Denial of Service (DoS) Technical Primer

Chris McNab

Principal Consultant, Matta Security Limited

chris.mcnab@trustmatta.com

Topics Covered

- What is Denial of Service?
- Categories and types of Denial of Service attacks
  - Direct Denial of Service attacks
    - Single-tier attacks
    - Dual-tier attacks
    - Triple-tier 'distributed' attacks
  - Indirect Denial of Service attacks
    - The LoveBug virus
    - Code Red and Nimda worms
- Denial of Service prevention strategies and resources

What is Denial of Service?

Denial of Service (refered to as DoS for the remainder of this presentation), is a computer or network state which is induced purposefully by an attacker to inhibit that computer or network's ability to function correctly and provide service.

DoS attacks are launched on the Internet landscape in network form, where the attacking computer sends crafted network packets (TCP, UDP or ICMP) to the target host.

The Underlying DoS Concept

As with any form of 'hack attack', a vulnerability is exploited so that the attacker can change the operating state of a machine. Early Microsoft Windows 95 machines were vulnerable to 'winnuke' and 'ping of death' attacks, where the TCP/IP stack implemented by Microsoft was simple and could not handle large fragmented packets or out-of-bound data correctly. Hackers wrote simple programs that sent crafted out-of-bound and fragmented packets to the target IP address, causing it to crash and display the infamous 'blue screen of death'.

Other attack types take advantage of vulnerabilities at network level with the way that the Internet sends data between networks and responds to certain data.

.

Direct and Indirect DoS

Internet-based network attacks can be categorised in two ways..

- Direct DoS attack model, where a specific DoS system is developed and rolled out by an attacker with an aim to take down a specific network or computer.
- Indirect DoS attack model, where a worm or virus is at large in the wild, which causes DoS and disruption as a result of its spreading.

