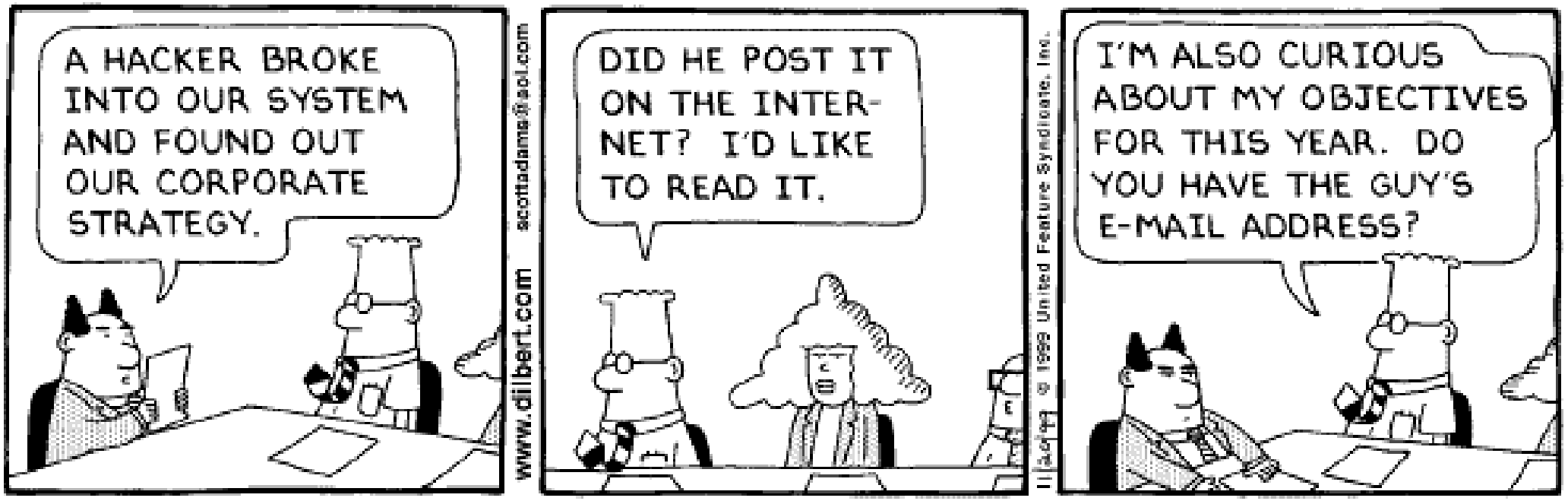
Israeli Internet Hacking Analysis for 1999

