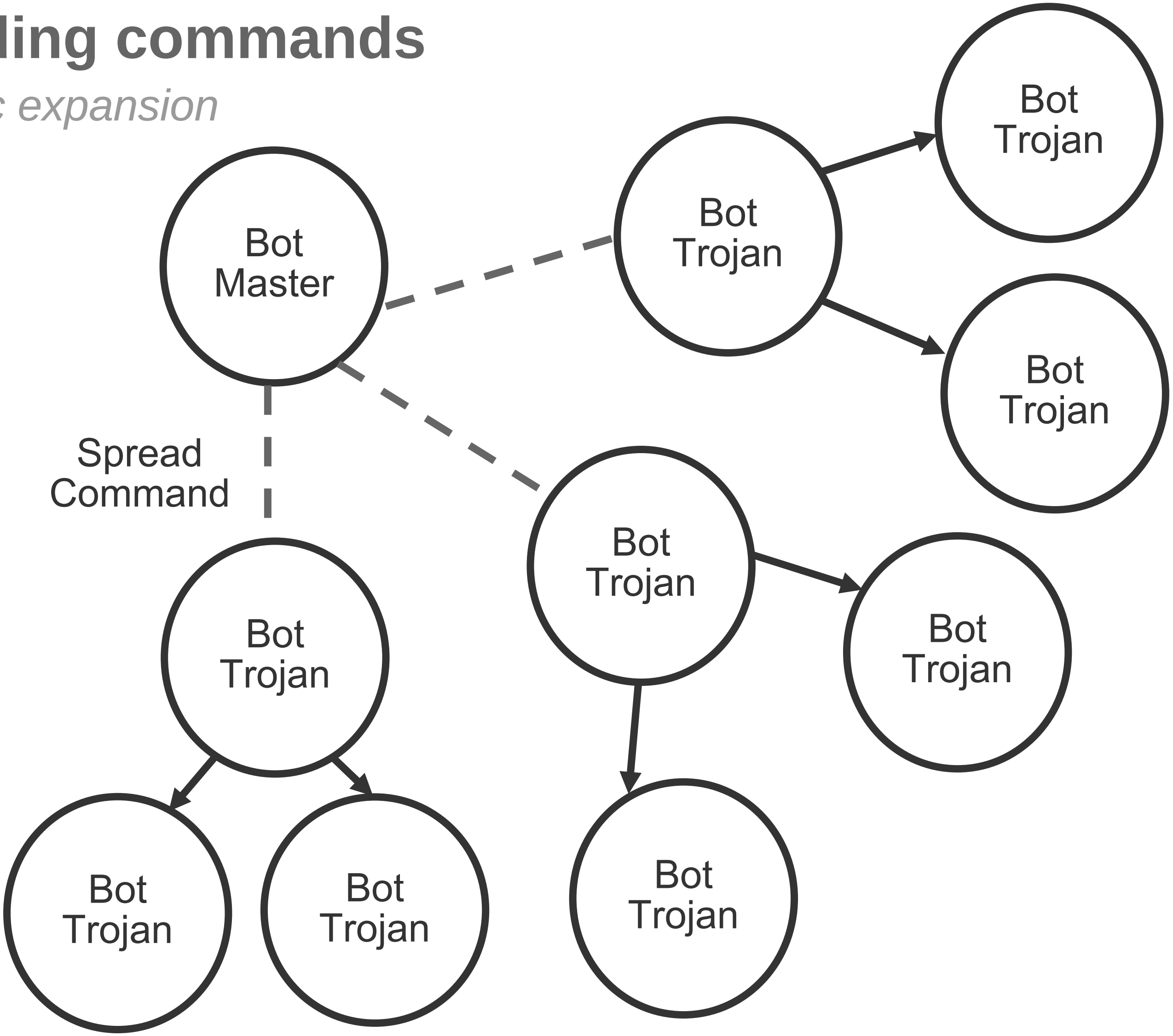
Expanding their reach

Birth of a Bot Master

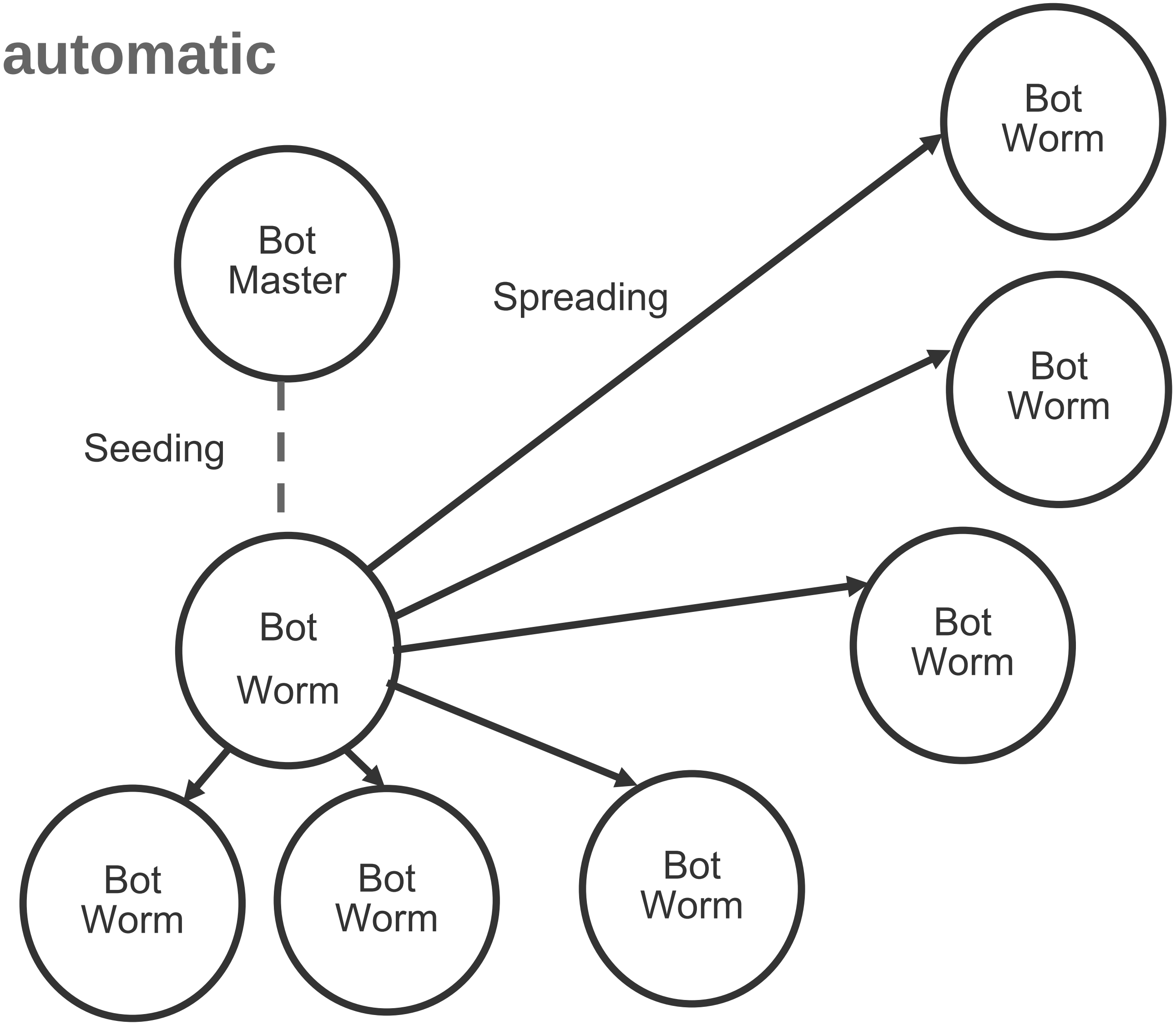


Spreading commands

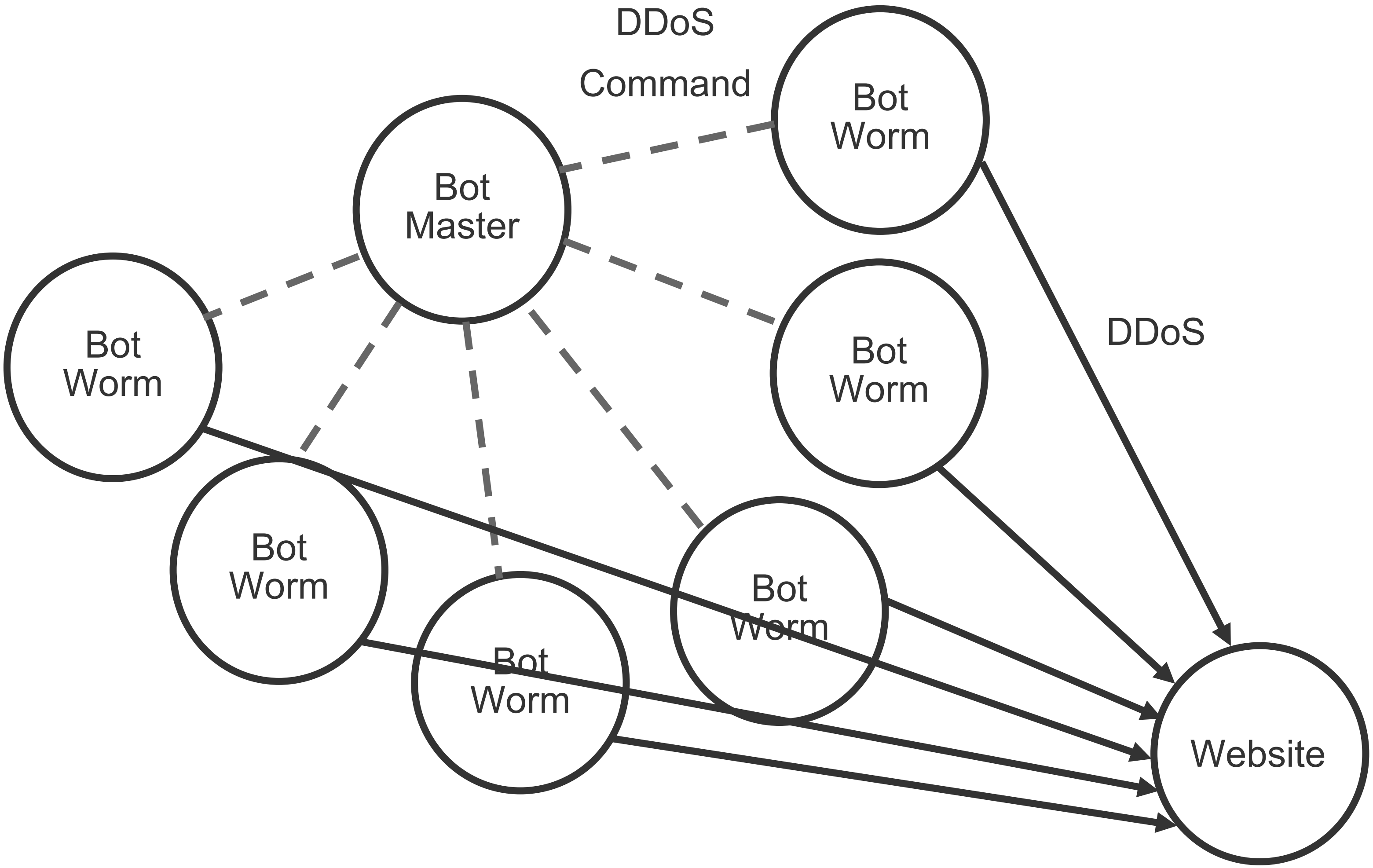
Automatic expansion



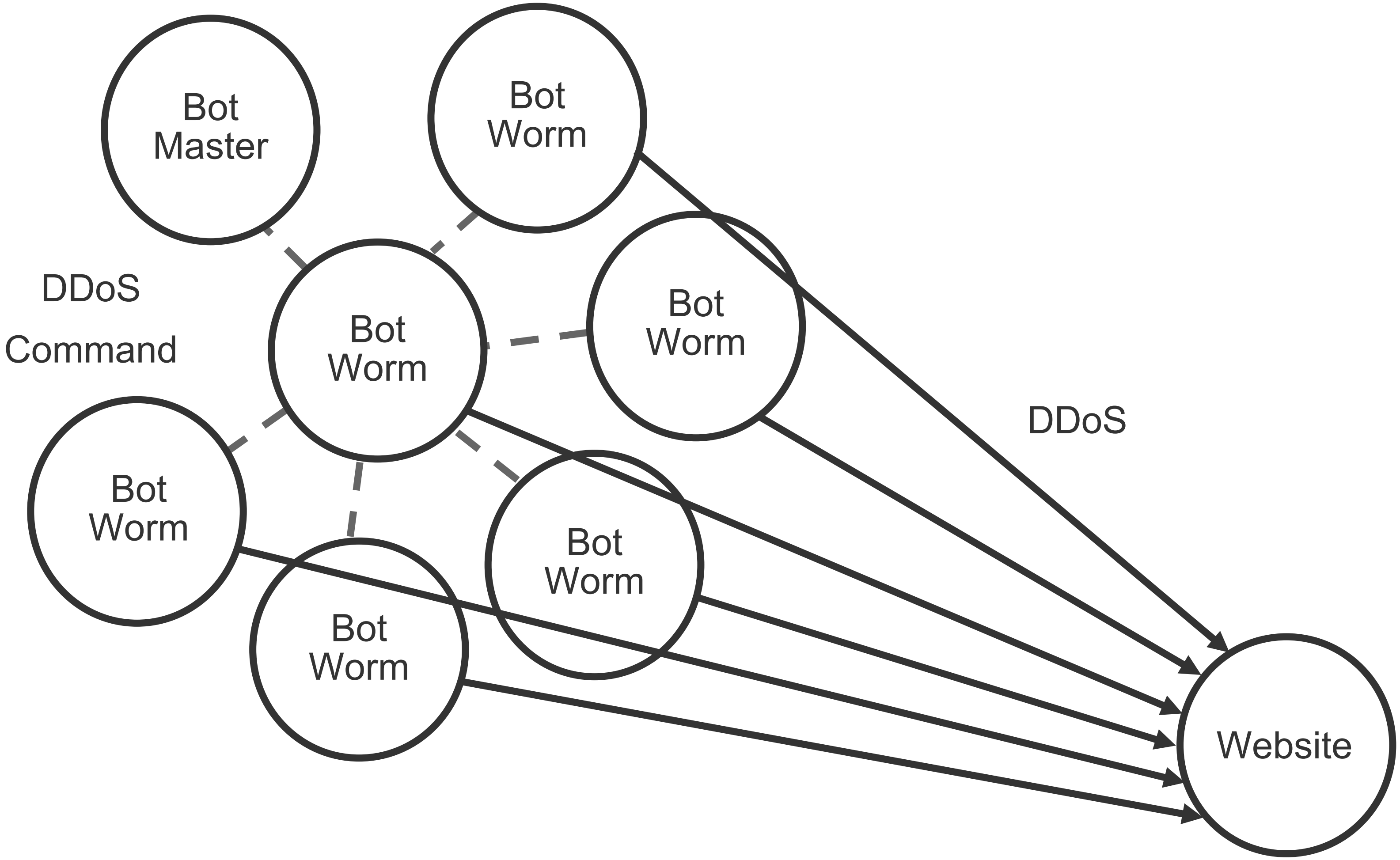
Truly automatic



Equality in the eyes of the master

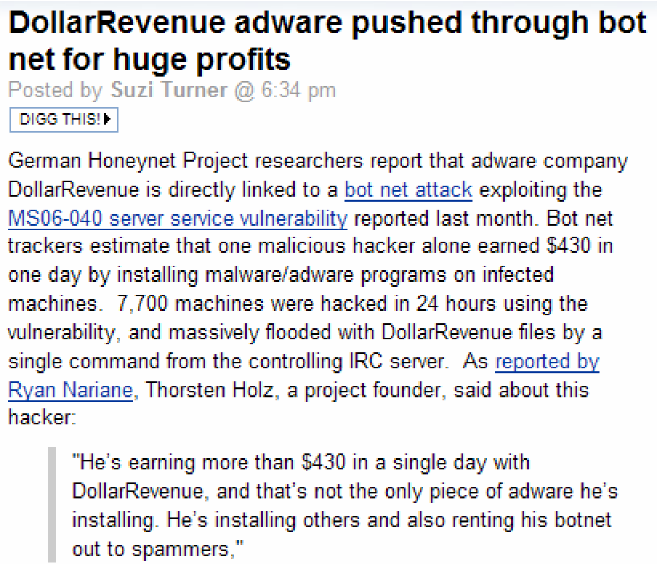


Moving up in the world



As the world turns…

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

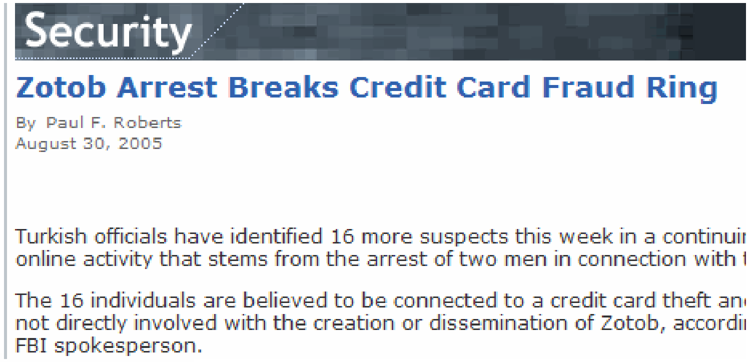


DollarRevenue adware pushed through bot net for huge profits

Posted by Suzi Turner @ 6:34 pm