Direct DoS Attack Systems

Over the years, direct DoS attack systems have improved -

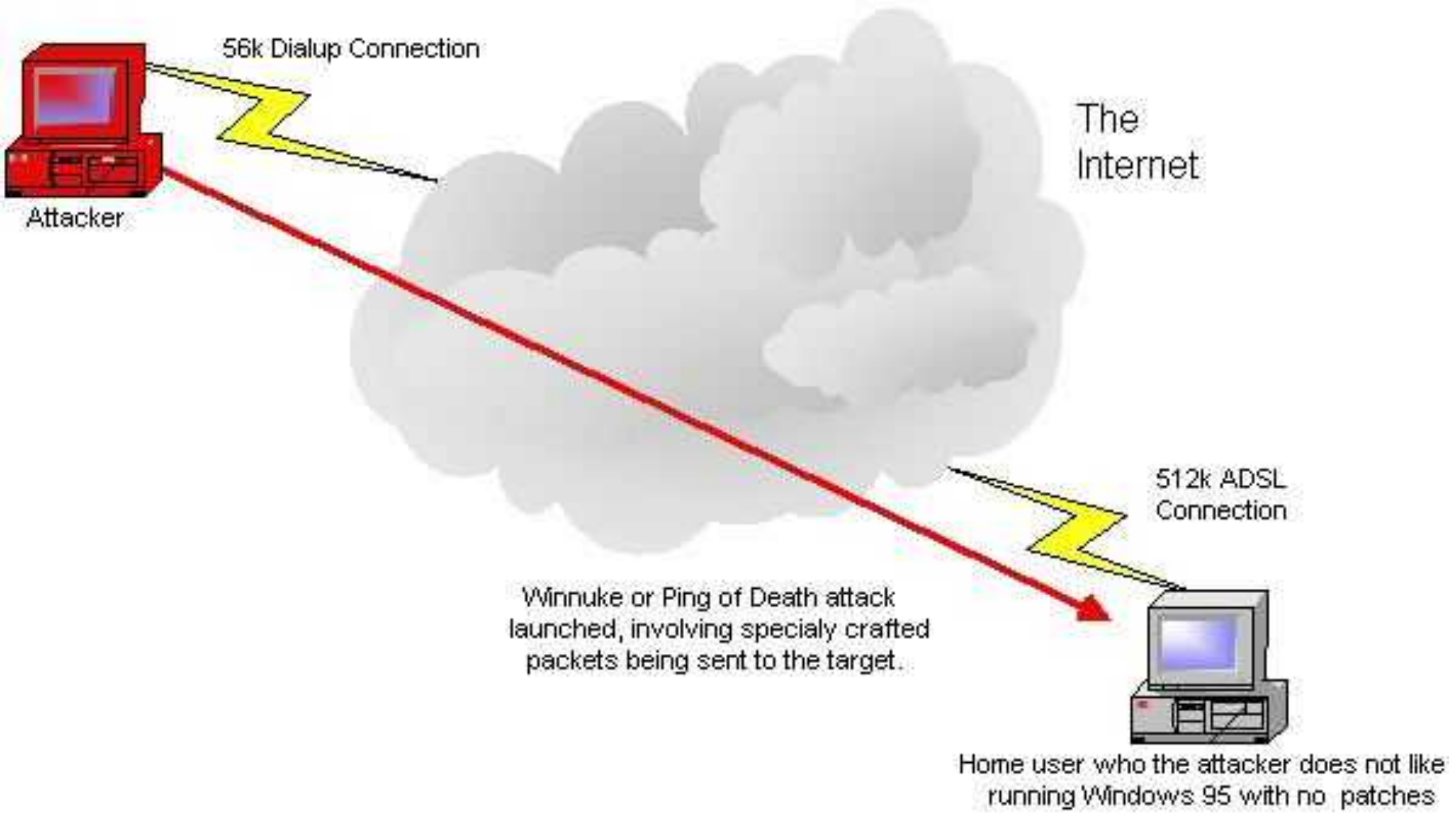
- 1990 - 1997 single-tier DoS attack systems
- late 1997 dual-tier DoS attack systems
- 1998 – 2000 triple-tier DoS attack systems

