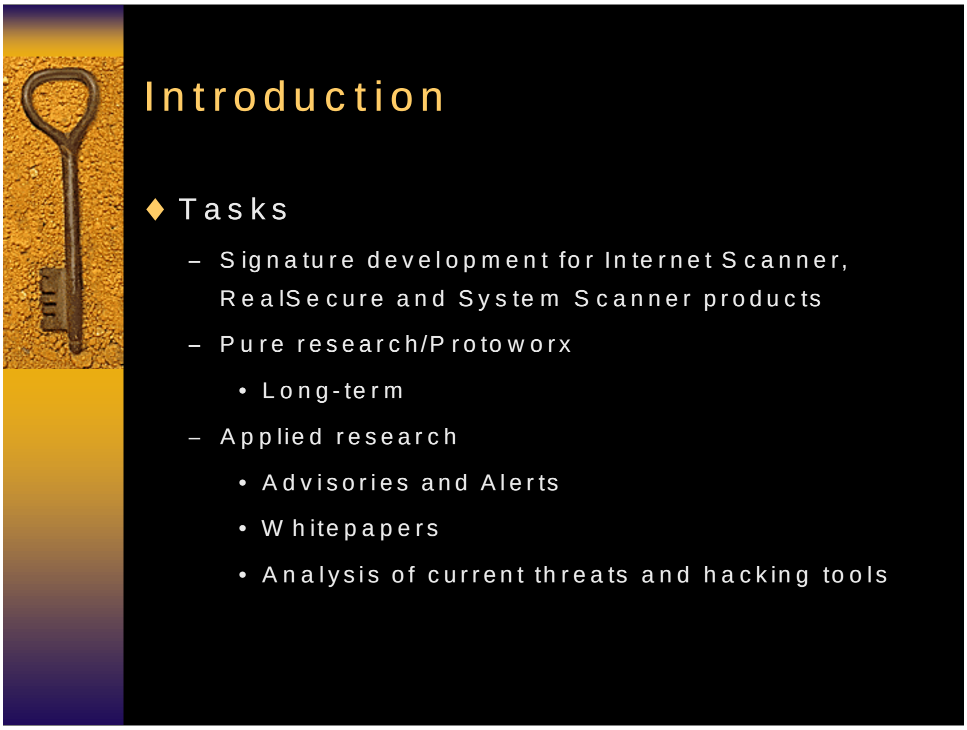
Vulnerability Trends

Dan Ingevaldson

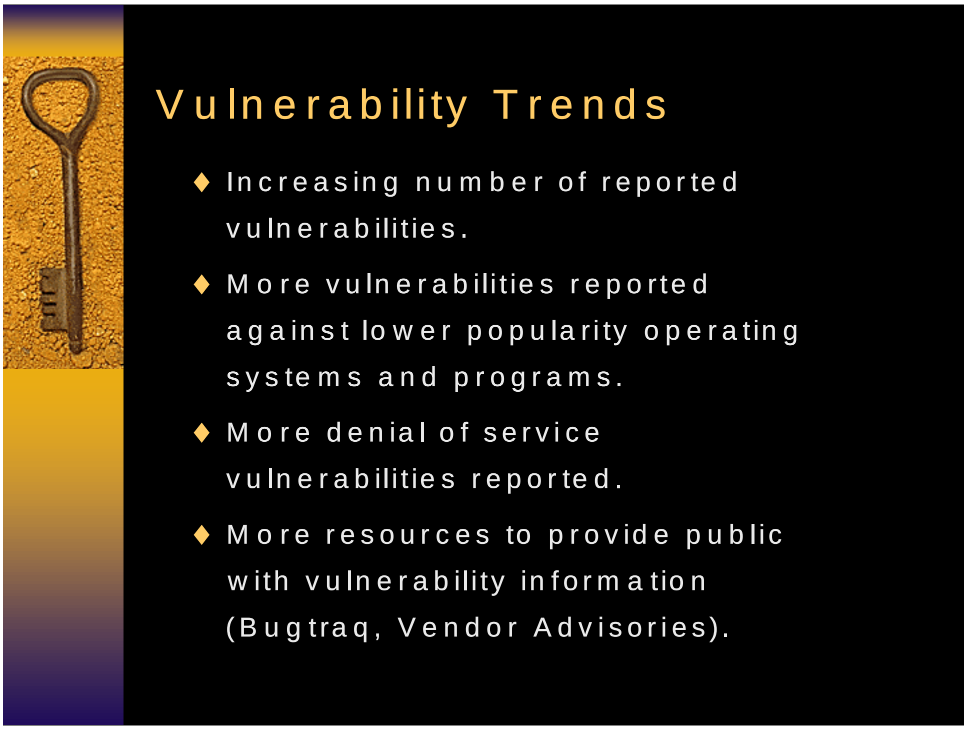
Technical Product Manager

ISS X-Force



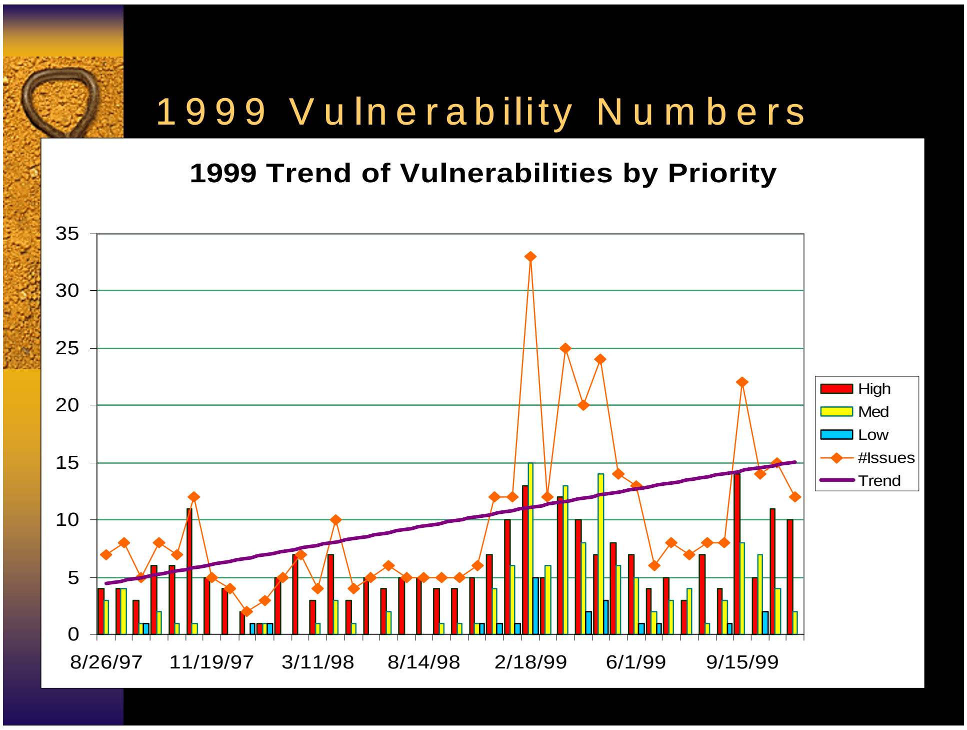
Introduction

- Tasks
  - Signature development for Internet Scanner, RealSecure and System Scanner products
  - Pure research/Protoworx
    - Long-term
  - Applied research
    - Advisories and Alerts
    - Whitepapers
    - Analysis of current threats and hacking tools