German Honeynet Project researchers report that adware company DollarRevenue is directly linked to a bot net attack exploiting the MS06-040 server service vulnerability reported last month. Bot net trackers estimate that one malicious hacker alone earned $430 in one day by installing malware/adware programs on infected machines. 7,700 machines were hacked in 24 hours using the vulnerability, and massively flooded with DollarRevenue files by a single command from the controlling IRC server. As reported by Ryan Nariane, Thorsten Holz, a project founder, said about this hacker:

> "He's earning more than $430 in a single day with DollarRevenue, and that's not the only piece of adware he's installing. He's installing others and also renting his botnet out to spammers,"

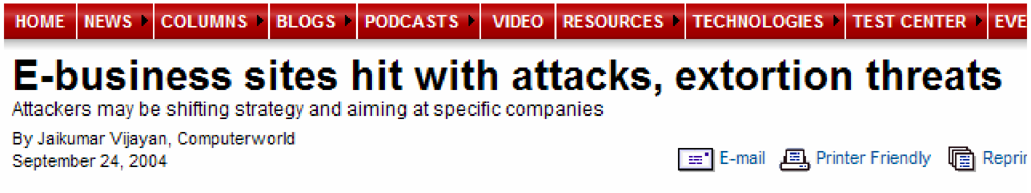


Zotob Arrest Breaks Credit Card Fraud Ring

By Paul F. Roberts
August 30, 2005

Turkish officials have identified 16 more suspects this week in a continuir online activity that stems from the arrest of two men in connection with t

The 16 individuals are believed to be connected to a credit card theft an not directly involved with the creation or dissemination of Zotob, accordi FBI spokesperson.