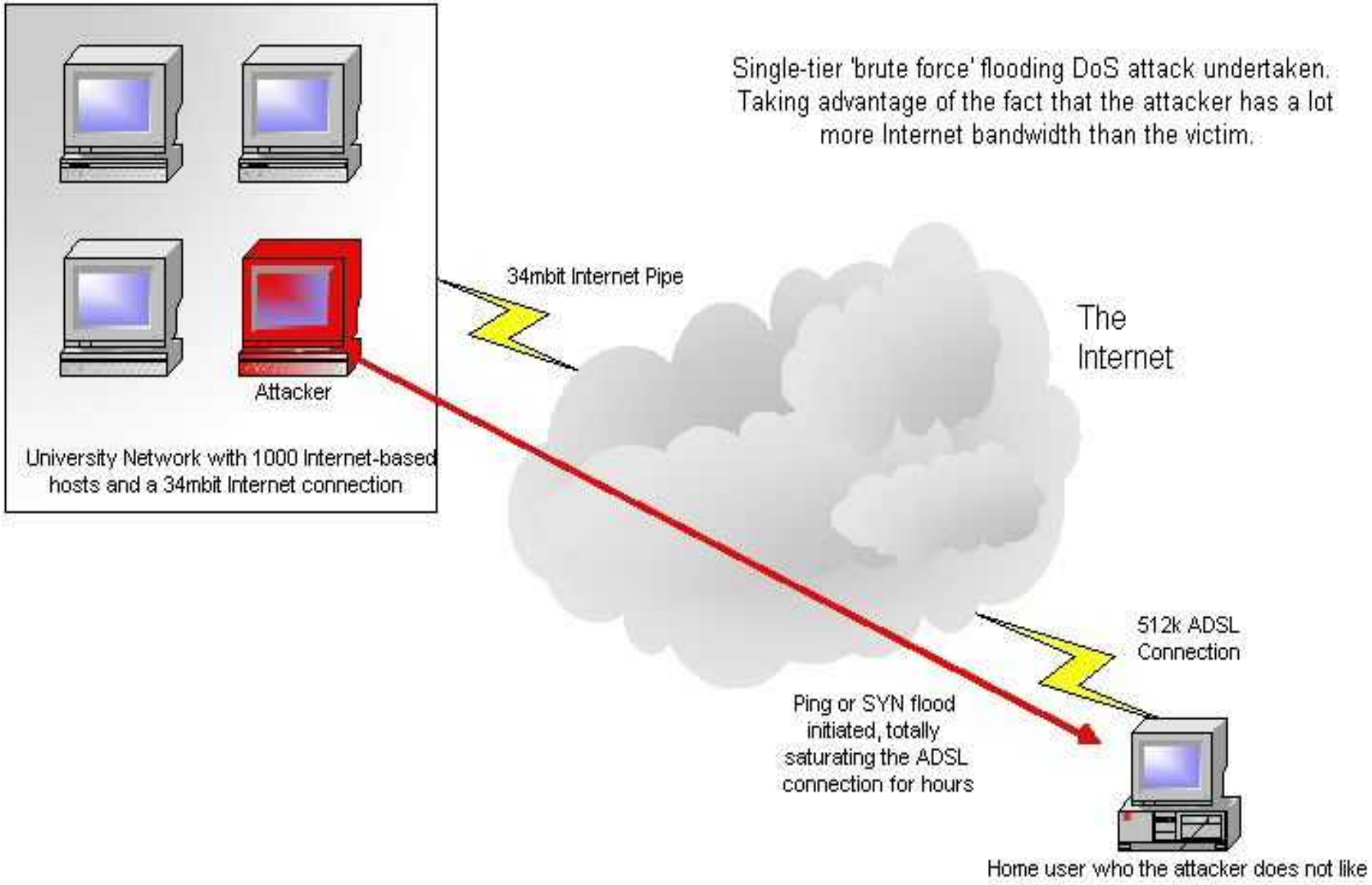
An interesting fact is that All direct DoS attack systems originate and were developed by users of Internet Relay Chat (IRC) networks, in some cases to specifically take down IRC servers (with dual & triple-tier attacks).

Direct Single-tier DoS Attacks

- Straightforward 'point-to-point' attack
- Application / system level vulnerabilities abused
- If no application / system level vulnerabilities exist, brute force is used by attackers with more bandwidth than the victim
- Examples
  - Ping of Death
  - SYN floods
  - Other malformed packet attacks

Single-tier system level DoS attack undertaken. Taking advantage of the fact that the victim is running a vulnerable Operating System and has not applied security patches




Single-tier 'brute force' flooding DoS attack undertaken. Taking advantage of the fact that the attacker has a lot more Internet bandwidth than the victim.
34mbit Internet Pipe
The Internet
Attacker
University Network with 1000 Internet-based hosts and a 34mbit Internet connection
512k ADSL Connection
Ping or SYN flood initiated, totally saturating the ADSL connection for hours
Home user who the attacker does not like

