Israeli Internet Hacking Analysis for 2000

Hank Nussbacher
hank@interall.co.il

Internet Society of Israel Conference
Tel Aviv, Israel, March 4, 2001

Preamble

- The word hacking is used to mean cracking systems
- Raw data: incident reports and Excel spreadsheet won't be made available so don't ask for it!
- Names listed in this presentation have not been changed so as to not protect the innocent

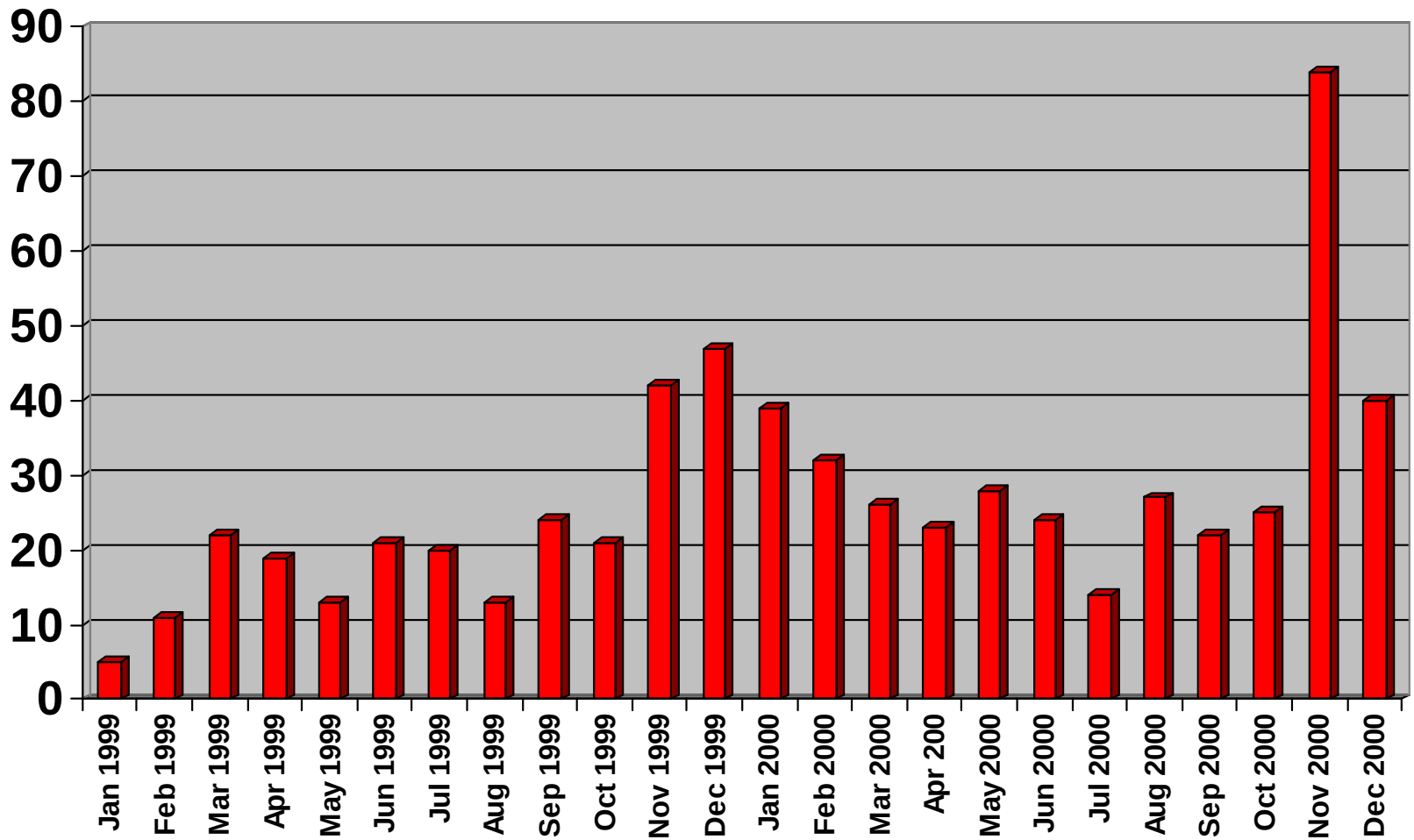
From where does the data come?