Hank Nussbacher
hank@interall.co.il

Internet Society of Israel Conference
Tel Aviv, Israel, February 16, 2000

Israeli Internet Hacking Analysis for 1999



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

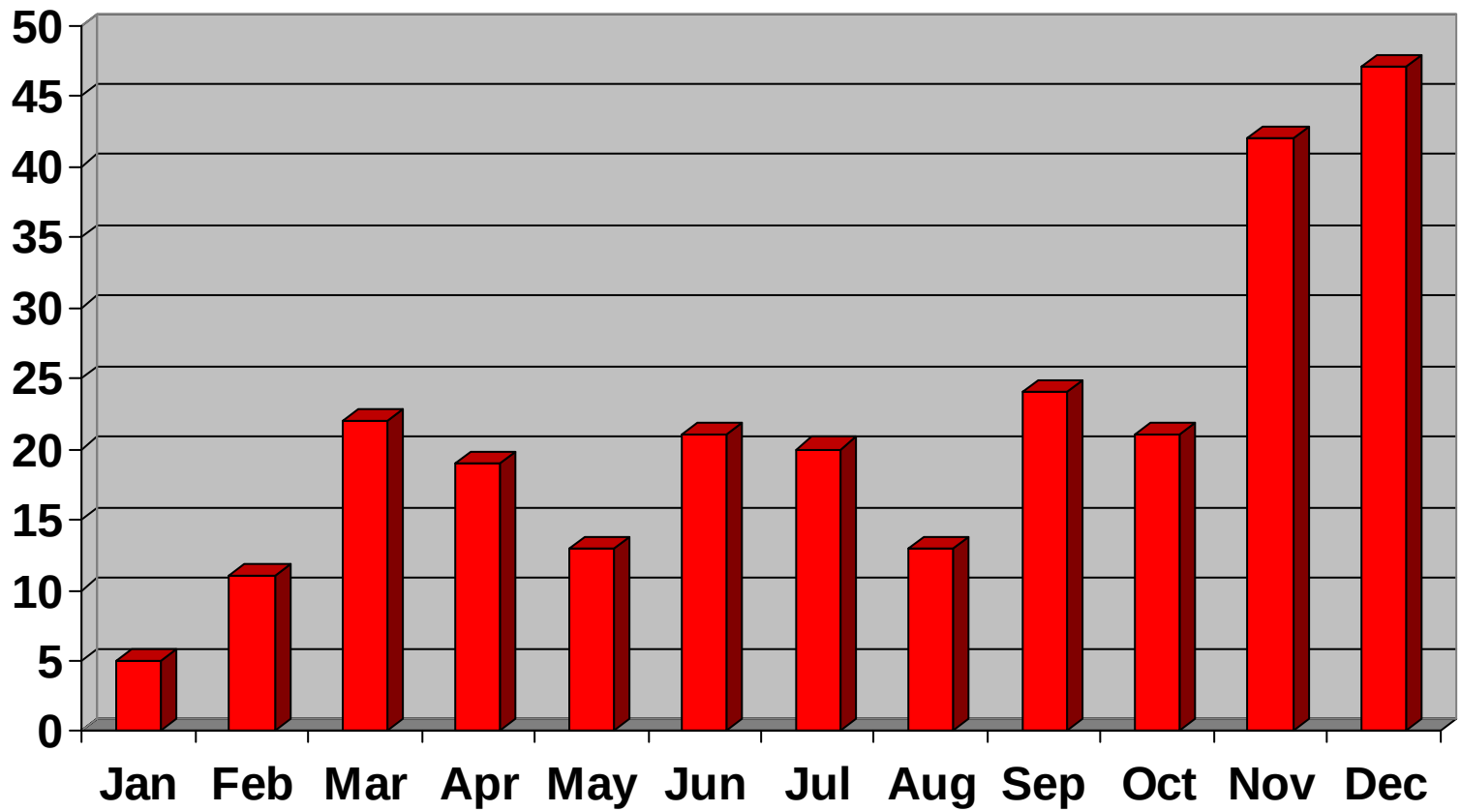
From where does the data come?

- 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)

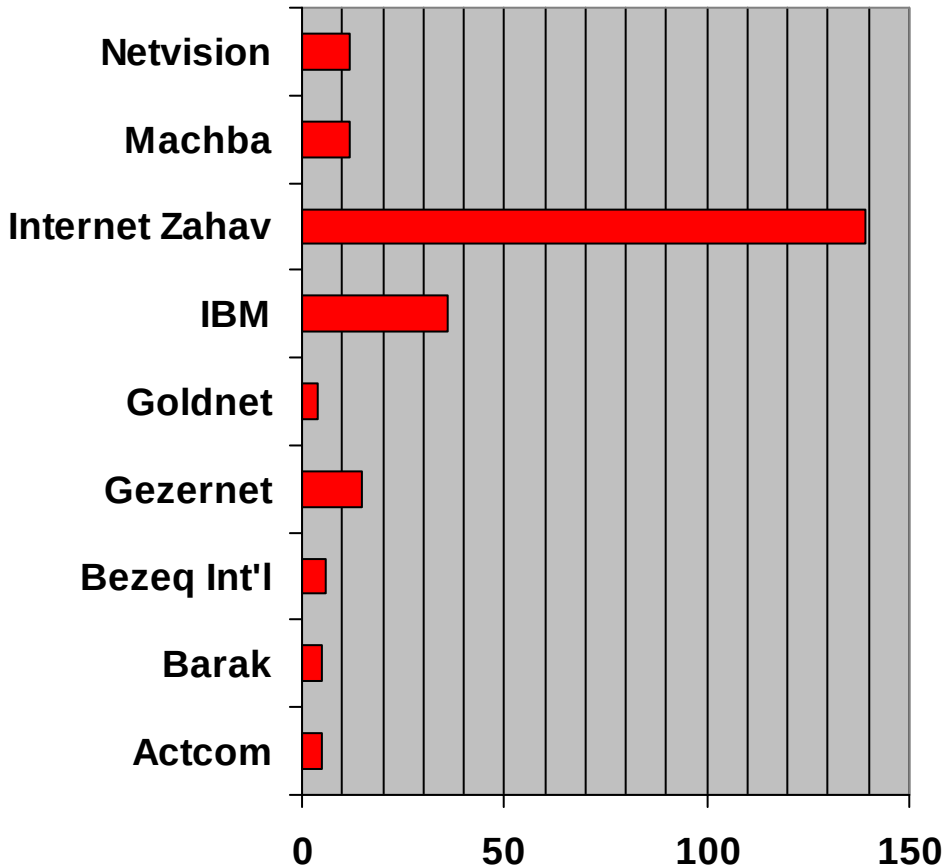
How many incidents reported?

