DoS Attacks

..by Sree Santhosh

OUTLINE

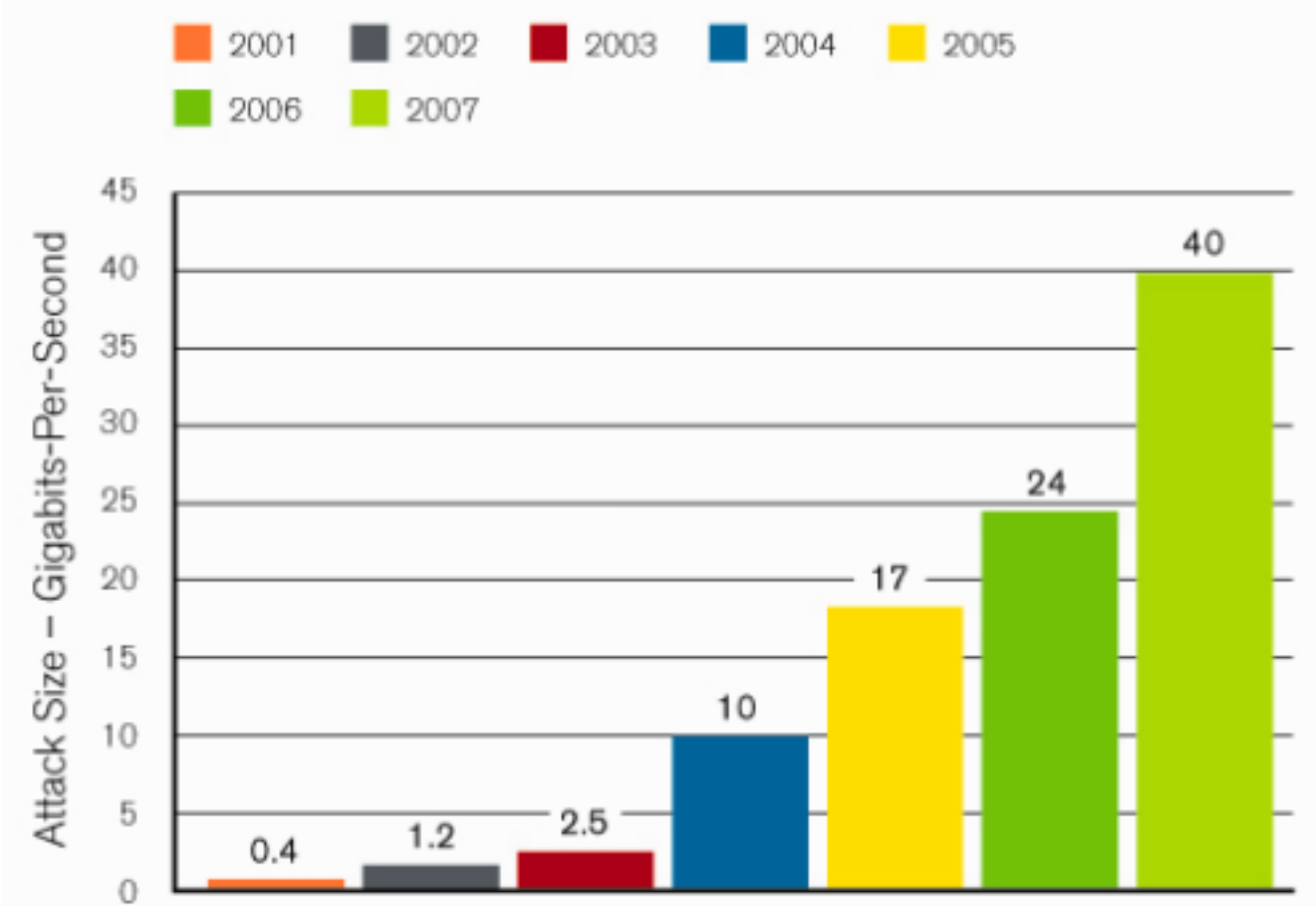
- “DoS Attacks” – What Is
- History
- Types of Attacks
- Main targets today
- How to Defend
- Prosecution
- Conclusion

WHAT IS “DOS ATTACK”

Denial-Of-Service Attack = DOS Attack is a malicious attempt by a single person or a group of people to cause the victim, site or node to deny service to it customers.