- My name registered on most Israeli IP blocks as contact - *hank@isoc.org.il*
  - 192.114.0.0/16, 192.115.0.0/16, 192.116.0.0/16, 192.117.0.0/16, 192.118.0.0/16
- Users report incidents to cert@cert.ac.il
  - Firewall logs, Jammer, BlackICE
- Users report incidents to contact name for .il domain
- My estimate is that only 50% of incidents reach me (other than for IBM -> AT&T)

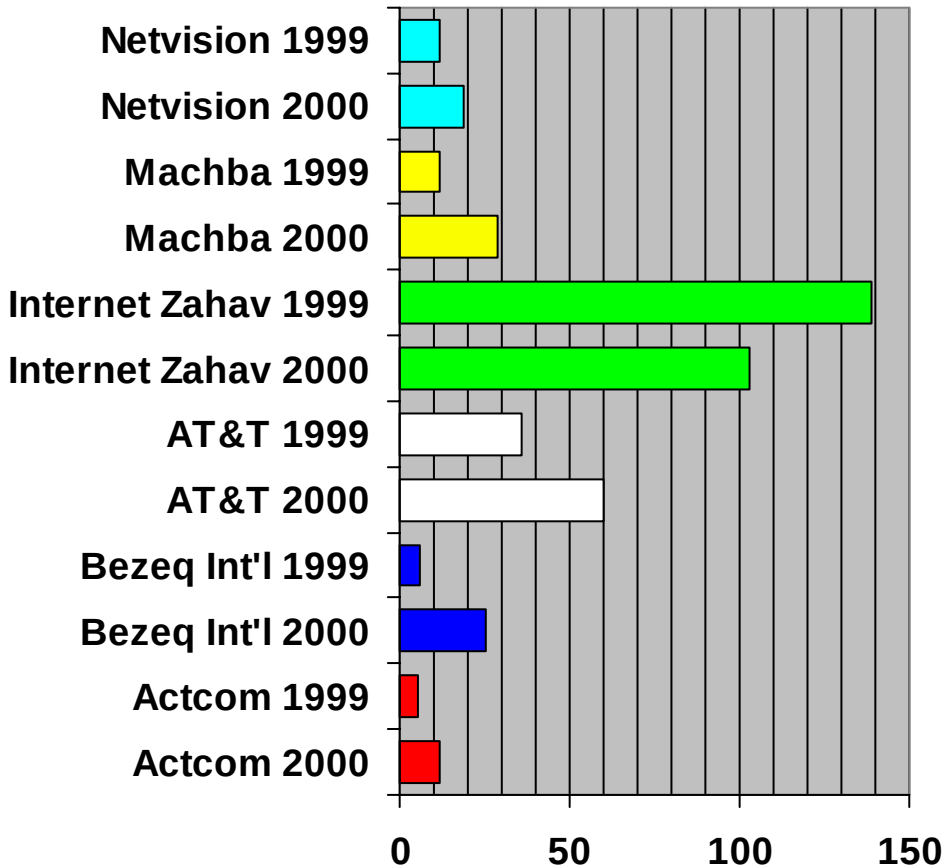
How many incidents reported?

