Chap 10

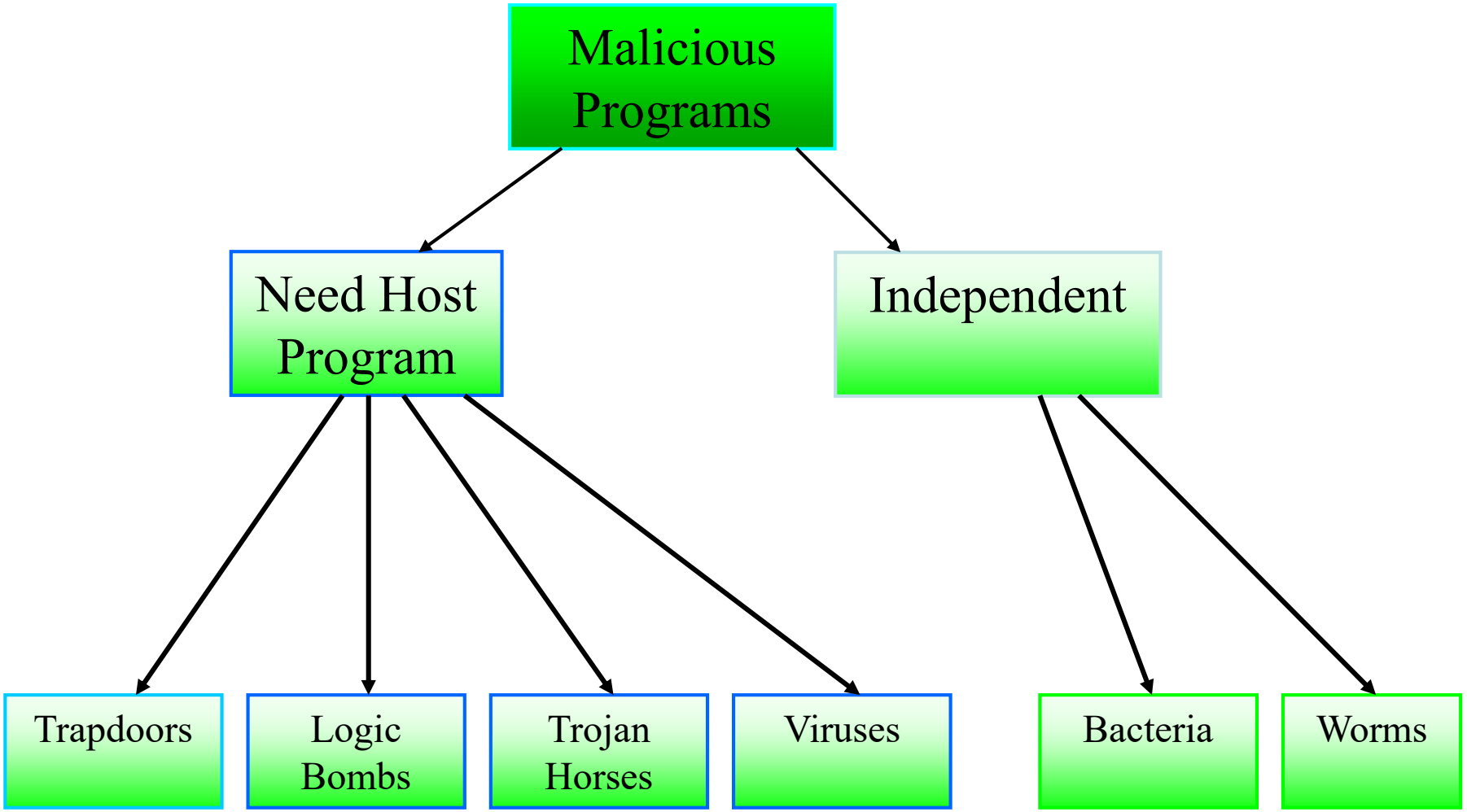
Malicious Software

Viruses and ”Malicious Programs”

- Computer “Viruses” and related programs have the ability to replicate themselves on an ever increasing number of computers. They originally spread by people sharing programs. Now they spread primarily over the Internet (a “Worm”).

- Other “Malicious Programs” may be installed by hand on a single machine. They may also be built into widely distributed commercial software packages. These are very hard to detect before the payload activates (Trojan Horses, Trap Doors, and Logic Bombs).