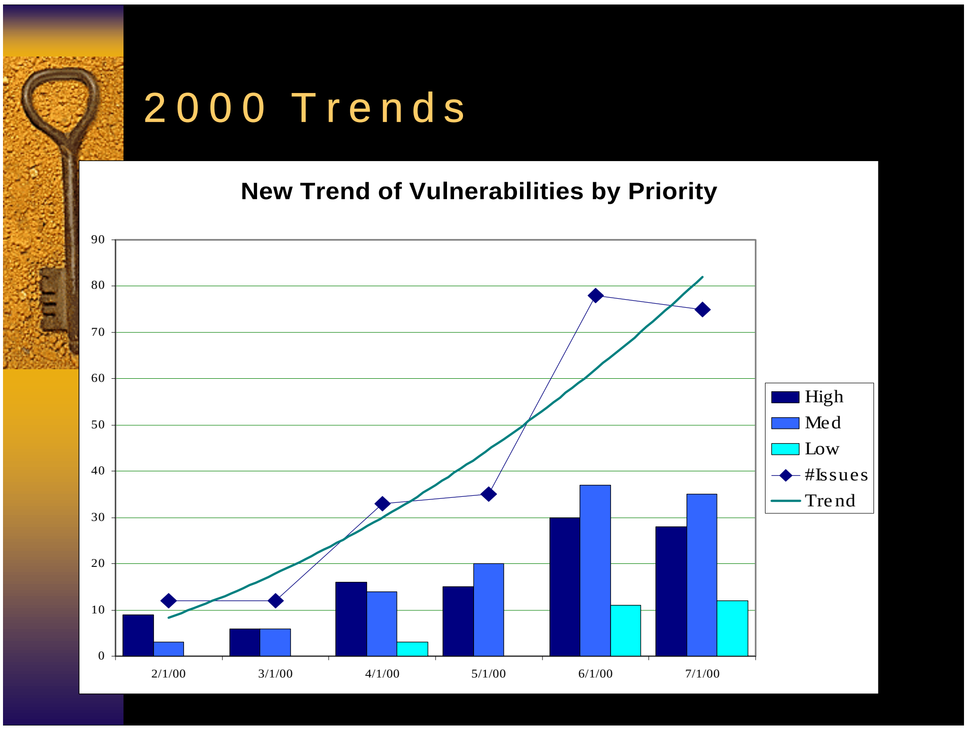
Vulnerability Trends

- Increasing number of reported vulnerabilities.
- More vulnerabilities reported against lower popularity operating systems and programs.
- More denial of service vulnerabilities reported.
- More resources to provide public with vulnerability information (Bugtraq, Vendor Advisories).

