A large-scale view of recent worm attacks

Sean Donelan
Affiliation not given for identification

Helping? Network users

- Education campaigns
- Free anti-virus software
- Free personal firewall software
- Port filters (port 80 anyone?)
- Notification of compromised systems
- Incident Response
- Intrusion Detection/Intrusion Prevention
- Managed Security Services

Chronology of recent Worms

Jul 16 – Microsoft Security Bulletin MS03-026

Jul 17 – CERT/CC advisory CA-2003-16

Jul 24 – Department of Homeland Security advisory

Jul 25 – Increase in TCP/135 scans reported by ISP

Several universities report compromised computers

Jul 30 – DHS issues second advisory

Jul 31 – CERT/CC issues second advisory

Extensive news coverage in trade and general press

Chronology of recent Worms

Aug 11 – BLASTER worm appears on Internet

- Microsoft 2-hour hold times on toll-free number
- Microsoft assisted 40,000 customers

Aug 16 – Scheduled DDOS attack on windowsupdate.com

- Microsoft drops “A” records from DNS

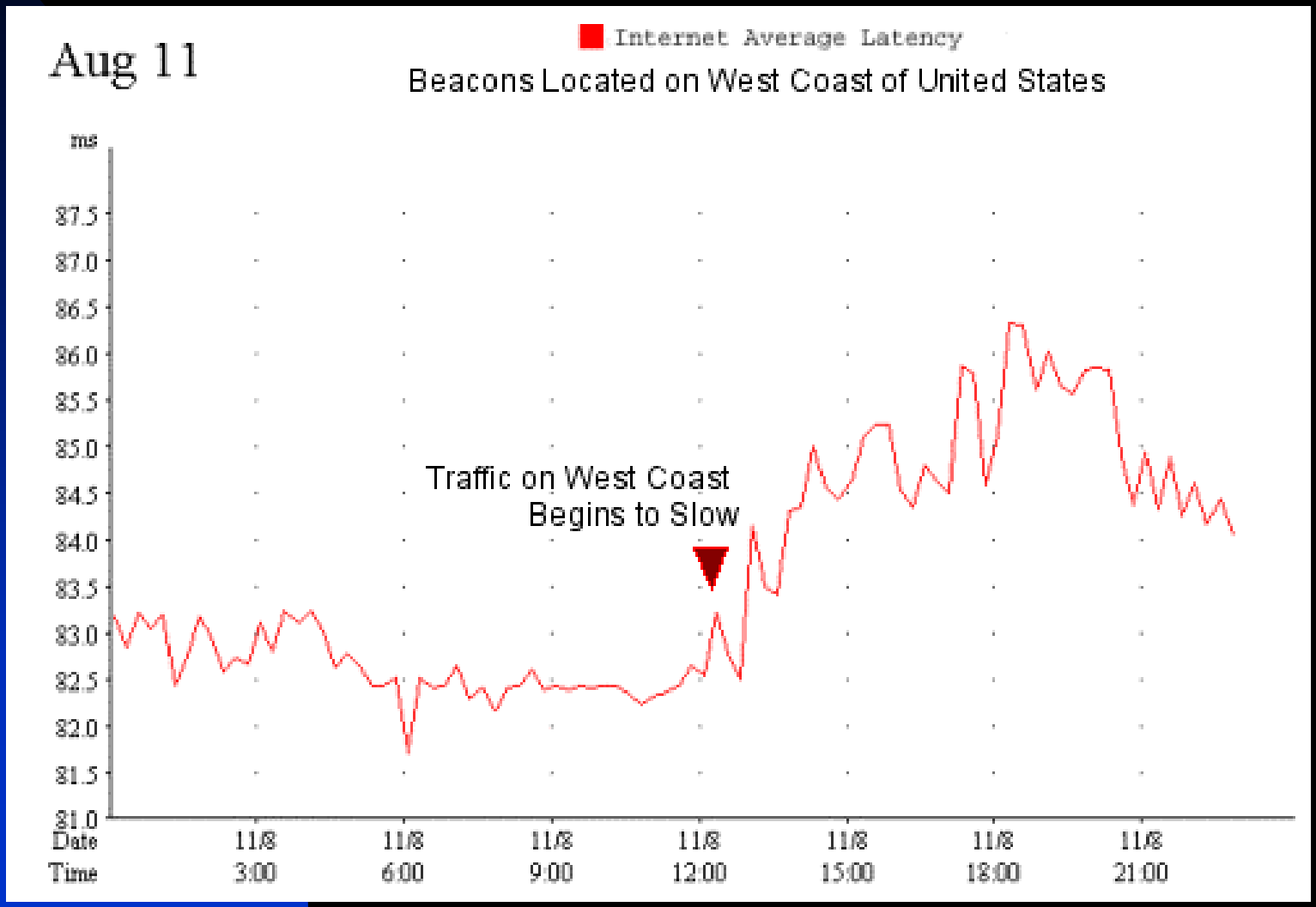
Aug 18 – Nachi/Welchia worm appears on Internet