Taxanomy of Malicious Programs



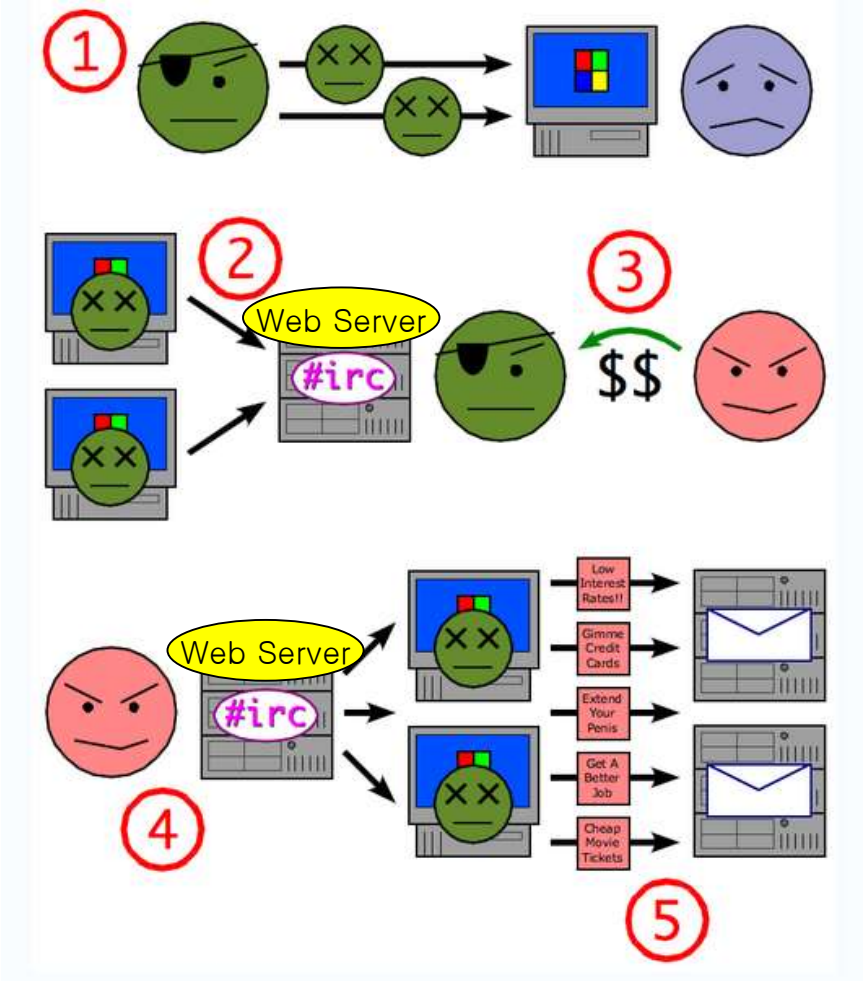
Definitions

- Virus - code that copies itself into other programs.
- A “Bacteria” replicates until it fills all disk space, or CPU cycles.
- Payload - harmful things the malicious program does, after it has had time to spread.
  - A "payload" is code designed to do more than spread the worm - it might delete files on a host system
- Worm - a program that replicates itself across the network (usually riding on email messages or attached documents (e.g., macro viruses).

Definitions

- Trojan Horse - instructions in an otherwise good program that cause bad things to happen (sending your data or password to an attacker over the net).
- Logic Bomb - malicious code that activates on an event (e.g., date).
- Trap Door (or Back Door) - undocumented entry point written into code for debugging that can allow unwanted users.
- Easter Egg - extraneous code that does something "cool." A way for programmers to show that they control the product.
- Botnet - is generally used to refer to a collection of compromised computers

A Configuration of Botnet



Virus Phases

- **Dormant phase** - the virus is idle
- **Propagation phase** - the virus places an identical copy of itself into other programs
- **Triggering phase –** the virus is activated to perform the function for which it was intended
- **Execution phase** – the function is performed