- How many incidents reported?
  - 1999: 259 2000: 385
- How many incidents reported that involved Israelis hacking foreign sites?
  - 1999: 238 2000: 272
- How many incidents reported that involved foreigners hacking Israeli sites?
  - 1999: 10 2000: 99
- How many incidents reported that involved Israelis hacking Israeli sites?
  - 1999: 11 2000: 14

Monthly Distribution

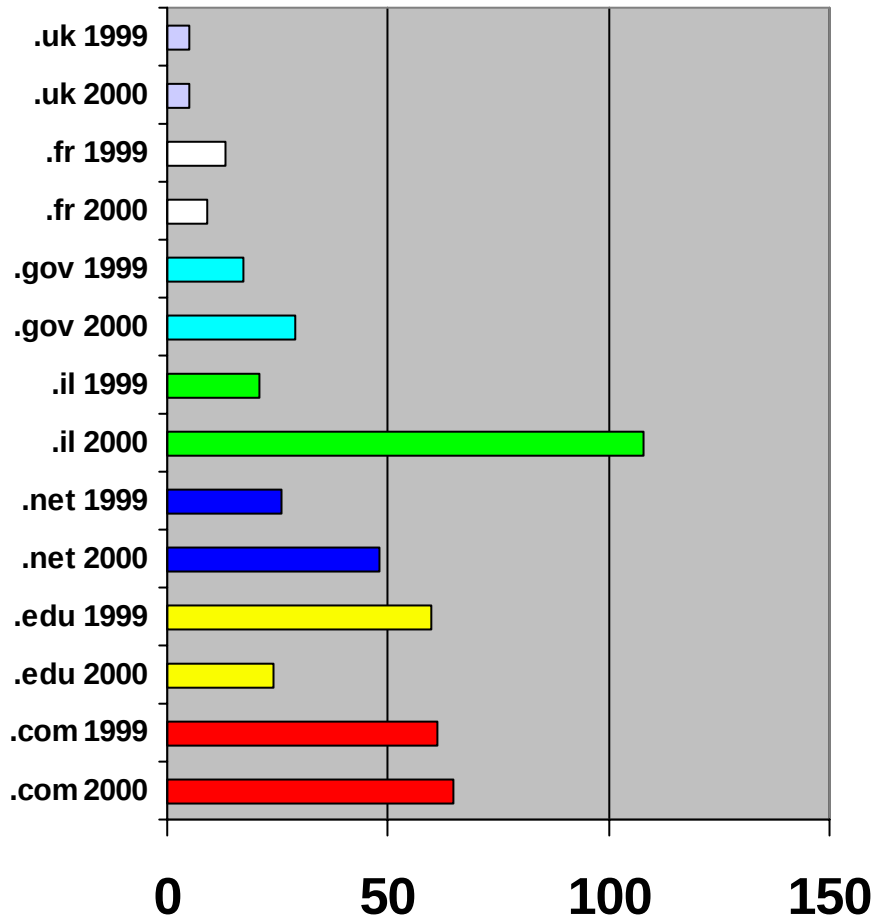


From which ISPs?



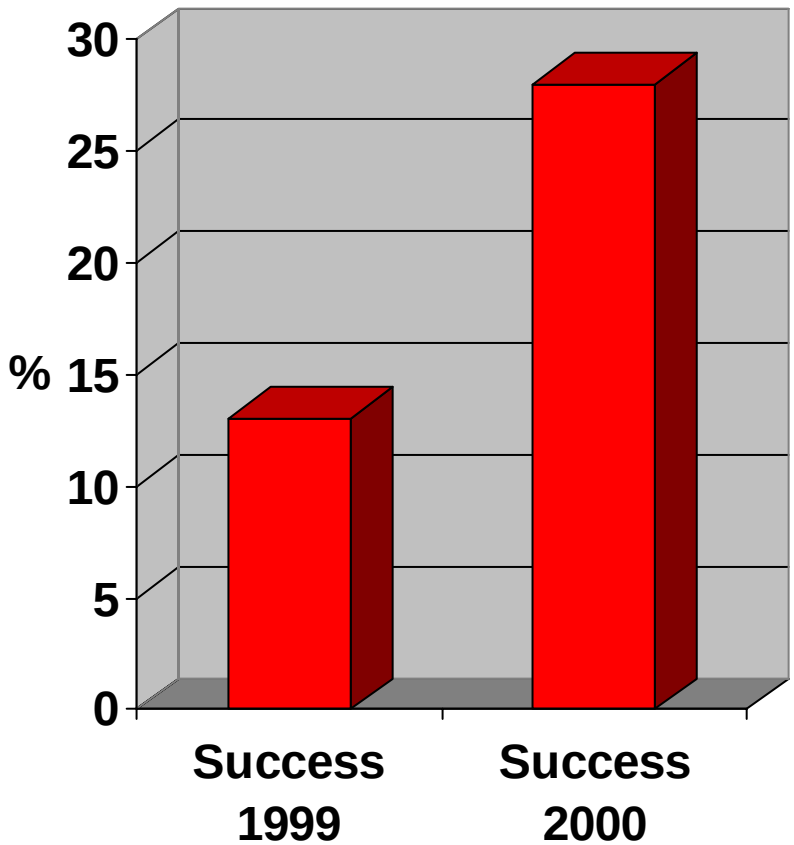
- Only those that had more than 10 incidents recorded
- AT&T has all incidents recorded - since I am recorded as contact for their IPs
  - the other ISPs are underrecorded