- DoS = when a single host attacks
- DDoS = when multiple hosts attack simultaneously

ATTACK SIZE IN GBITS-PER-SECOND



ATTACK SIZE IN GBITS-PER-SECOND

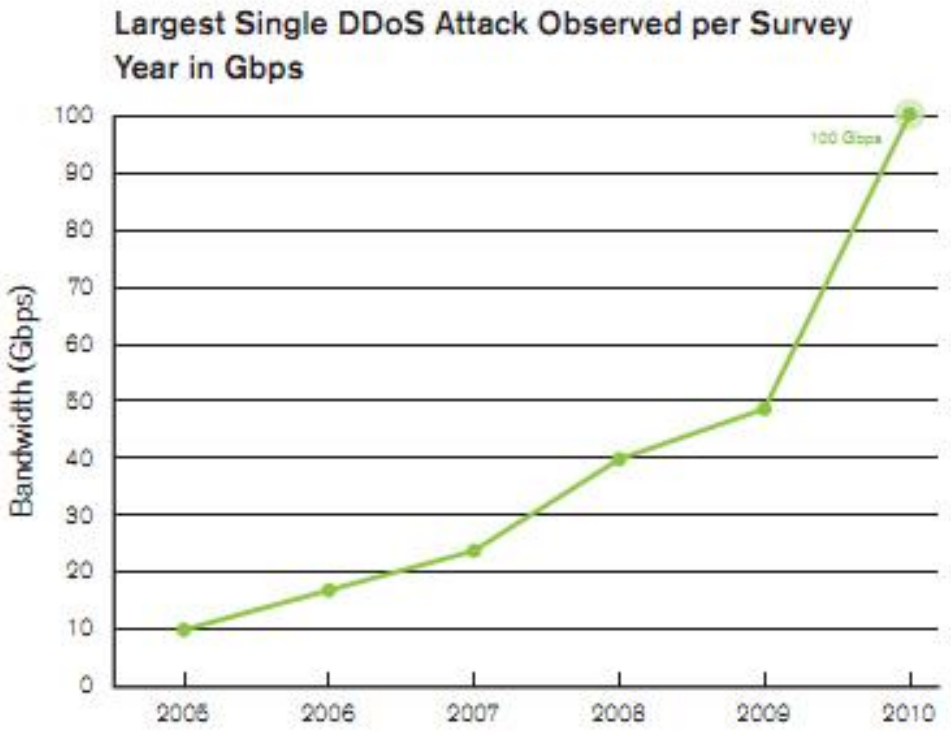


Figure 1
Source: Arbor Networks, Inc.

IDEA OF “DOS ATTACKS”

- Purpose is to shut down a site, not penetrate it.
- Purpose may be vandalism, extortion or social action (including terrorism) (Sports betting sites often extorted)
- Modification of internal data, change of programs (Includes defacement of web sites)

HISTORY

Morris Worm (November 2, 1988)

- First DDoS attack to cripple large amounts of network infrastructure
- Self-replicating, self-propagating.
- Exploited software commonality (monoculture)

1. Fingerd buffer overflow exploit
2. Sendmail root vulnerability
3. Weak passwords

HISTORY

Morris Worm effect

- Infected systems became “catatonic”
- Took roughly three days to come under control
- Ultimately infected 10% of Internet computers (6,000) and cost $ million to clean up.
- Morris convicted under computer fraud and abuse act, three years probation, fine of $10,000

HISTORY

SQL Slammer (January, 25 2003)