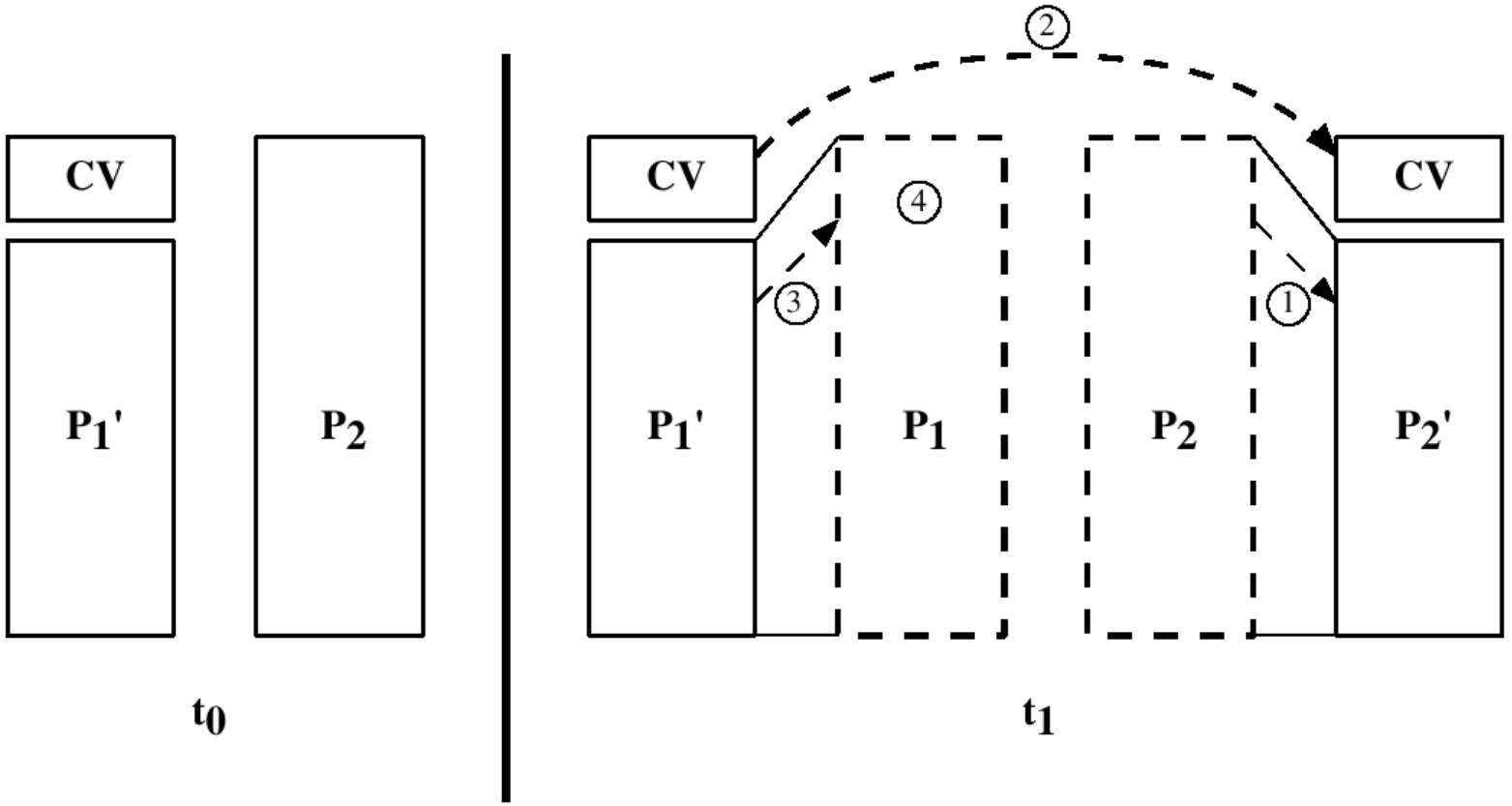
Virus Protection

- **Have a well-known virus protection program, configured to scan disks and downloads automatically for known viruses.**
- **Do not execute programs (or "macro's") from unknown sources (e.g., PS files, Hypercard files, MS Office documents)**
- **Avoid the most common operating systems and email programs, if possible.**

Virus Structure

```
        program V :=

{goto main;
        1234567;

            subroutine infect-executable :=
                {loop:
                file := get-random-executable-file;
                if (first-line-of-file = 1234567)
                        then goto loop
                        else prepend V to file; }

            subroutine do-damage :=
                {whatever damage is to be done}

            subroutine trigger-pulled :=
                {return true if some condition holds}

main:       main-program :=
                {infect-executable;
                if trigger-pulled then do-damage;
                goto next;}

next:

}
```

A Compression Virus



Types of Viruses

- **Parasitic Virus** - attaches itself to executable files as part of their code. Runs whenever the host program runs.
- **Memory-resident Virus** - Lodges in main memory as part of the residual operating system.
- **Boot Sector Virus** - infects the boot sector of a disk, and spreads when the operating system boots up (original DOS viruses).
- **Stealth Virus** - explicitly designed to hide from Virus Scanning programs.
- **Polymorphic Virus** - mutates with every new host to prevent signature detection.
- **Metamorphic Virus** – Mutates with every infection, rewriting itself completely at each iteration of its behavior as well as its appearance

Macro Viruses

- Microsoft Office applications allow “macros” to be part of the document. The macro could run whenever the document is opened, or when a certain command is selected (Save File).
- A macro virus is platform independent.
- Infect documents, delete files, generate email and edit letters.
  - Easily spread, by email
  - Infect dcoumts, not executable portions of code

Antivirus Approaches

1st Generation, Scanners: searched files for any of a library of known virus “signatures.” Checked executable files for length changes.