- How many incidents reported?
  - 259
- How many incidents reported that involved Israelis hacking foreign sites?
  - 238
- How many incidents reported that involved foreigners hacking Israeli sites?
  - 10
- How many incidents reported that involved Israelis hacking Israeli sites?
  - 11

Monthly Distribution

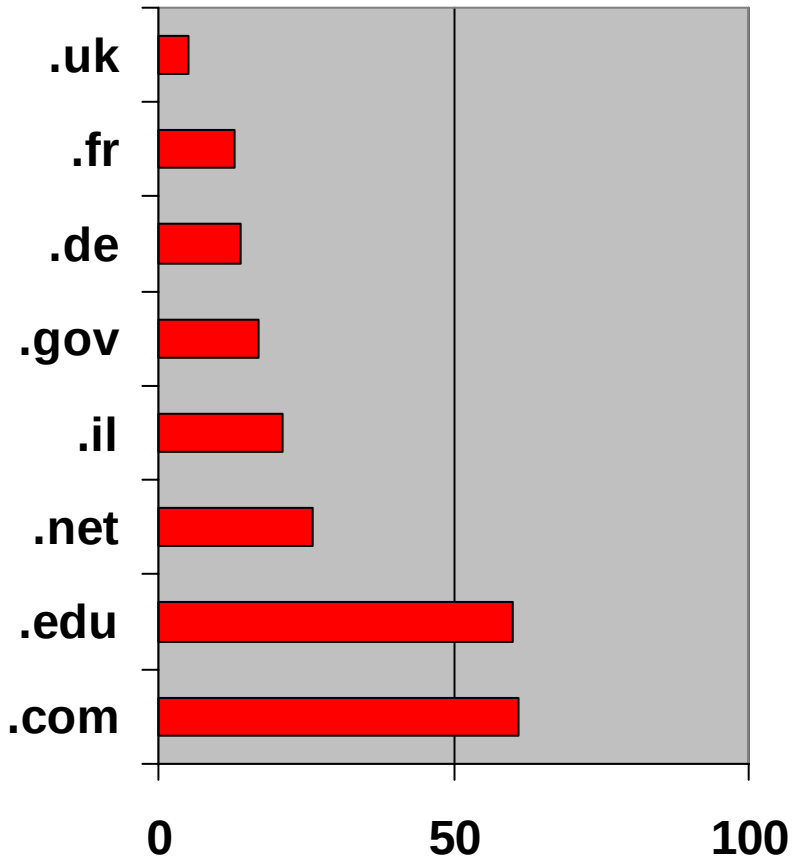


From which ISPs?