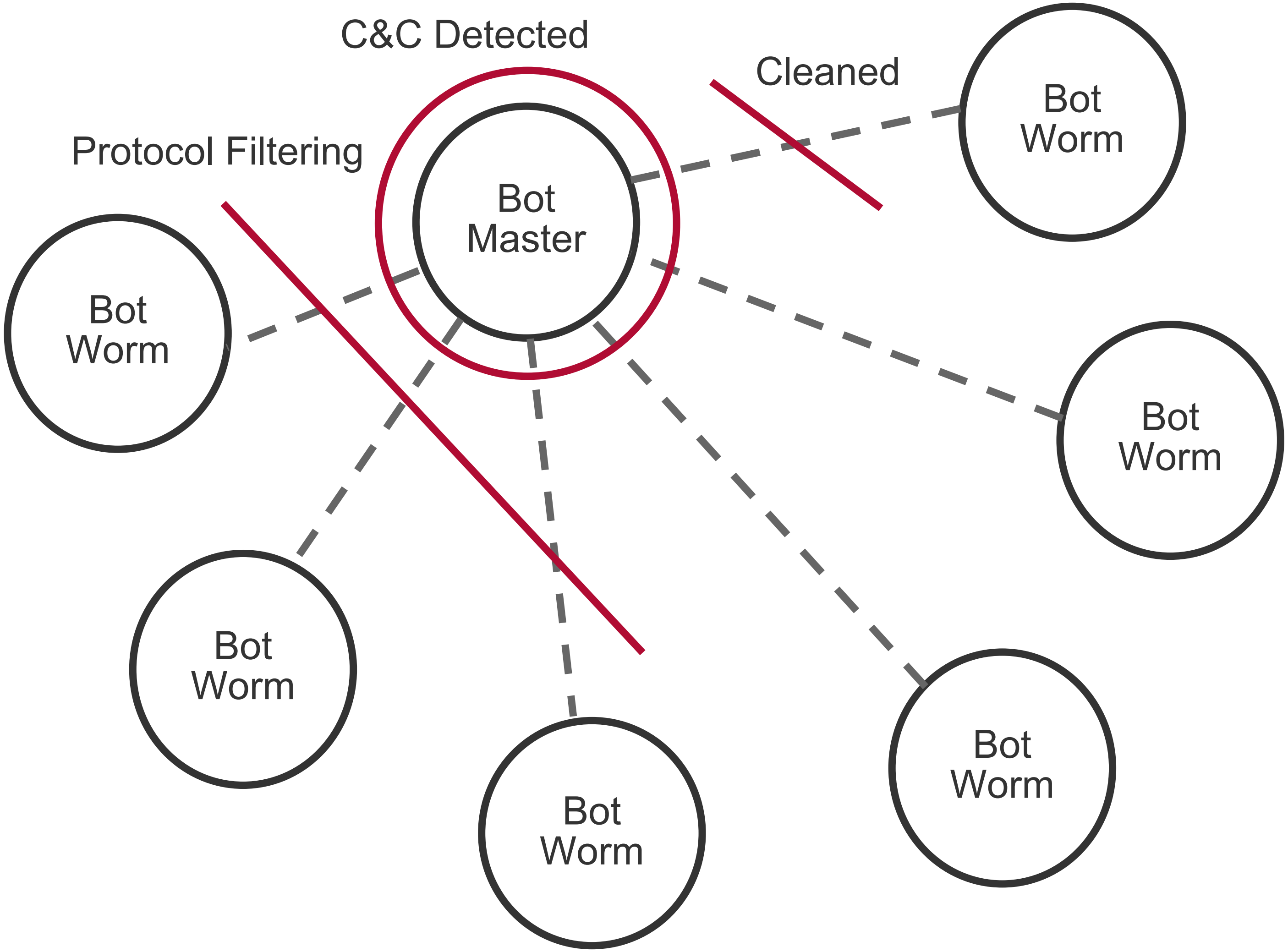


E-business sites hit with attacks, extortion threats

Attackers may be shifting strategy and aiming at specific companies

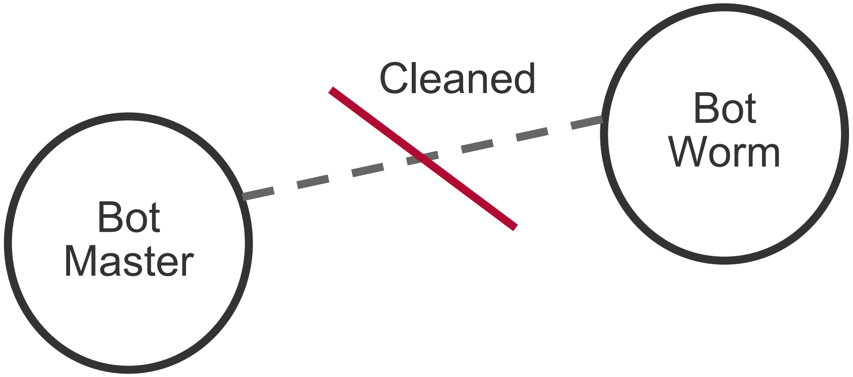
By Jaikumar Vijayan, Computerworld
September 24, 2004

Mitigation techniques



Evading cleaning

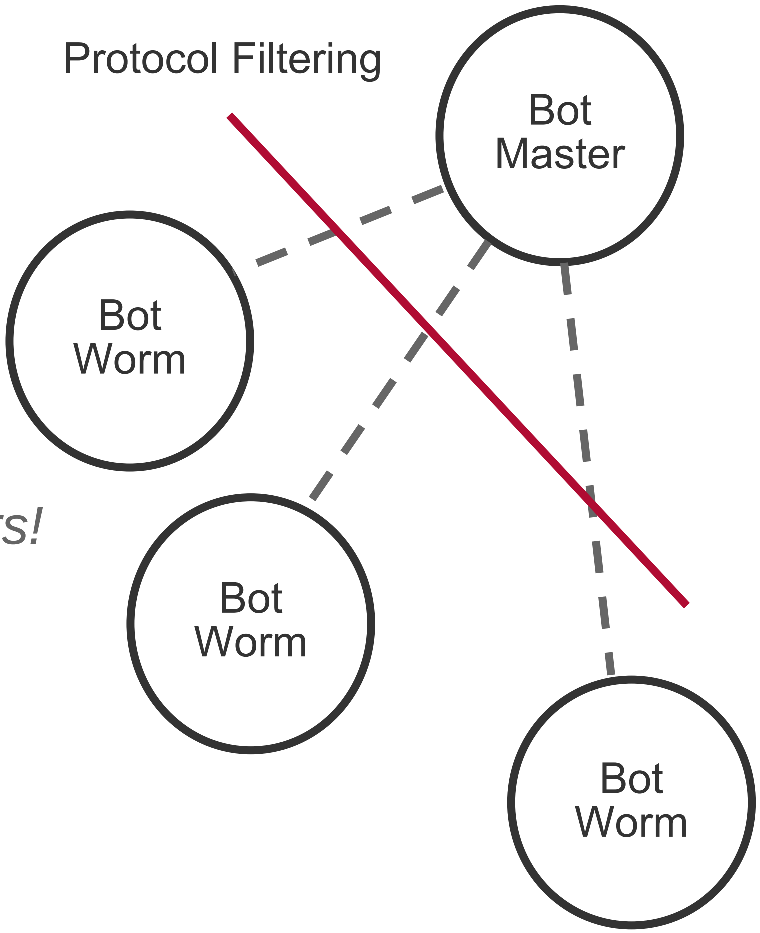
- Polymorphism
- Run-time packers
- Minor variants
- Self-updating
- Application Vulnerabilities
- Changing file-types
- Disabling security apps
- Rootkits



Evading port/protocol filtering

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

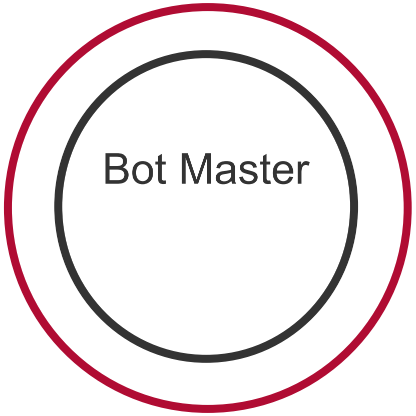
Not readily available for home users!