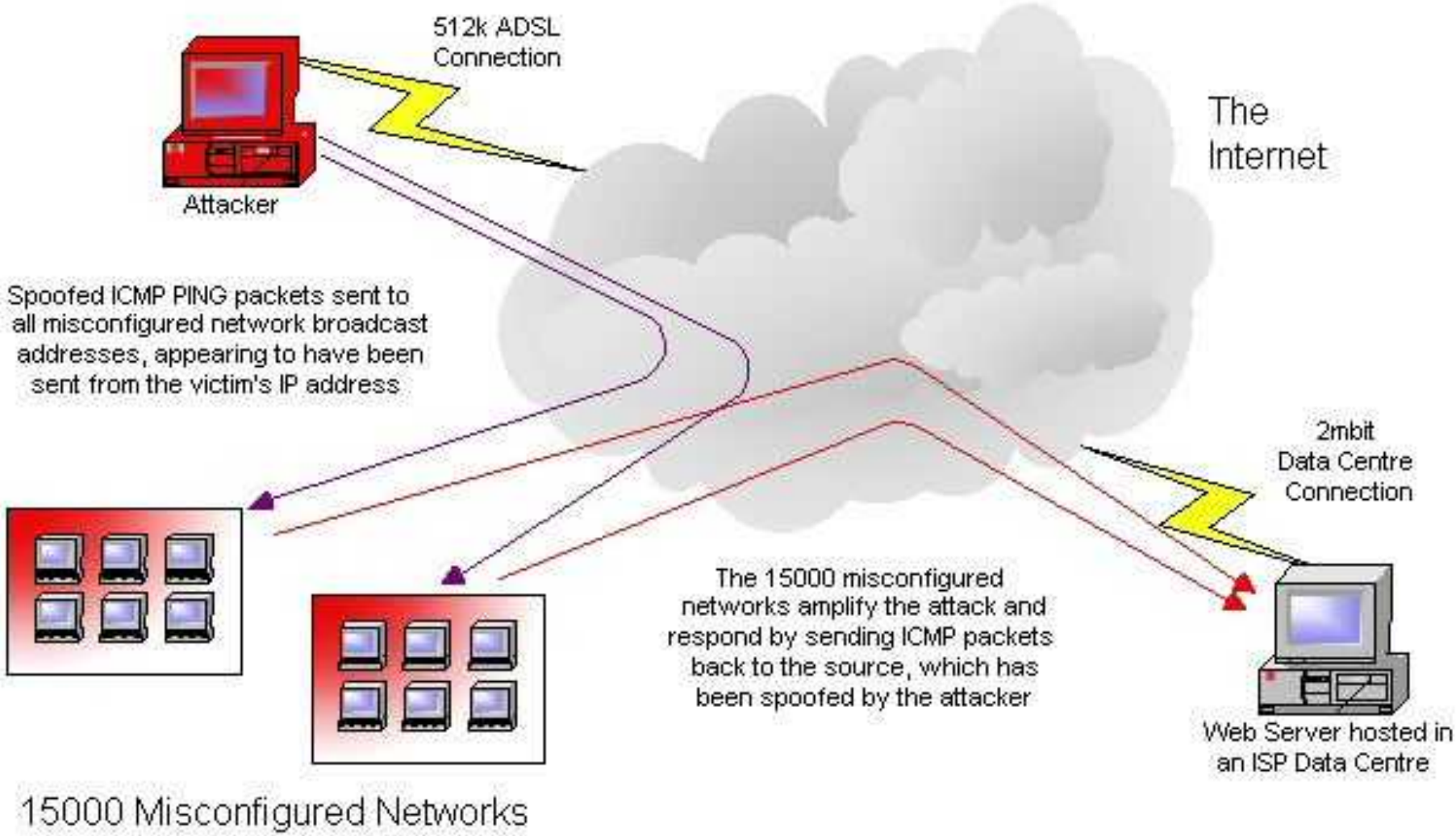
Protecting Against Direct Single-tier DoS Attacks

- Ensuring all relevant security hotfixes and service packs are installed on your hosts to prevent system level attacks through malformed packets.
- Deploying a personal IDS or firewall system if you're using a dialup, to identify the sources of attacks and protect in most cases.

Direct Dual-tier DoS Attacks

- More complex attack model
- Network level vulnerabilities abused
  - Misconfigured network broadcasts
- Difficult for victim to trace and identify attacker
- Examples
  - Smurf

Dual-tier network level DoS attack undertaken. Taking advantage of the fact many Internet-based networks are misconfigured and can be used as 'smurf amplifiers'. By abusing these misconfigured networks, a user with a 512k ADSL connection can totally flood a web server in a data centre on a 2mbit connection



Protecting Against Direct Dual-tier DoS Attacks

- Prevention at the source, ensuring that your networks are not misconfigured to be used as 'smurf amplifiers'.
- Deploying a network-based IDS to identify DoS attempts and identify the attacker himself by analysing network traffic at the time of the attack.
- Ensuring you have a contact detail at your ISP in order to quickly block packets from misconfigured networks in the event of a serious attack.