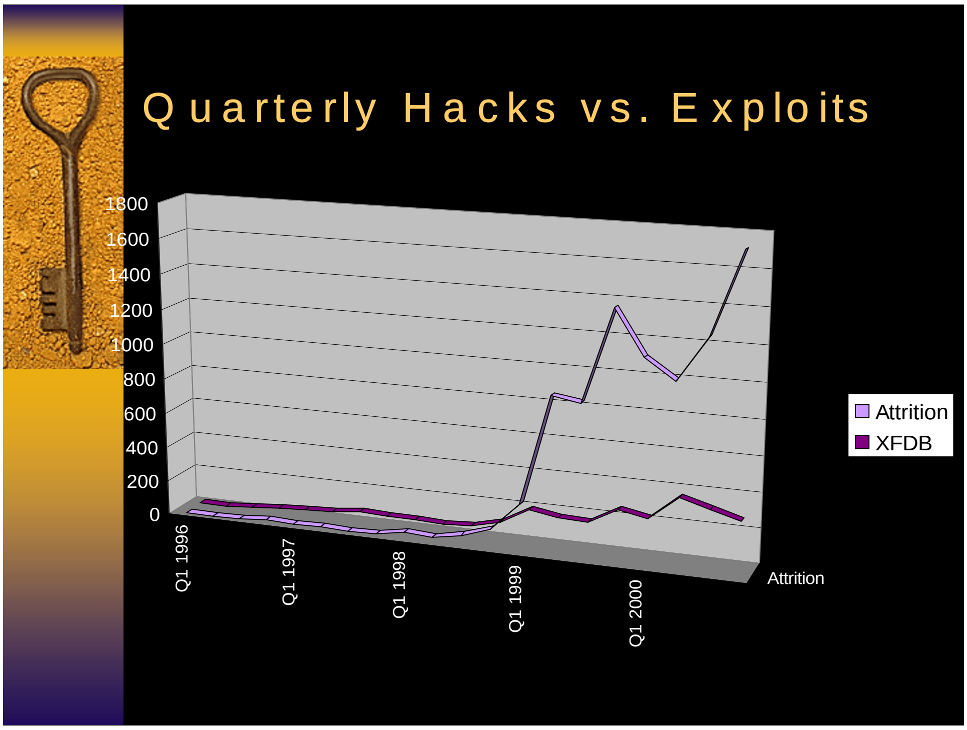


1999 Vulnerability Numbers

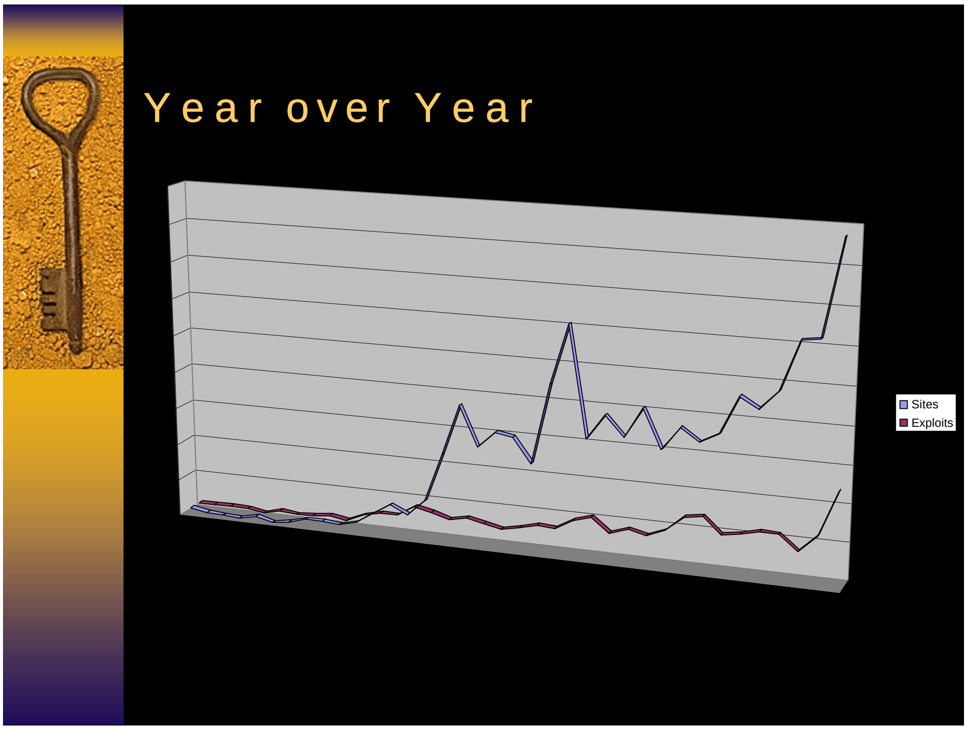
1999 Trend of Vulnerabilities by Priority