Evading C&C shutdown

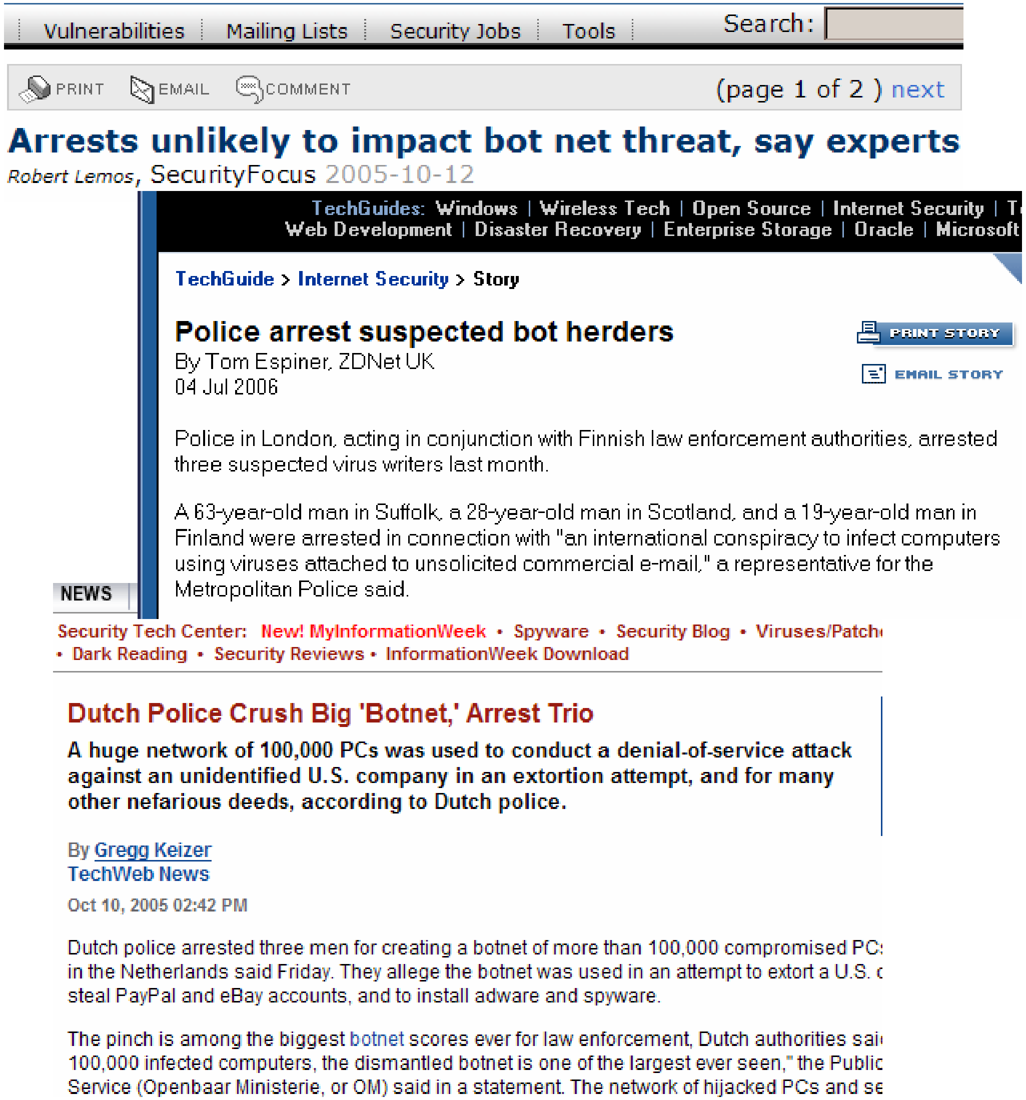
- Dynamic DNS
- “Friendly” ISPs
- Smaller botnets
- Lieutenants
- Peer to Peer networks

C&C Detected



Legal troubles

- ▶ Proxies
- ▶ Paypal/eGold
- ▶ Bureaucracy
- ▶ International law


Vulnerabilities | Mailing Lists | Security Jobs | Tools
Search:
PRINT EMAIL COMMENT
(page 1 of 2) next

Arrests unlikely to impact bot net threat, say experts

Robert Lemos, SecurityFocus 2005-10-12

TechGuides: Windows | Wireless Tech | Open Source | Internet Security | T
Web Development | Disaster Recovery | Enterprise Storage | Oracle | Microsoft
TechGuide > Internet Security > Story
PRINT STORY
EMAIL STORY
NEWS

Police arrest suspected bot herders

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.

Security Tech Center: New! MyInformationWeek • Spyware • Security Blog • Viruses/Patch
• Dark Reading • Security Reviews • InformationWeek Download

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 PC in the Netherlands said Friday. They allege the botnet was used in an attempt to extort a U.S. c steal PayPal and eBay accounts, and to install adware and spyware.