Which domains are being hacked



- **Most attacked sites:**
  - home.com (15)
  - llnl.gov (22)
  - ornl.gov (10)
  - cw.net (9)
  - renater.fr (8)
  - rr.com (7)
  - vt.edu (7)

Are the attacks successful?



- 13% of reported attacks in 1999 are successful
- 28% of reported attacks in 2000 are successful
  - most are site defacements
- Which ISP has the most successful hackers?
  - Internet Zahav

What were the most popular attacks in 1999?

- Port scans - 32%
- Telnet attempts - 11%
- Netbus and Back Orifice - 10%
- DoS - 8%
  - Smurf, Mail bombing, WinNuke, SYN flooding
- RPC attacks - 5%

What were the most popular attacks in 2000?

- Site defacements - 25%
  - only 2 out of 94 site defacements happened before Rosh HaShana
- Port scans - 21%
- Netbus, Sub-7, Hacka'Tack and Back Orifice - 17%
- FTP scans - 6%
- Telnet attempts - 5%
- DoS - 4%
  - Smurf, Mail bombing, WinNuke, SYN flooding

Site defacements

- First recorded site defacement - most.gov.il - April 23, 2000
- Second recorded site defacement - webgate.co.il - June 27, 2000
- Third recorded site defacement - tel-aviv.gov.il - Aug 29, 2000
- October 3 - start of massive site defacements

