ISP Security BoF – NANOG 28 Attacks

- Total through 01 June 2003 – 1311.
- Size – 2 x 5Gbps, several x 1Gbps.
- Mostly ICMP and UDP.
- Rarely use spoofed source addresses
  - Why bother when you have 140K bots? :/

ISP Security BoF – NANOG 28
Scans

- Win2K shares – TCP 445
  - Initially null passwords.
  - Now includes brute force password crackers.
  - Locks down the host after infection – a miscreant patching service!
- Subseven – TCP 27374
  - Requires a previous infection by Subseven.
- Kuang2 – TCP 17300
  - Requires a previous infection by Kuang2.
- Telnet – TCP 23
  - Seeking easily compromised routers, both Cayman and Cisco.
- ICMP – 8 0
  - Seeking smurf amplifiers.

ISP Security BoF – NANOG 28
Malware

- GT family – Coldlife, GTSEV1, GTSEV2.
- Sdbot – 0.5a, 0.5b, 0.5b + SYN.
- Spybot – 1.2, 1.2 + TCP 445.
- Laws of supply and demand.
- Many bots include key logging and other advanced features. It isn't only about DDoS.
  - Bots + Quake.
  - The mysterious CDROM drive.
- What sneaks in under all this noise?

ISP Security BoF – NANOG 28
Statistics as of 01 June 2003

- Hacked hosts – 423262
- Abused proxies – 192608
- Compromised routers – 5410

- Q: How hard is it to obtain a compromised device?
- A: Can you type any of the following?
  - !cisco
  - !cayman
  - !proxy