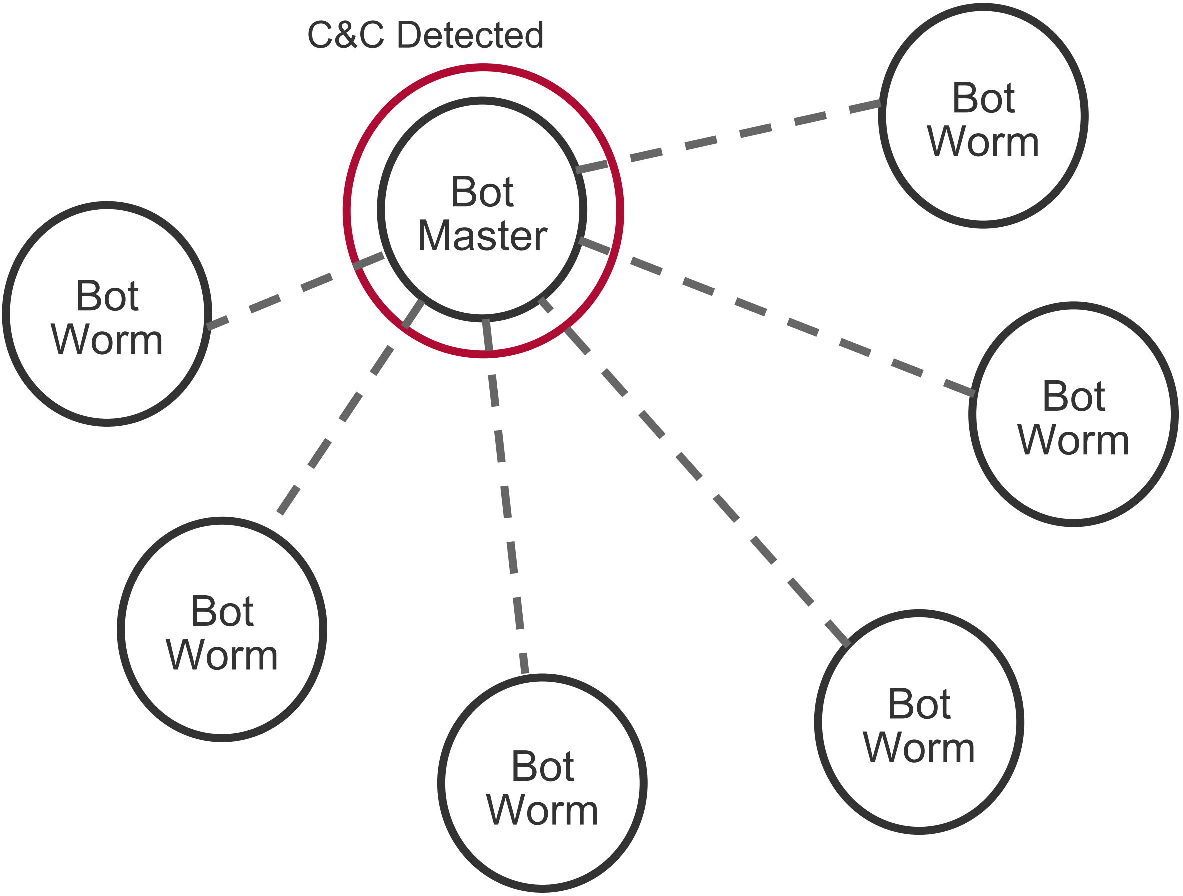
The pinch is among the biggest botnet scores ever for law enforcement, Dutch authorities sai 100,000 infected computers, the dismantled botnet is one of the largest ever seen," the Public Service (Openbaar Ministerie, or OM) said in a statement. The network of hijacked PCs and se

Lessons learned

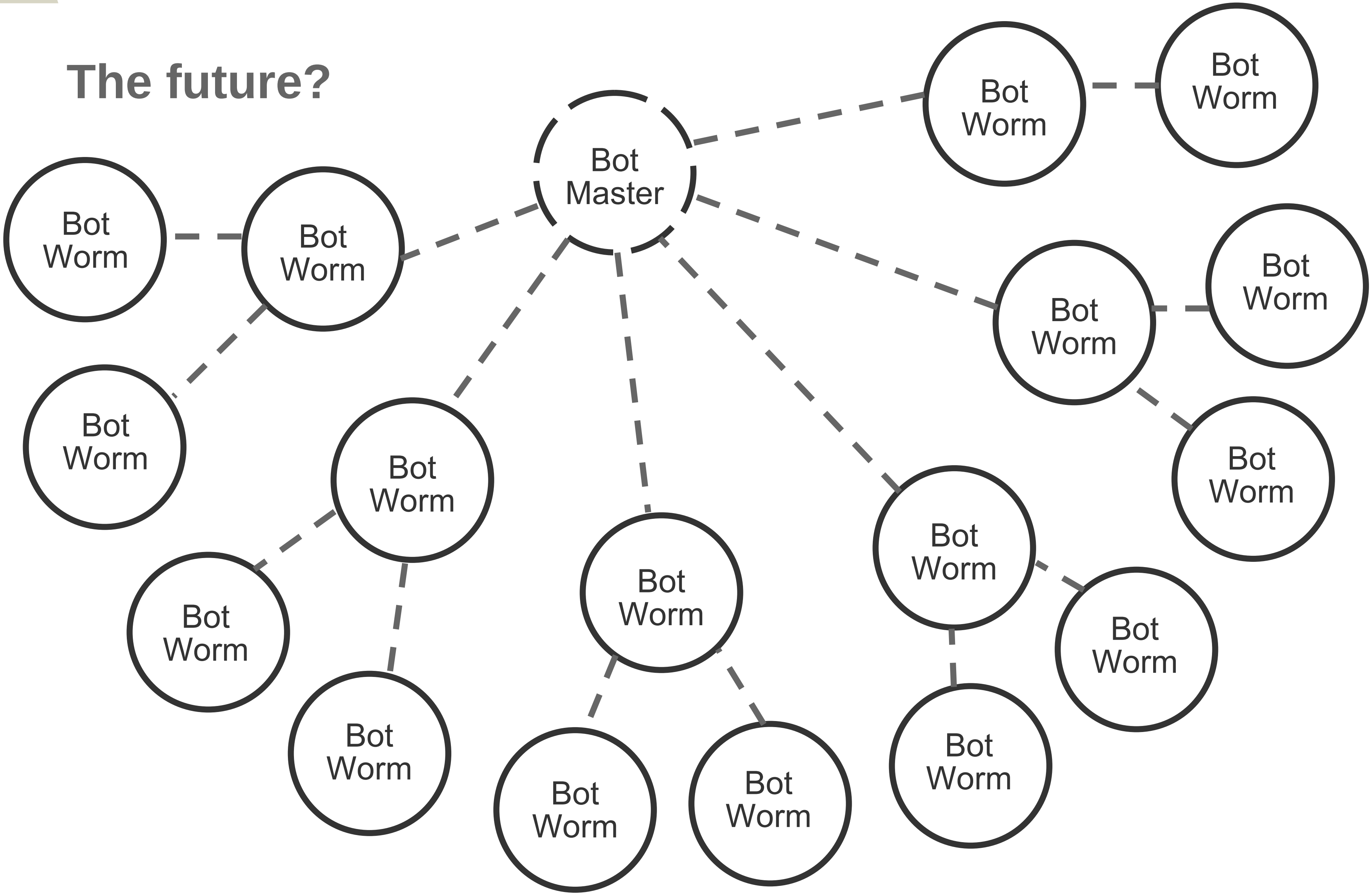
- Smaller
- Mobility
- Camouflage
- Vulnerabilities

Remaining issues

- Central C&C
- Self-healing

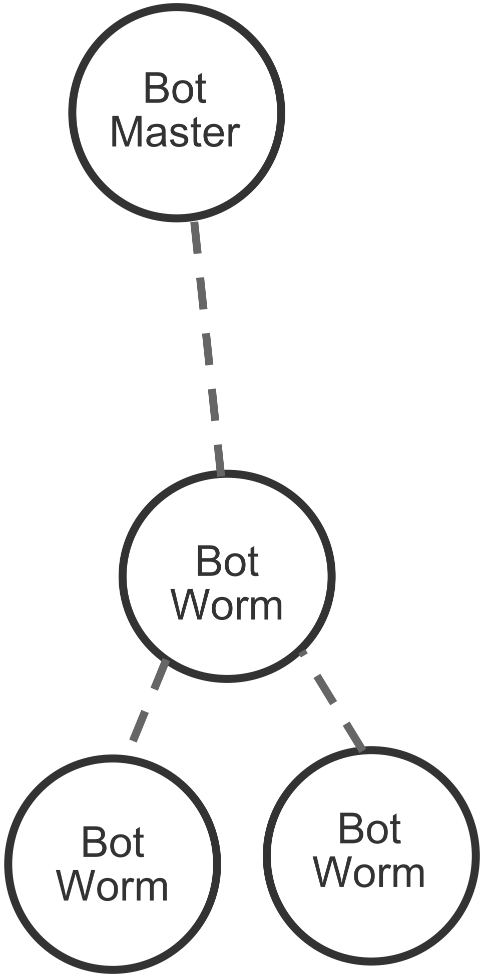


The future?