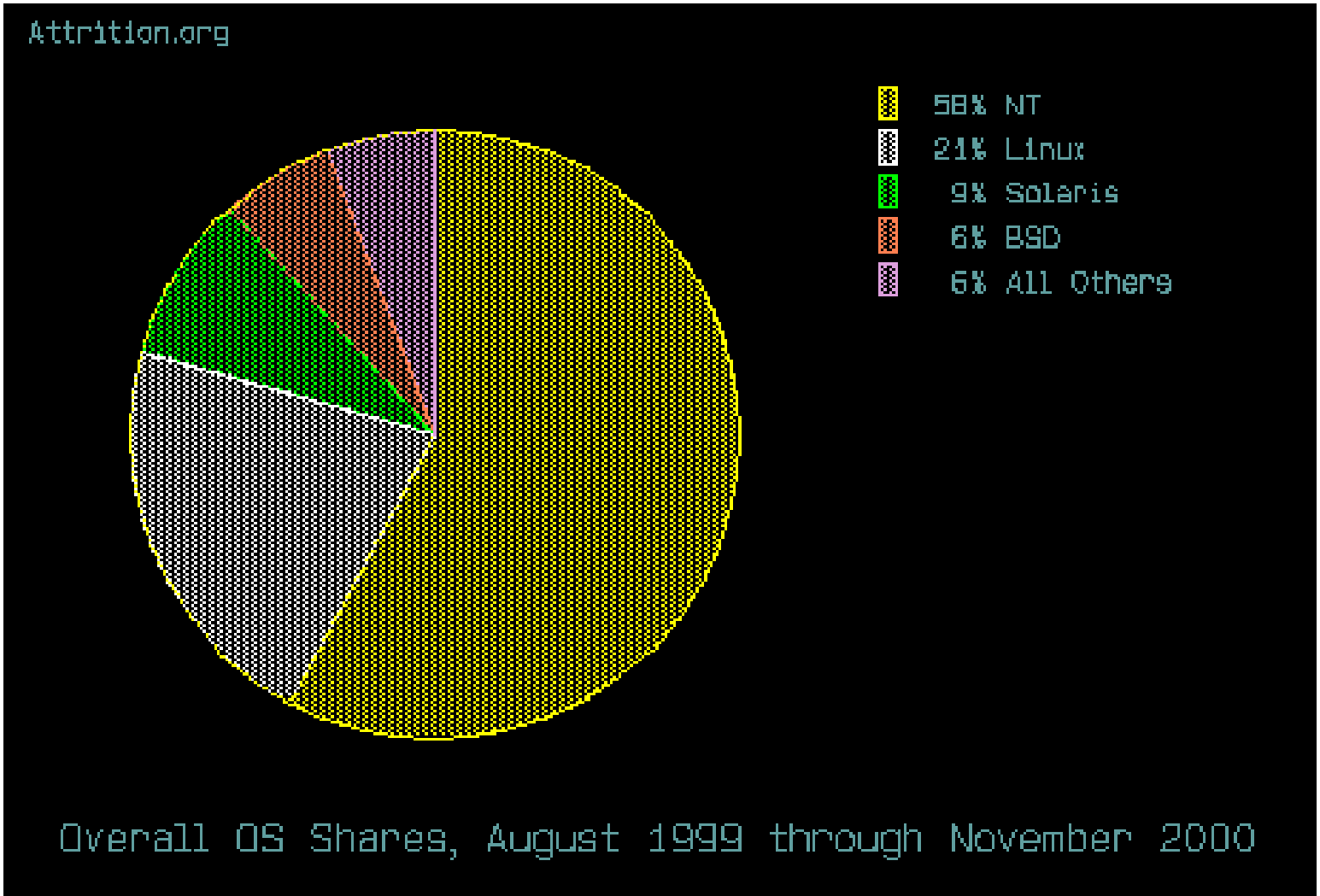
Site defacements - part II

- Last 3 months
  - 57 - co.il
  - 27 - ac.il
  - 4 - org.il
  - 1 - k12.il
  - 1 - gov.il
  - 1 - net.il
  - Total - 88 site defacements
- On December 29, 80+ sites defaced by Gforce Pakistan - #1 defacer group in the world