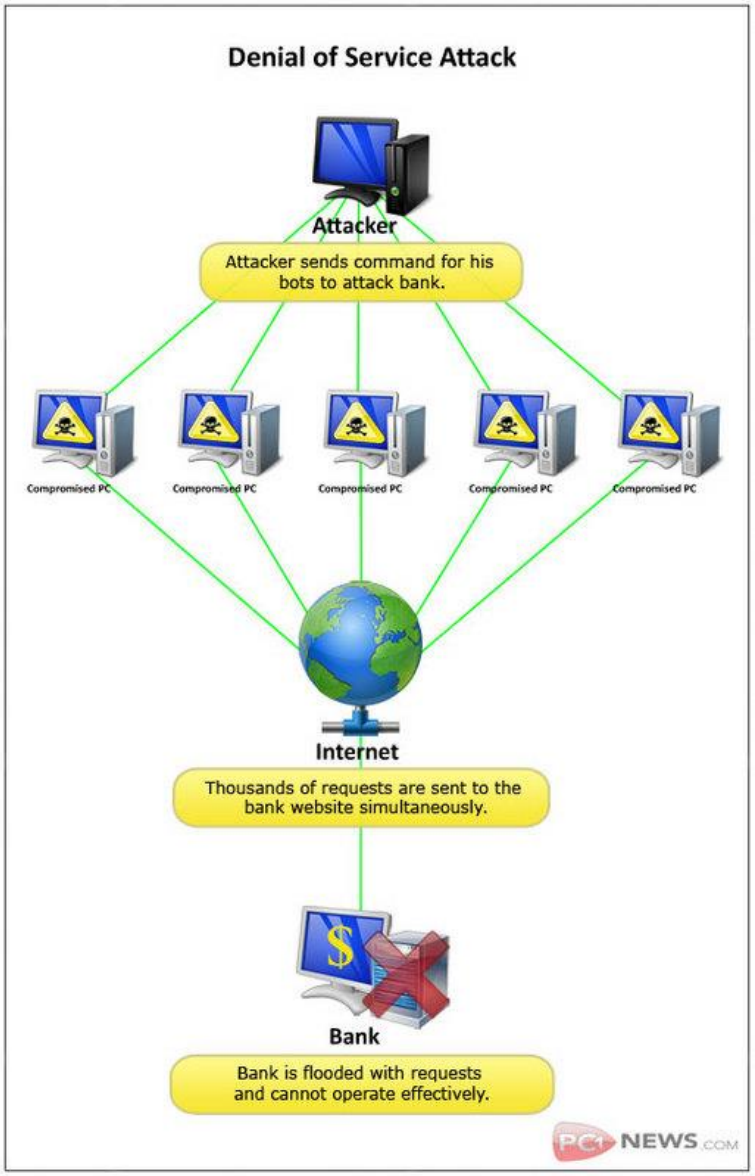
- Exploited common software (Microsoft SQL Server) as well as hardware (Intel x86), spread rapidly in a distinct monoculture.
- Non-destructive. Modified no data on infected system
- Extremely simple in construction (376 bytes)
- Devastating:
  1. 120,000 computers infected at peak (1/26/2003)
  2. Exhausted network bandwidth
  3. Crashed network infrastructure (multicast state creation)
  4. Shut down communication (fire-fighting) capability

HISTORY

SQL Slammer effect

- Extremely Virulent
- Caused economic damage outside of IT infrastructure (multiple ATM outages)
- Original perpetrators have never been identified or brought to justice

TYPES OF DOS ATTACKS



TYPES OF DOS ATTACKS

- Penetration
- Eavesdropping
- Man-In-The-Middle
- Flooding

TYPES OF DOS ATTACKS

Penetration

- Attacker gets inside your machine
- Can take over machine and do whatever he wants
- Achieves entry via software flaw(s), stolen passwords or insider access

TYPES OF DOS ATTACKS

Eavesdropping

- Attacker gains access to same network
- Listens to traffic going in and out of your machine