Bot 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
Bot Worm
Bot Worm
Bot Worm
Bot Worm
Bot Worm
Bot Worm
Bot Worm

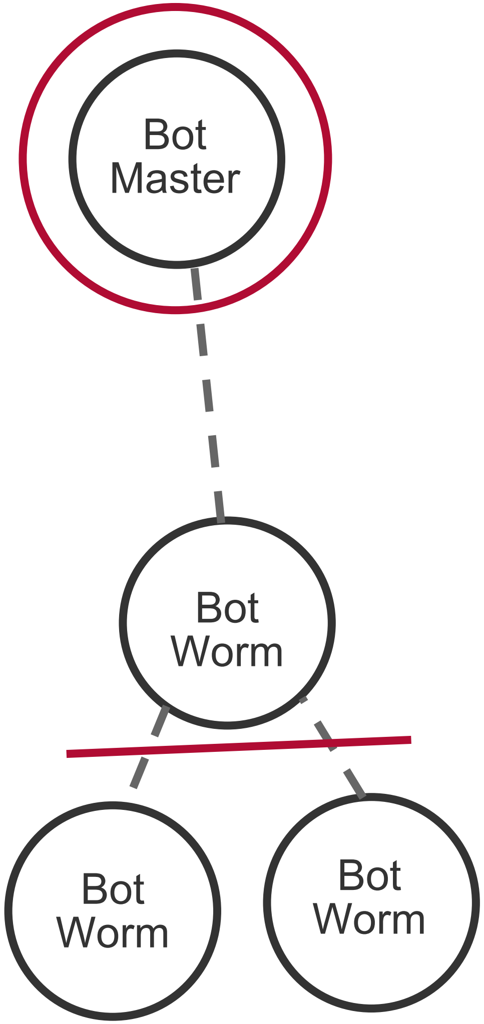
Early Development

- 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

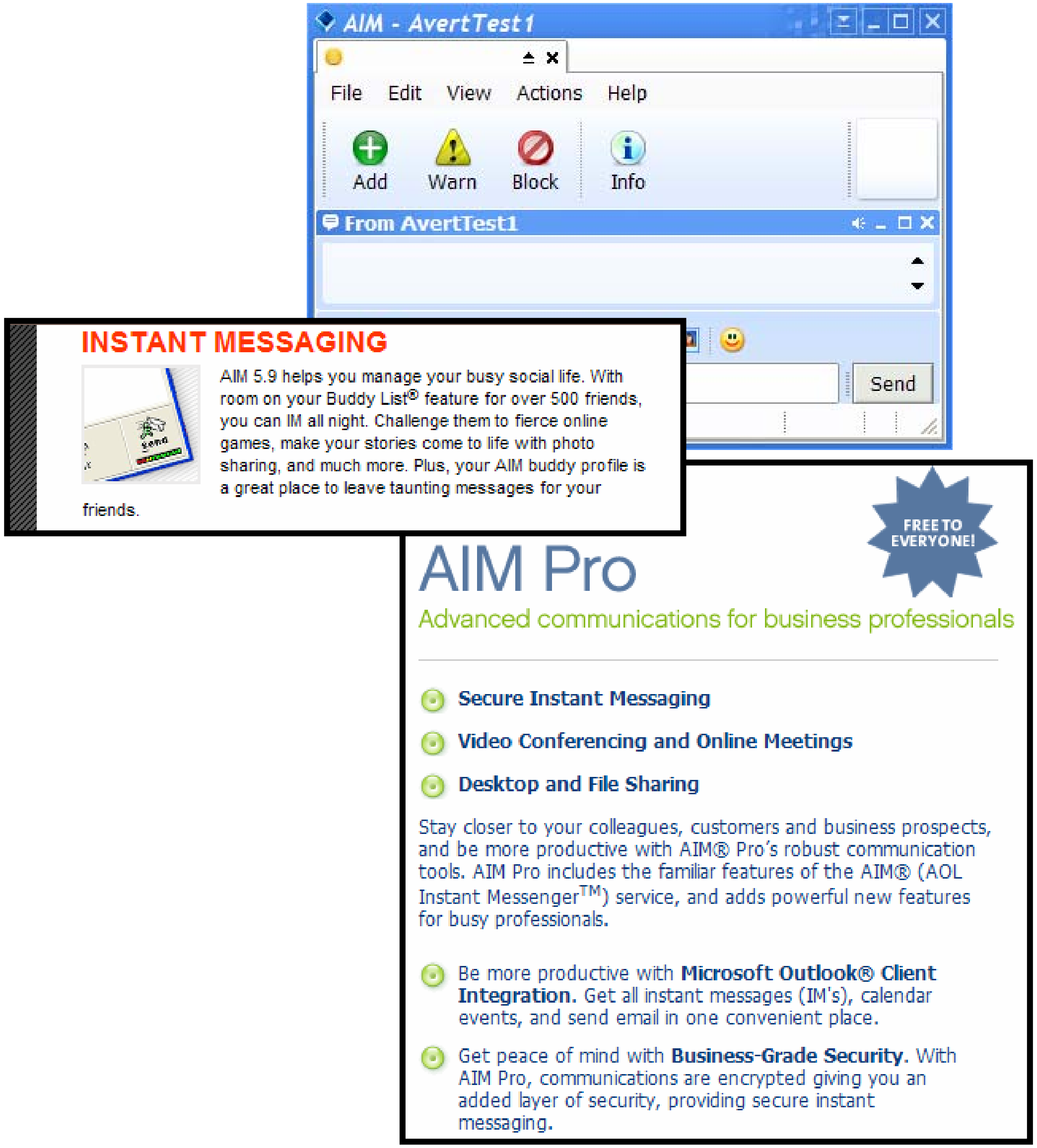


Solution? IM!

- >70 Million users
- All interconnected
- Businesses/Home users

Why AIM?

- ▶ Already familiar
- ▶ Up to 500 “buddies”
- ▶ Multiple sessions
- ▶ “Away” messages



INSTANT MESSAGING

AIM 5.9 helps you manage your busy social life. With room on your Buddy List® feature for over 500 friends, you can IM all night. Challenge them to fierce online games, make your stories come to life with photo sharing, and much more. Plus, your AIM buddy profile is a great place to leave taunting messages for your friends.