2000 Trends



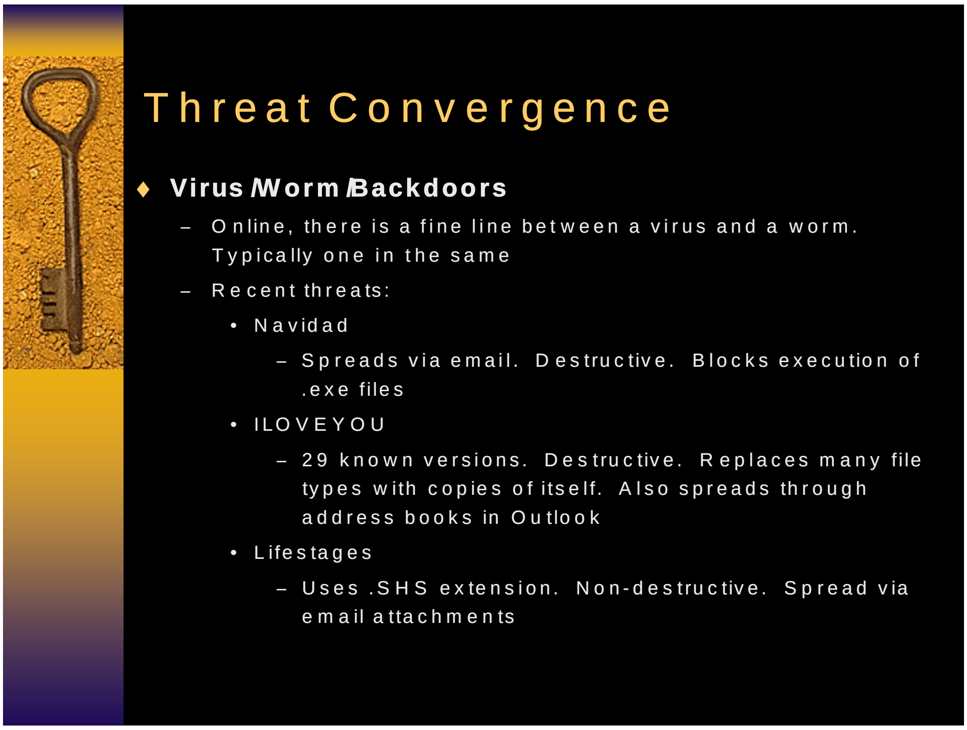
Quarterly Hacks vs. Exploits



Year over Year

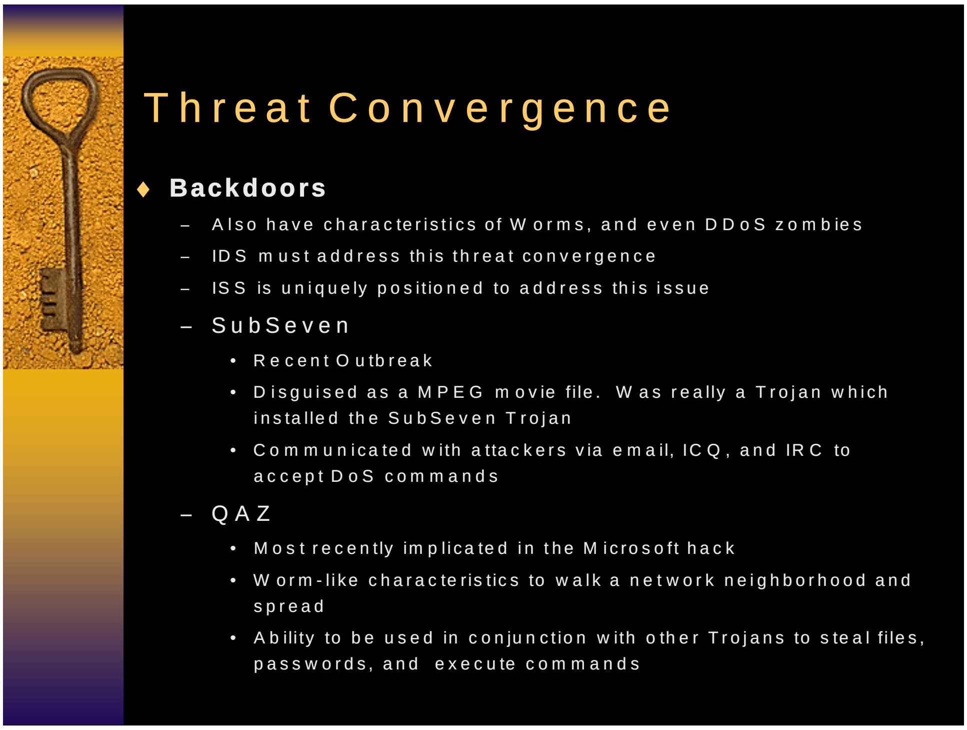
New threat Technologies

- Backdoor/Trojan/Virus
- Chat Systems (yikes!)
- DDoS
- Dynamic Perimeter?
- Moving UP the stack