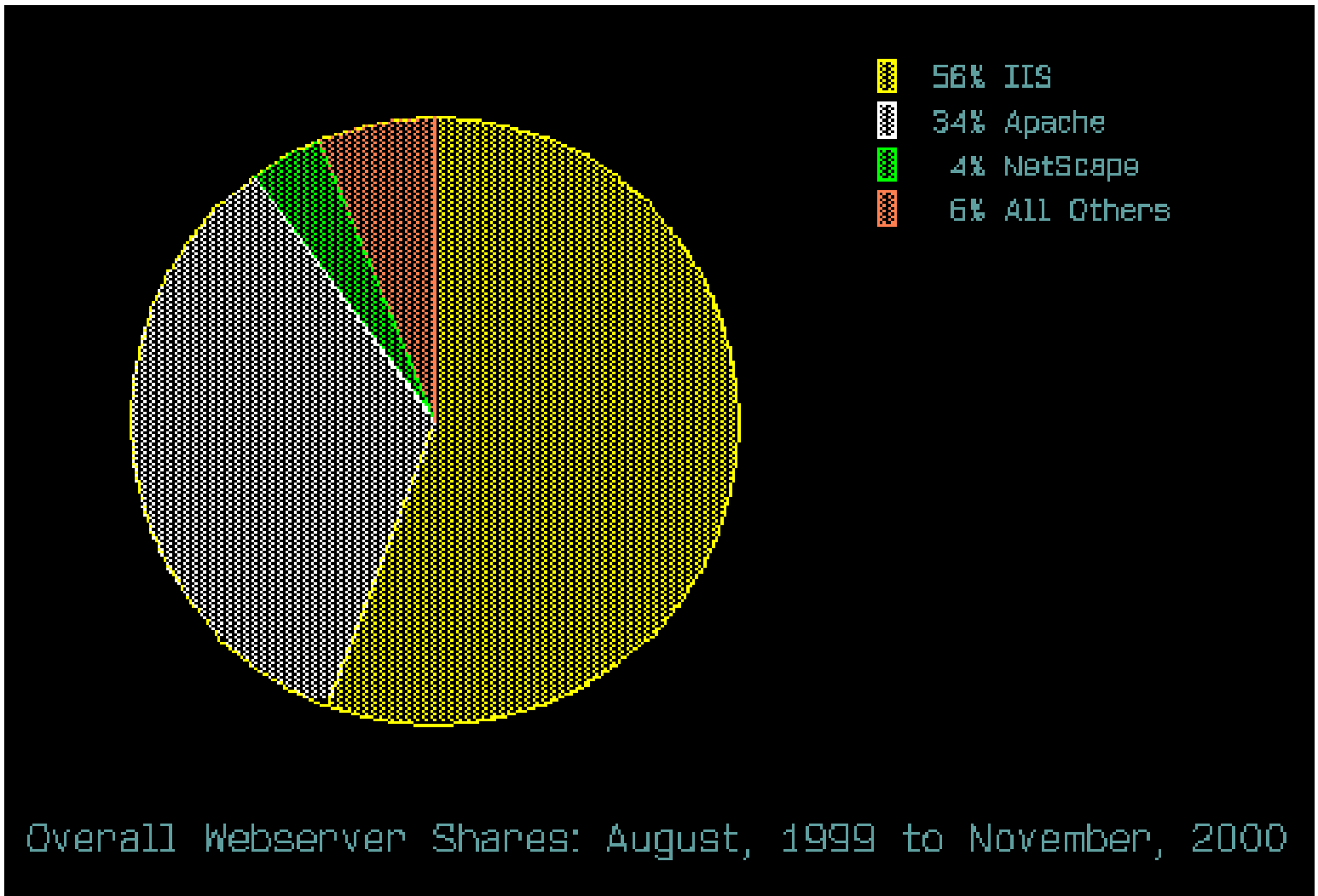
Site defacements - part III

- Many other countries with many more site defacements
  - Brazil - 683
  - UK - 234
  - Mexico - 207
- To see more details:
  - http://www.attrition.org/mirror/attrition/months.html

Site defacements - part IV



Site defacements - part V



Which IPs are the worst hackers?

- **192.115.216.131-159**
  - Jan 2 - Sept 30, 2000
  - 33 reported incidents
  - Netbus, BO, Sub-7 scans to mainly .com & .net
  - belongs to AT&T
- **192.116.226.252**
  - Jan 10 - July 5, 2000
  - 16 reported incidents
  - SNMP, ICMP, port scans to many .gov sites
  - belongs to Internet Zahav

Lessons learned

- **Israeli ISPs don't want to handle the problem**
  - **too much work and effort involved**
    - legal - lawyers don't understand hacking, courts give lenient sentences
    - police - overworked, lack of public interest
  - **too few skills to handle the problem**
    - Good security sysadmins earn over 20K NIS/month
  - **lose of revenue if customer leaves**
- **Survival of the fittest**
  - **Arab hackers doing us a favor in weeding out the sites with poor server security**