AIM Pro

Advanced communications for business professionals

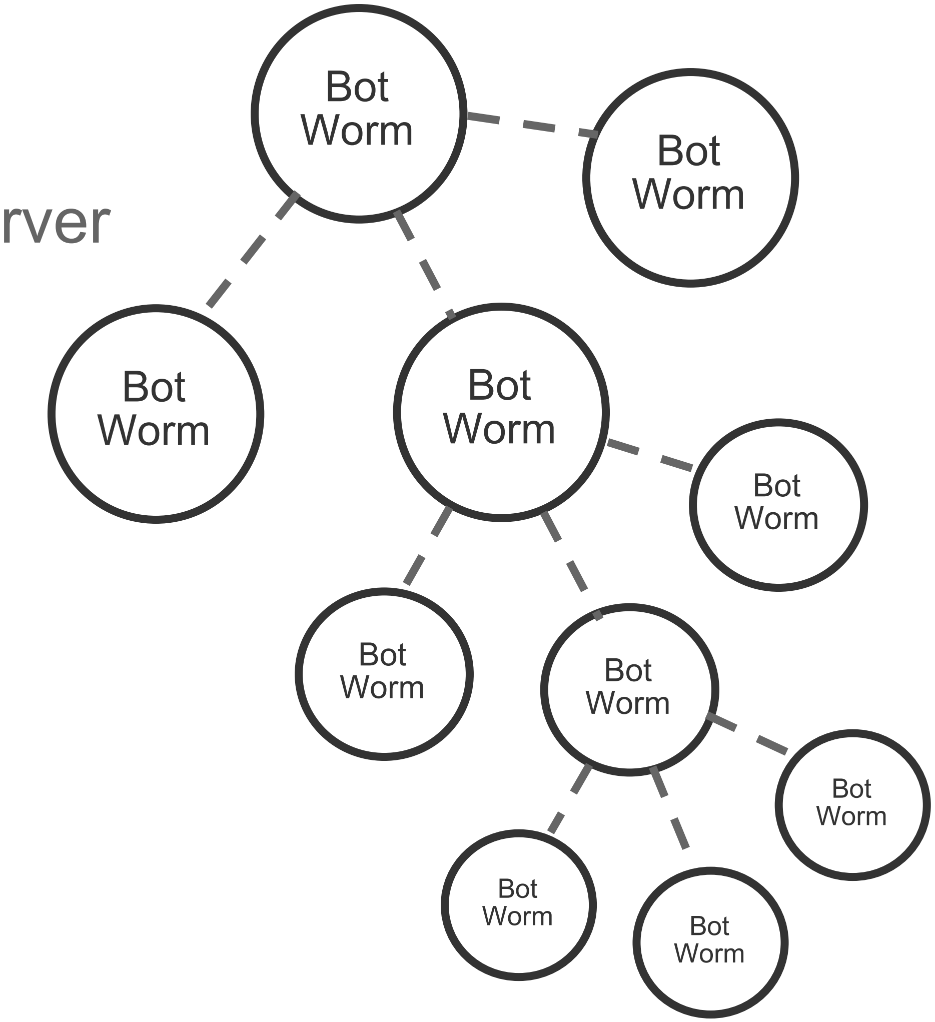
- Secure Instant Messaging
- Video Conferencing and Online Meetings
- Desktop and File Sharing

Stay closer to your colleagues, customers and business prospects, and be more productive with AIM® Pro’s robust communication tools. AIM Pro includes the familiar features of the AIM® (AOL Instant Messenger^TM) service, and adds powerful new features for busy professionals.

- Be more productive with **Microsoft Outlook® Client Integration.** Get all instant messages (IM's), calendar events, and send email in one convenient place.
- Get peace of mind with **Business-Grade Security.** With AIM Pro, communications are encrypted giving you an added layer of security, providing secure instant messaging.

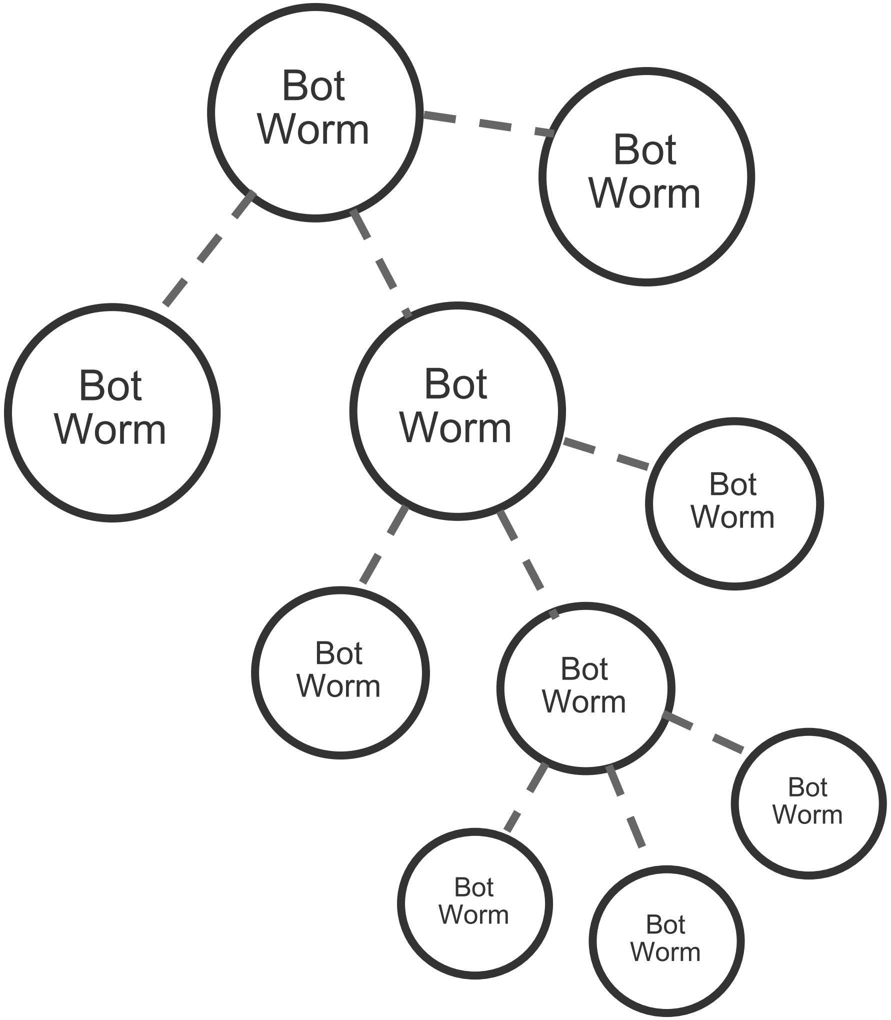
Hurdles

- 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