TYPES OF DOS ATTACKS

Man-in-the-Middle

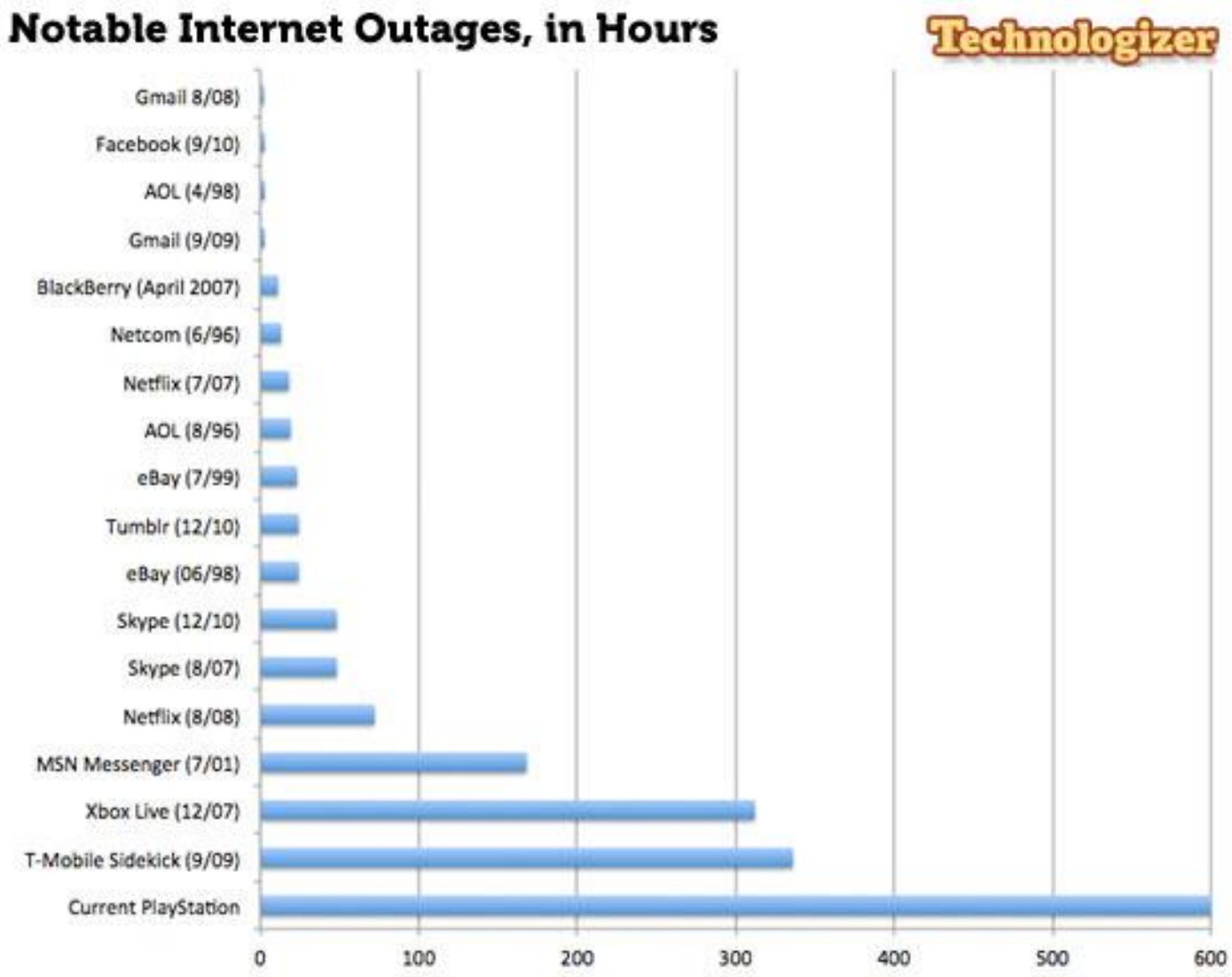
- Attacker listens to output and controls output
- Can substitute messages in both directions

TYPES OF DOS ATTACKS

Flooding

- In a flood attack, attackers send a very high volume of traffic to a system so that it cannot examine and allow permitted network traffic. For example, an ICMP flood attack occurs when a system receives too many ICMP ping commands and must use all its resources to send reply commands.

MAIN TARGETS



ESTONIAN CYBERWAR APRIL 27, 2007

- Weeks of cyber attacks followed, targeting government and banks, ministries, newspapers and broadcasters Web sites of Estonia.
- Some attacks took the form of distributed denial of service (DDoS) attacks (using ping floods to expensive rentals of botnets).
- 128 unique DDOS attacks (115 ICMP floods, 4 TCP SYN floods and 9 generic traffic floods).
- Used hundreds or thousands of "zombie" computers and pelted Estonian Web sites with thousands of requests a second, boosting traffic far beyond normal levels.