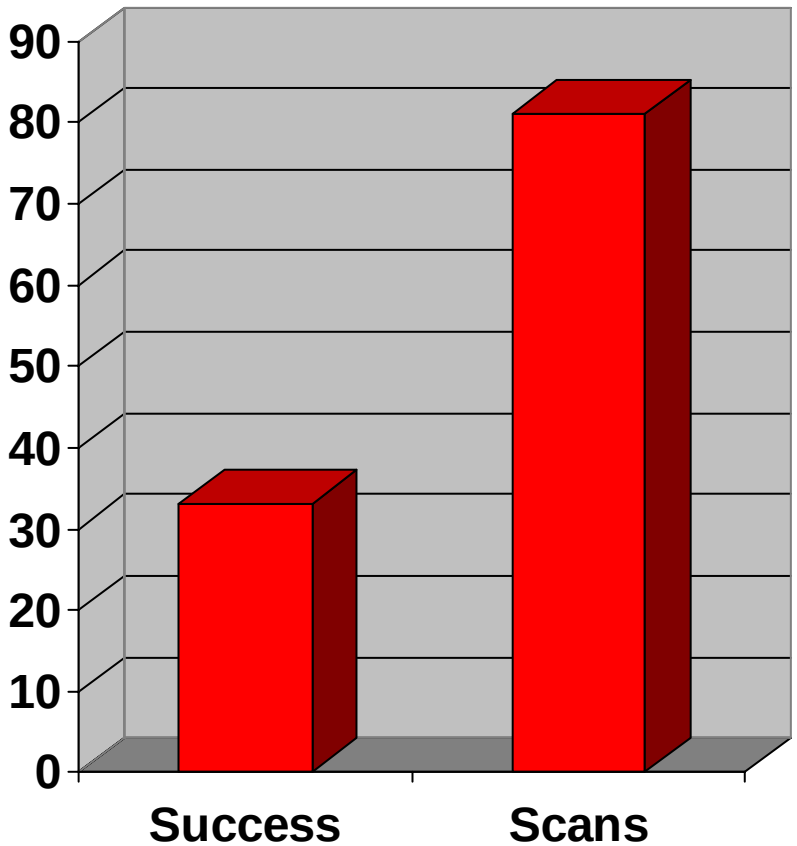
- Only those that had more than 5 incidents recorded
- IBM has all incidents recorded - since I am recorded as contact for their IPs
  - 19 in December
  - the other ISPs are underrecorded

Which domains are being hacked



- Most attacked sites:
  - balink.com (7)
  - llnl.gov (5)
  - mit.edu (4)
  - mminternet.com (4)
  - ornl.gov (5)
  - psu.edu (5)
  - rr.com (9) - all BO scans
  - ucsd.edu (4)
- .com - 18.7M hosts
- .edu - 5.1M hosts

Are the attacks successful?



- 32% of reported attacks are port scans
- 18% of reported attacks are successful
- Which ISP has the most successful hackers?
  - Internet Zahav

What are the most popular attacks?

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

Which IPs are the worst hackers?

- **192.114.163.214**
  - Nov 3 - Dec 17, 1999
  - 22 reported incidents
  - port scans to mainly .edu sites
  - belongs to Internet Zahav
- **192.115.4.198**
  - Nov 10 - Dec 10, 1999
  - 12 reported incidents
  - port scans to everyplace
  - belongs to Gezernet

Which IPs are the worst hackers?

- **192.115.206.2**
  - Sept 26 - Oct 23, 1999
  - 4 reported incidents
  - imap scans to European sites only
  - belongs to Netvision
- **192.117.178.200**
  - May 31 - Sept 12, 1999
  - 4 reported incidents
  - POP3 attacks and port scans to everyplace
  - belongs to Internet Zahav

Which IPs are the worst hackers?

- **192.115.216.129-157**
  - Mar 8 - Dec 26, 1999
  - 20 reported incidents
  - BO scans against .com sites
  - 2 successes (mit.edu and ibm.com)
  - belongs to AT&T (IBM)

Lessons learned

- **Academic sites more aware of hacking than commercial sites**
- **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**

Security is an illusion. Life is either a daring adventure or it is nothing at all

Helen Keller, 1957