Aug (18) 19 – Sobig.F e-mail virus appears on Internet

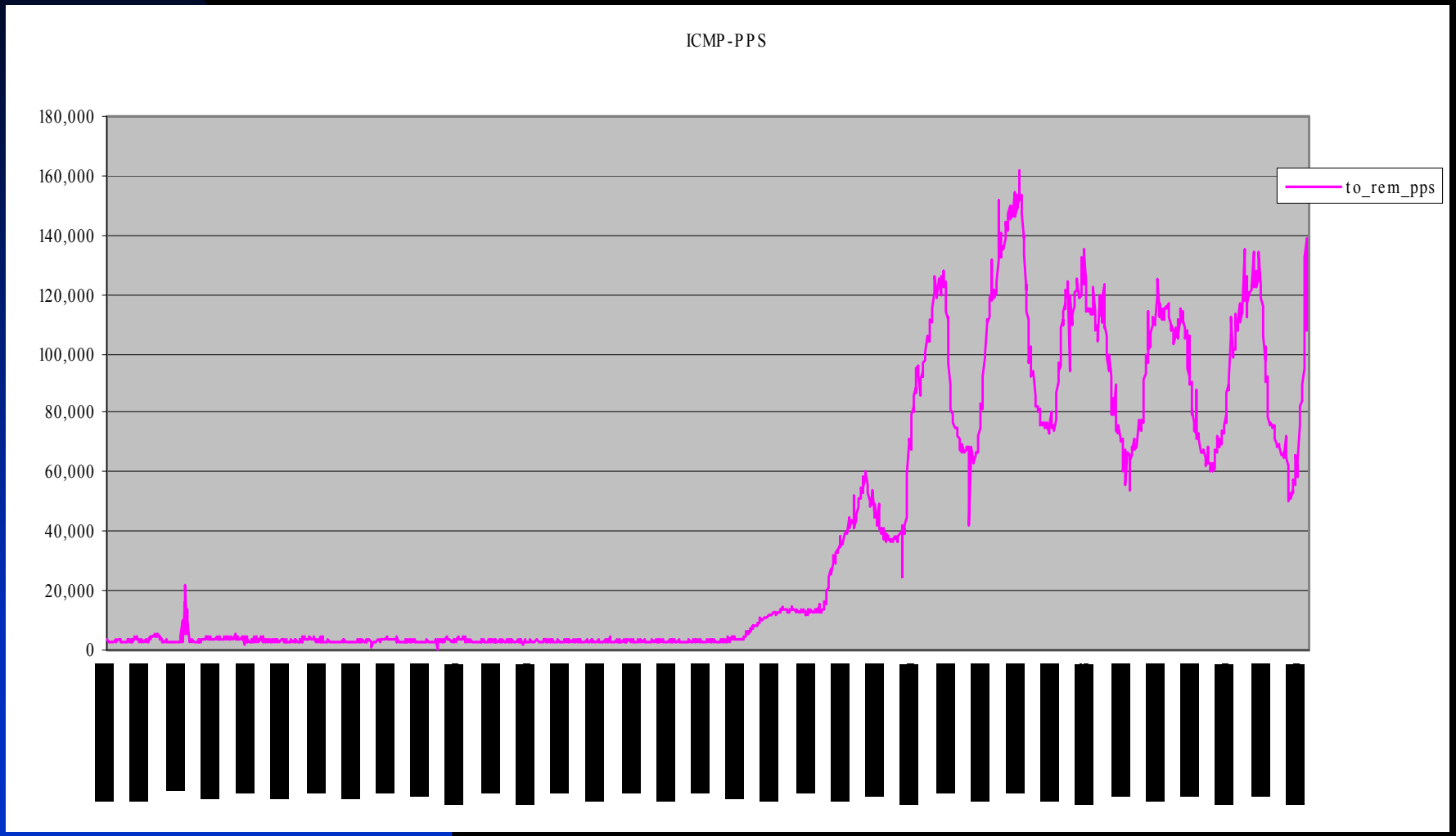
Sep 10 – Microsoft Security Bulletin MS03-039