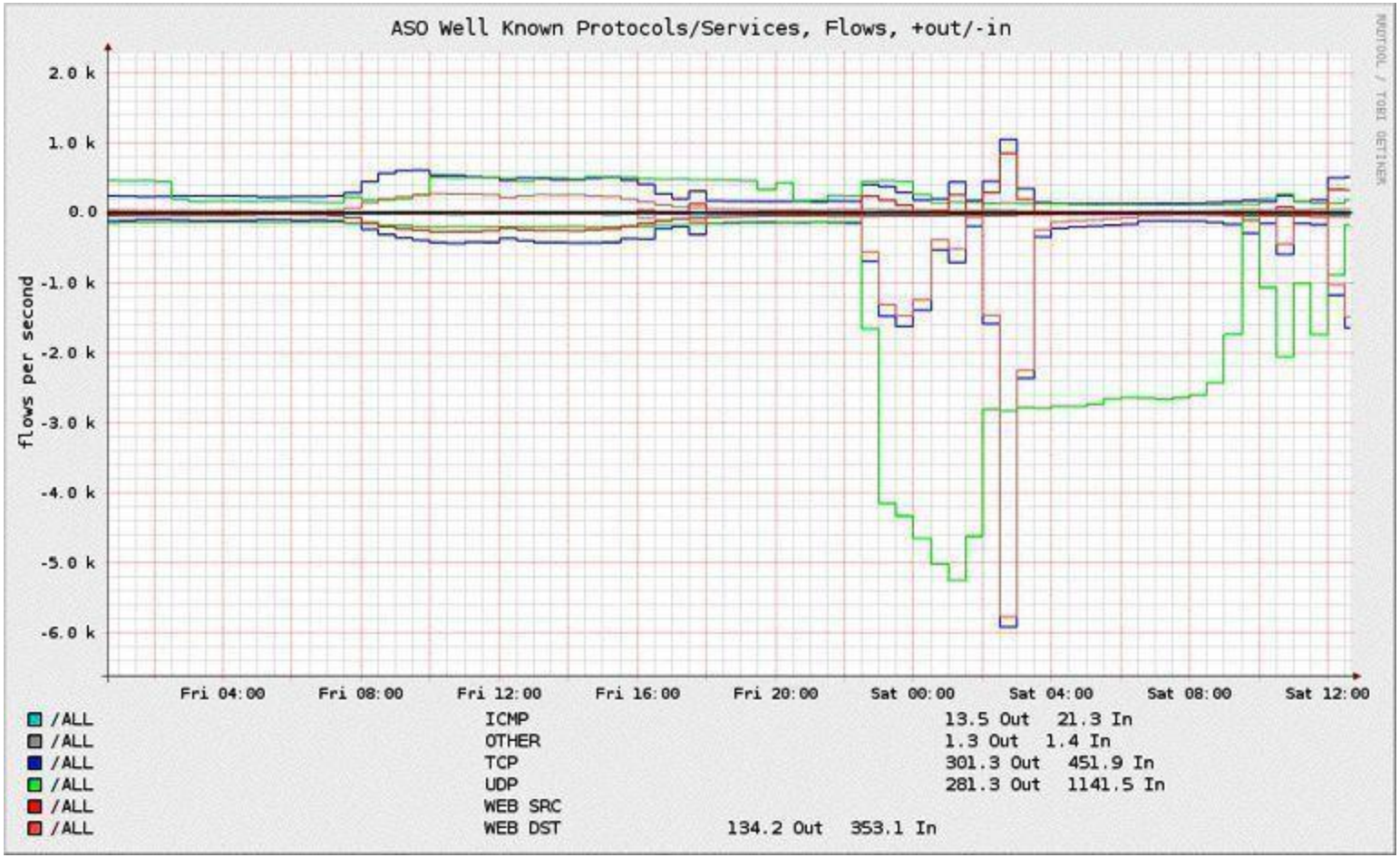
ESTONIAN CYBERWAR APRIL 27, 2007

- Inoperability of the following state and commercial sites:
  - The Estonian presidency and its parliament.
  - Almost all of the country's government ministries.
  - Political parties.
  - Three news organizations.
  - Two biggest banks and communication's firms.
  - Governmental ISP.
  - Telecom companies.

ESTONIAN CYBERWAR APRIL 27, 2007

- The attack heavily affected infrastructures of all network:
  - Routers damaged.
  - Routing tables changed.
  - DNS servers overloaded.
  - Email servers mainframes failure, and etc.

ESTONIAN CYBERWAR APRIL 27, 2007



HOW TO DEFEND

- Firewalls - can effectively prevent users from launching simple flooding type attacks from machines behind the firewall.
- Switches - Some switches provide automatic and/or system-wide rate limiting, traffic shaping, delayed binding to detect and remediate denial of service attacks
- Routers - If you add rules to take flow statistics out of the router during the DoS attacks, they further slow down and complicate the matter
- DDS based defense
- Clean pipes

PROSECUTION

- Different governmental legislation
- Too expensive
- National interests
- Hard to prove who used the computer

CONCLUSION

- ✓ Denial of Service is currently the most expensive computer crime for victim organizations.
- ✓ Strategic firewall placement allows companies to use the Internet during a DDoS attack, and it allows them to continue receiving the packets they want.
- ✓ Distributed Denial of Service Attacks could be Detected by Monitoring the Source IP.
- ✓ It is easy to generate a successful DDoS attack that bypasses these defenses.

Thank you