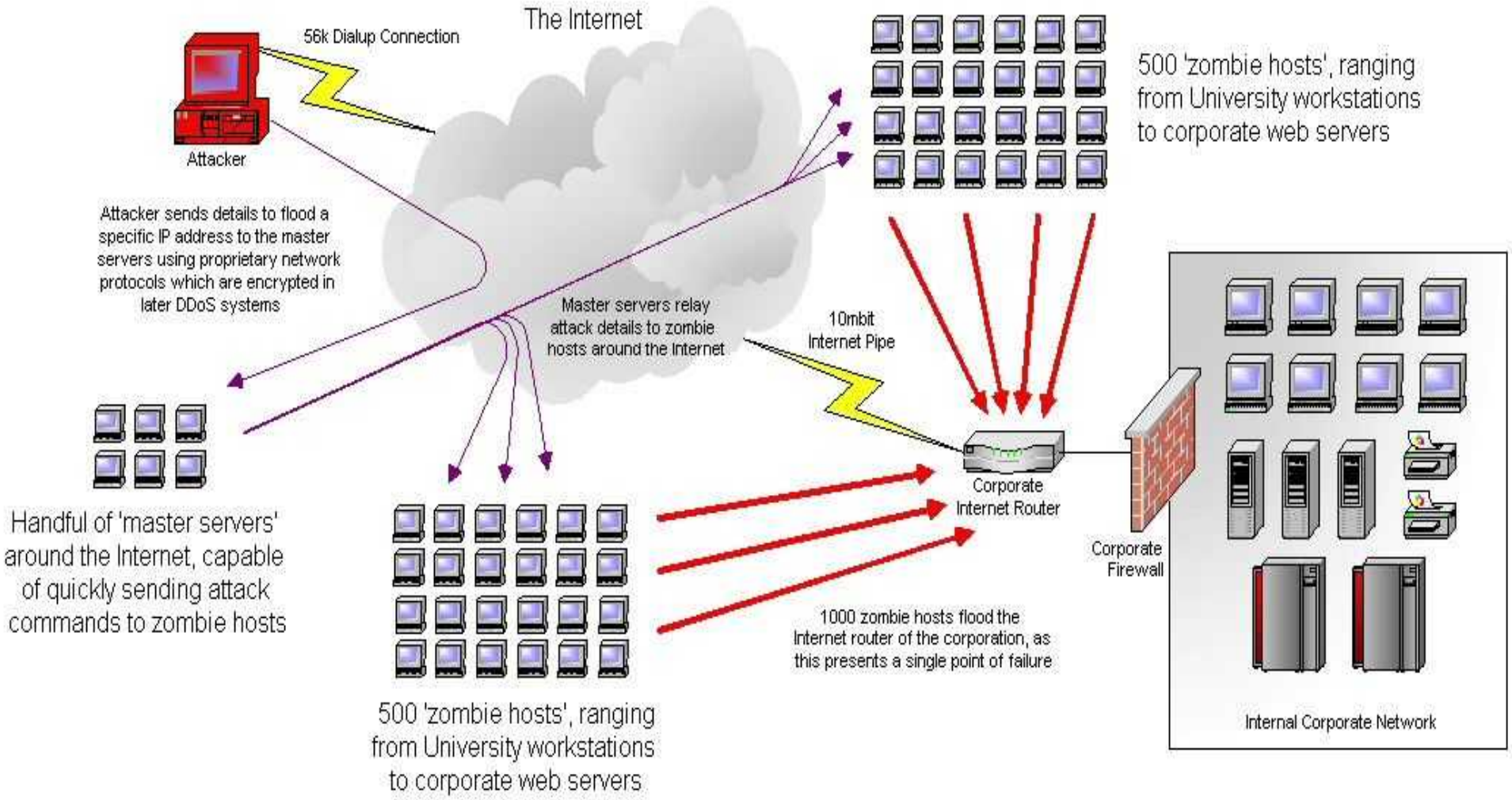
Direct Triple-tier DDoS Attacks

- Highly complex attack model, known as Distributed Denial of Service (DDoS).
- DDoS exploits vulnerabilities in the very fabric of the Internet, making it virtually impossible to protect your networks against this level of attack.
- Extremely dangerous attack type. When Yahoo! Came under attack from a DDoS flood network in the summer of 2000, it saw over 1Gbit of network traffic being sent to it's web farm.
- Examples
  - TFN2K
  - Stacheldraht
  - Mstream

The Components of a DDoS Flood Network

- Attacker
  - Often a hacker with good networking and routing knowledge.
- Master servers
  - Handful of backdoored machines running DDoS master software, controlling and keeping track of available zombie hosts.
  - Often master servers exist on very fast Internet connections, so that they can quickly process and communicate attack details with zombie hosts.
- Zombie hosts
  - Thousands of backdoored hosts over the world

Triple-tier network level DoS attack undertaken. The attacker has spent time setting up and configuring his flood network, which comprises of hundreds of compromised 'zombie' computers on the Internet, which are waiting for commands to flood target IP addresses on the Internet.



Protecting Against Direct Triple-tier DDoS Attacks

- Prevention at the source, ensuring that your hosts are not vulnerable to 'point and click' type automated attacks.
- Deployment of network-based IDS to identify -
  - •Master to Zombie DDoS control traffic
  - •Zombie to Victim flood attack traffic