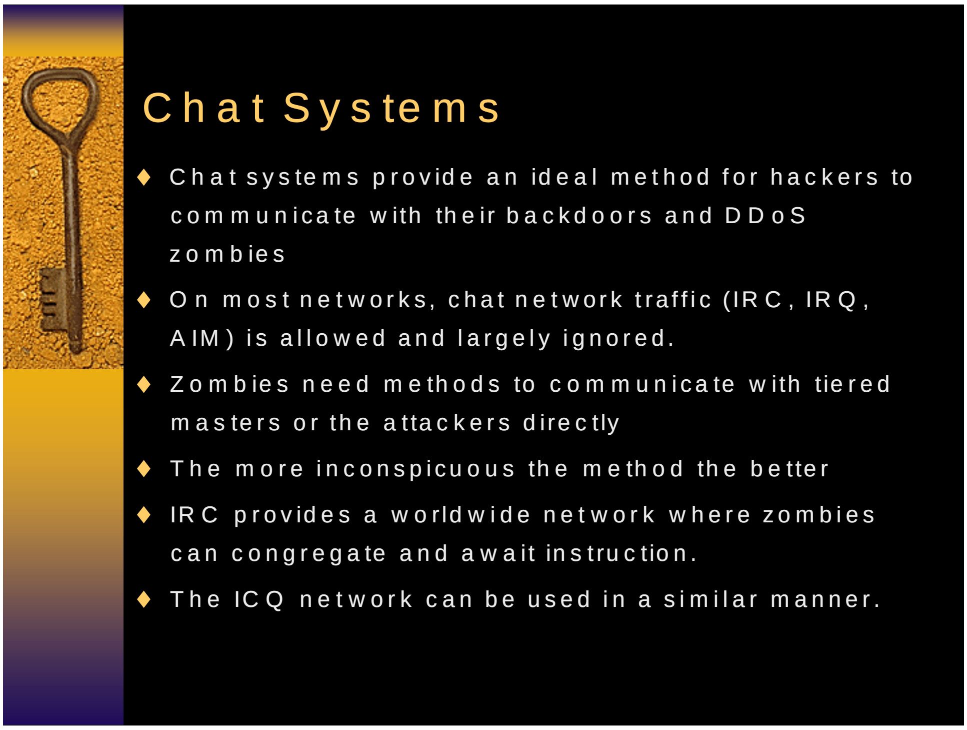
Threat Convergence

- **Virus /Worm /Backdoors**
  - Online, there is a fine line between a virus and a worm. Typically one in the same
  - Recent threats:
    - Navidad
      - Spreads via email. Destructive. Blocks execution of .exe files
    - ILOVEYOU
      - 29 known versions. Destructive. Replaces many file types with copies of itself. Also spreads through address books in Outlook
    - Lifestages
      - Uses .SHS extension. Non-destructive. Spread via email attachments



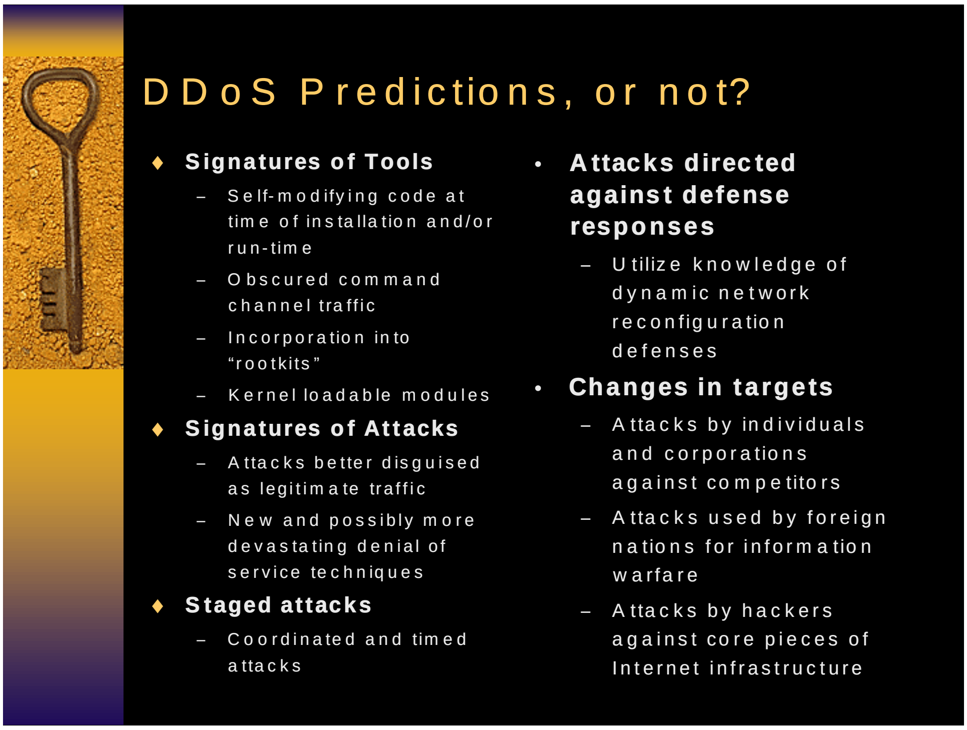
Threat Convergence

- **Backdoors**
  - Also have characteristics of Worms, and even DDoS zombies
  - IDS must address this threat convergence
  - ISS is uniquely positioned to address this issue
  - SubSeven
    - Recent Outbreak
    - Disguised as a MPEG movie file. Was really a Trojan which installed the SubSeven Trojan
    - Communicated with attackers via email, ICQ, and IRC to accept DoS commands
  - QAZ
    - Most recently implicated in the Microsoft hack
    - Worm-like characteristics to walk a network neighborhood and spread
    - Ability to be used in conjunction with other Trojans to steal files, passwords, and execute commands