Sep 18 – Swen e-mail virus masquerades as Microsoft security patch

Blaster Impact on Internet



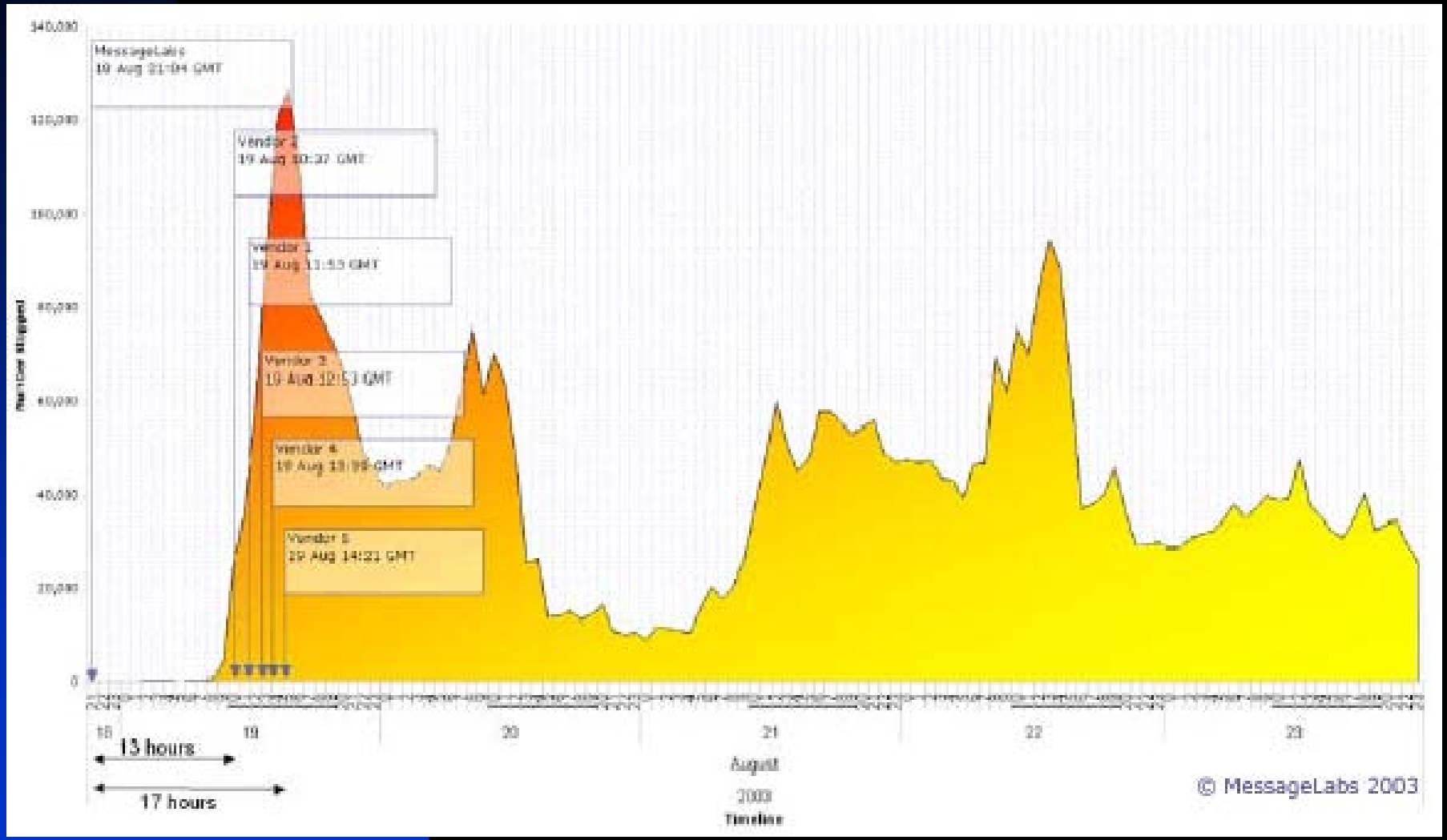
Nachi RPC worm (Edge Effect)



Why Nachi acted different

- Not all networks were equally affected
  - Network “telescopes” wouldn’t see many infections
- Target “Class B” /16 (65,535) network of host
- Target 3 adjacent /16 networks of host
  - Special Use Addresses adjacent to networks
  - 169.254/16, 10/8, 172.16/12, 192.168/16
- Target /16 network from hard-coded list of 76 networks in China (asia-pacific?)
- Target /16 network selected from the following /8 ranges: 60 to 66, 128 to 172, 192 to 200, 202, 203, 210, 211, 218, 219, 220

Sobig.F mail virus



Fixing Problems

- Patching follows a half-life decay (40% rule)
- Calling, email, press coverage has little effect on end-user repair behavior
  - Enterprise advantage: IT tech fixing the computer
  - Doing nothing has the same impact
- Elephants and Mice
  - Large organizations versus home users
- Connecting vulnerable computers to the network to download patches is a security risk
- 95/5 Rule?
  - Never reaches Zero
  - Morris worm compromised 10% of the ARPANET

Next Steps

- ????