- Ensuring you have a contact detail at your ISP in order to quickly block packets from zombie hosts and networks in the event of a serious attack.
- Implementation of a security policy defining how your organisation reacts to these threats effectively.

Indirect DoS Attacks

Indirect DoS attacks come about when a worm of virus is at large in the wild, which causes DoS and disruption as a result of its spreading.

Examples of worms and viruses which have caused indirect DoS in this fashion -

- The Love Bug
- Code Red and Code Red II
- Nimda

DoS Prevention Strategies

- Create a security policy covering DoS response
- Prepare for 100% bandwidth consumption, implement back-up lines for data and voice communications in the event of a DoS attack
- Ensure your Internet-based network security is at a good level to prevent compromises and misuse of your networks and bandwidth
- Embrace Intrusion Detection Systems (IDS) to identify DoS traffic and even the attacker in most cases
- Establish good communication channels between you and your ISP to block DoS attacks at Internet-level

DoS Prevention Resources

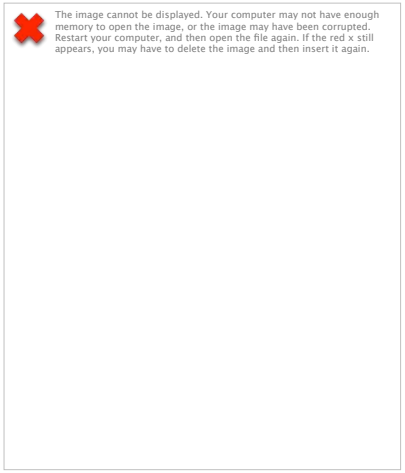
The following sites provide guidance when configuring firewalls, IDS and border routers to prevent DoS attacks from being effective -

http://www.nipc.gov
NIPC DoS tools

http://www.cert.org
CERT DoS information

http://razor.bindview.com
RAZOR 'zombie zapper'

http://staff.washington.edu/dittrich/misd/ddos/
Dave Dittrich's DDoS web site



The End
Thanks for Listening!

Chris McNab

Principal Consultant, Matta Security Limited

chris.mcnab@trustmatta.com