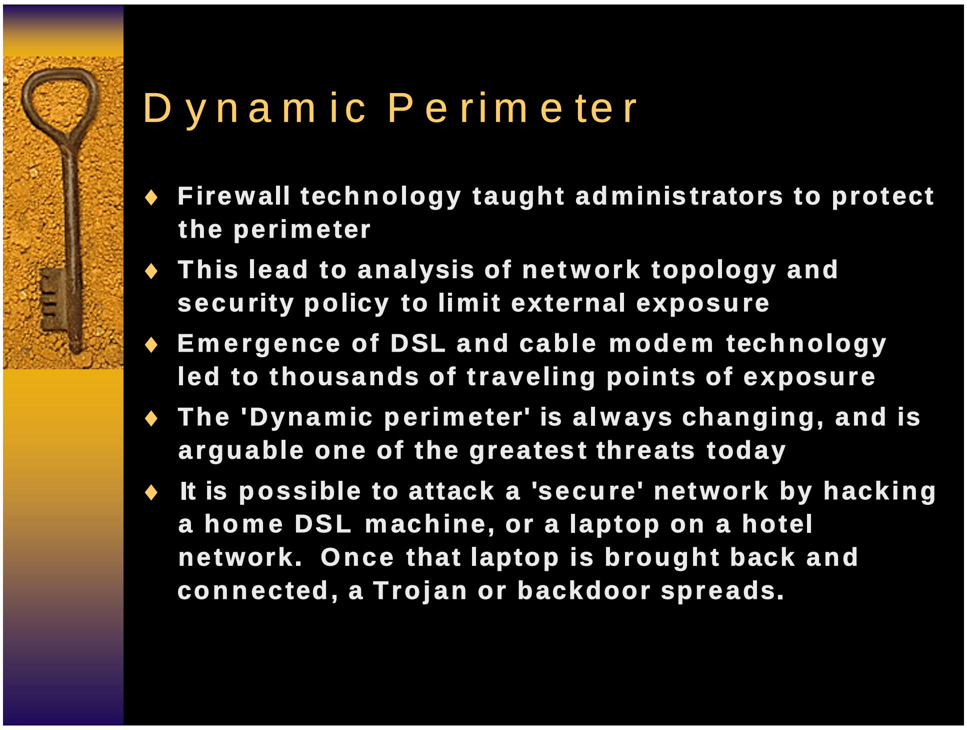
Chat Systems

- Chat systems provide an ideal method for hackers to communicate with their backdoors and DDoS zombies
- On most networks, chat network traffic (IRC, IRQ, AIM) is allowed and largely ignored.
- Zombies need methods to communicate with tiered masters or the attackers directly
- The more inconspicuous the method the better
- IRC provides a worldwide network where zombies can congregate and await instruction.
- The ICQ network can be used in a similar manner.



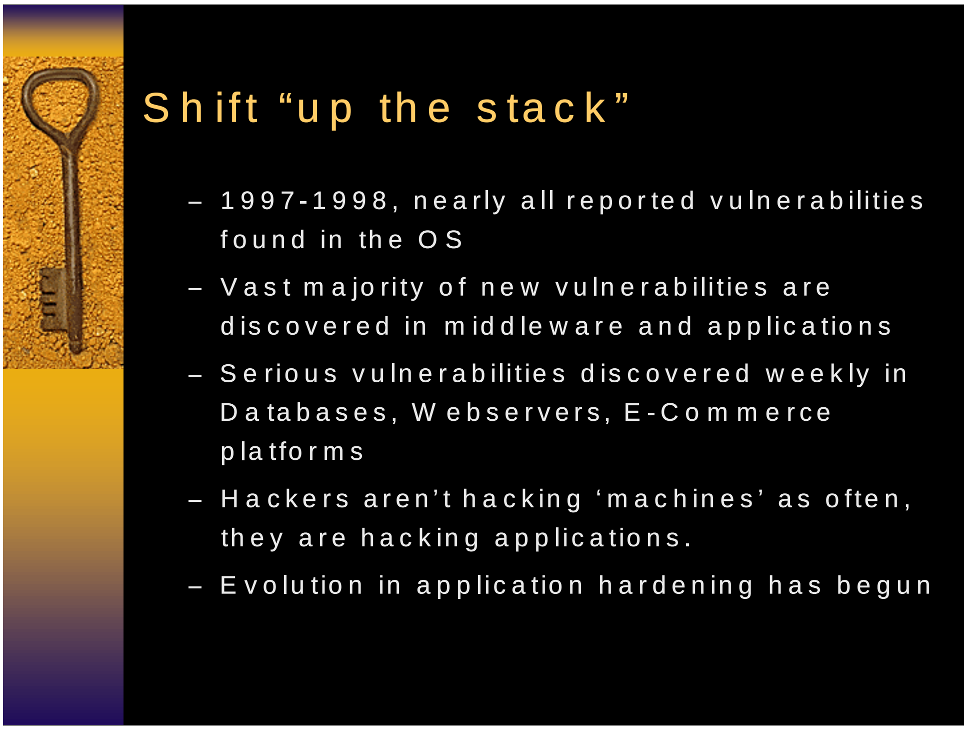
DDoS Predictions, or not?

- **Signatures of Tools**
  - Self-modifying code at time of installation and/or run-time
  - Obscured command channel traffic
  - Incorporation into “rootkits”
  - Kernel loadable modules
- **Signatures of Attacks**
  - Attacks better disguised as legitimate traffic
  - New and possibly more devastating denial of service techniques
- **Staged attacks**
  - Coordinated and timed attacks
- **Attacks directed against defense responses**
  - Utilize knowledge of dynamic network reconfiguration defenses
- **Changes in targets**
  - Attacks by individuals and corporations against competitors
  - Attacks used by foreign nations for information warfare
  - Attacks by hackers against core pieces of Internet infrastructure



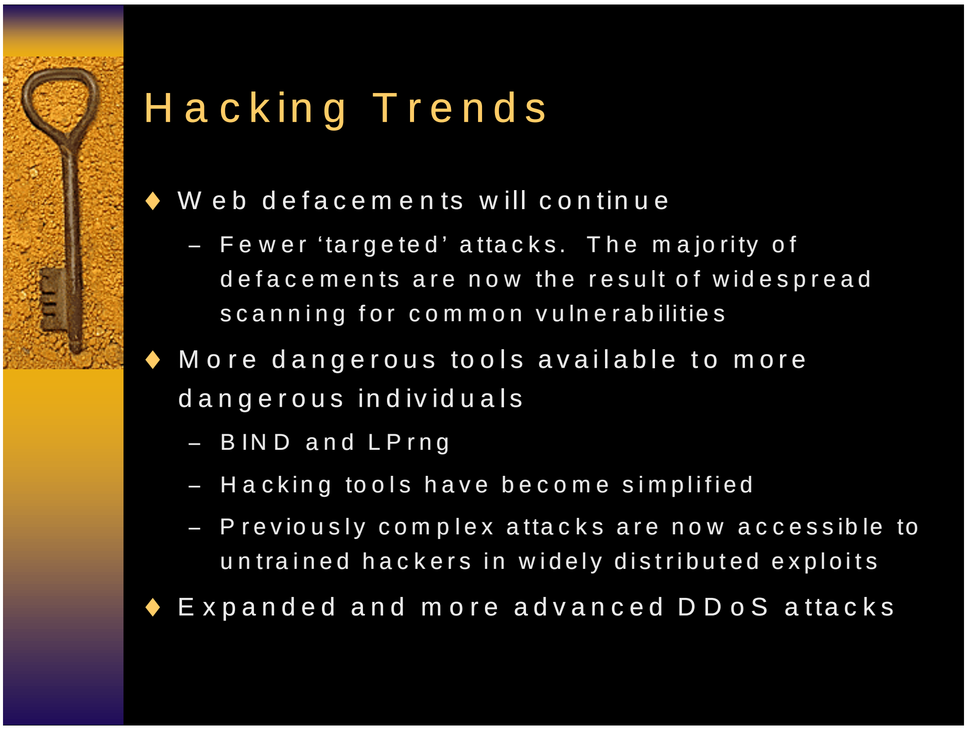
Dynamic Perimeter

- Firewall technology taught administrators to protect the perimeter
- This lead to analysis of network topology and security policy to limit external exposure
- Emergence of DSL and cable modem technology led to thousands of traveling points of exposure
- The 'Dynamic perimeter' is always changing, and is arguable one of the greatest threats today
- It is possible to attack a 'secure' network by hacking a home DSL machine, or a laptop on a hotel network. Once that laptop is brought back and connected, a Trojan or backdoor spreads.



Shift “up the stack”

- 1997-1998, nearly all reported vulnerabilities found in the OS
- Vast majority of new vulnerabilities are discovered in middleware and applications
- Serious vulnerabilities discovered weekly in Databases, Webservers, E-Commerce platforms
- Hackers aren’t hacking ‘machines’ as often, they are hacking applications.
- Evolution in application hardening has begun



Hacking Trends

- Web defacements will continue
  - Fewer 'targeted' attacks. The majority of defacements are now the result of widespread scanning for common vulnerabilities
- More dangerous tools available to more dangerous individuals
  - BIND and LPrng
  - Hacking tools have become simplified
  - Previously complex attacks are now accessible to untrained hackers in widely distributed exploits
- Expanded and more advanced DDoS attacks

Vulnerability Trends

Dan Ingevaldson

Technical Product Manager

ISS X-Force