2nd Generation, Heuristic Scanners: looks for more general signs than specific signatures (code segments common to many viruses). Checked files for checksum or hash changes.

3rd Generation, Activity Traps: stay resident in memory and look for certain patterns of software behavior (e.g., scanning files).

4th Generation, Full Featured: combine the best of the techniques above.

Advanced Antivirus Techniques

- Generic Decryption (GD)
  - CPU Emulator: software-based virtual computer
  - Virus Signature Scanner: a module that scans the target code looking for known virus signatures
  - Emulation Control Module: controls the execution of the target code
- For how long should a GD scanner run each interpretation?

Advanced Antivirus Techniques

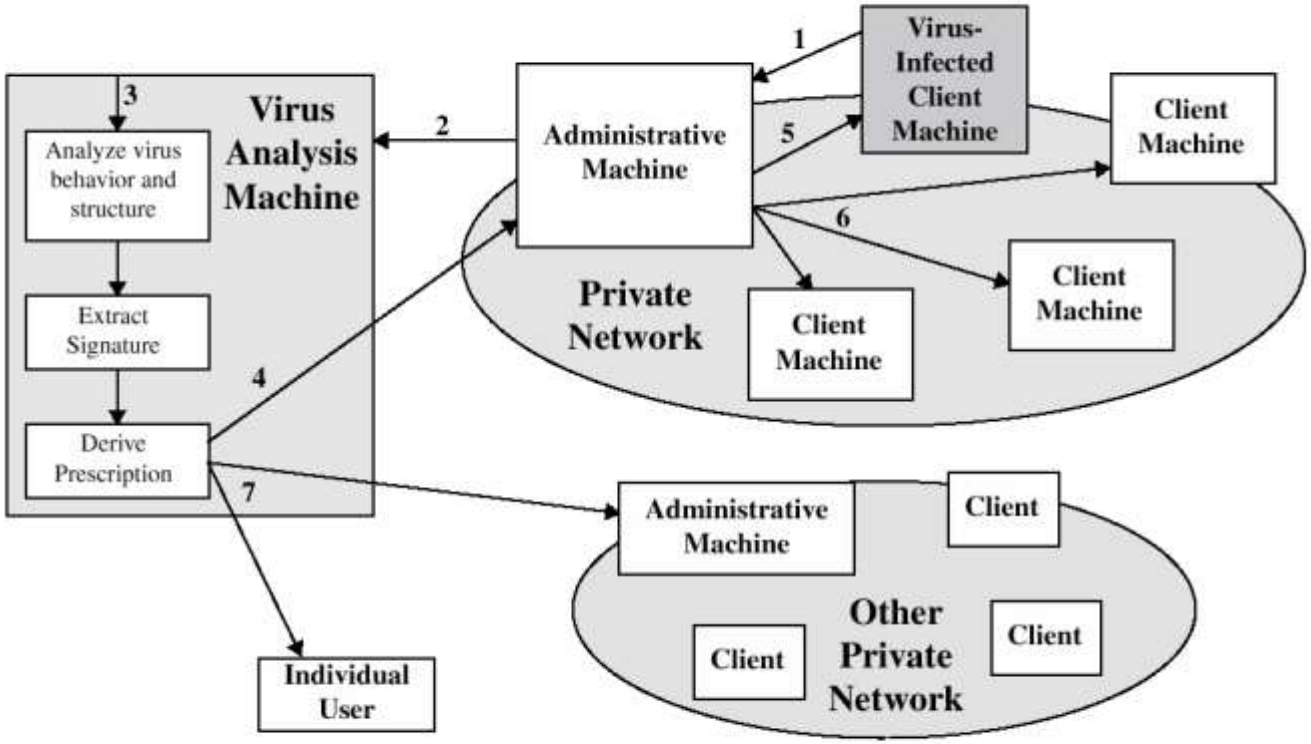
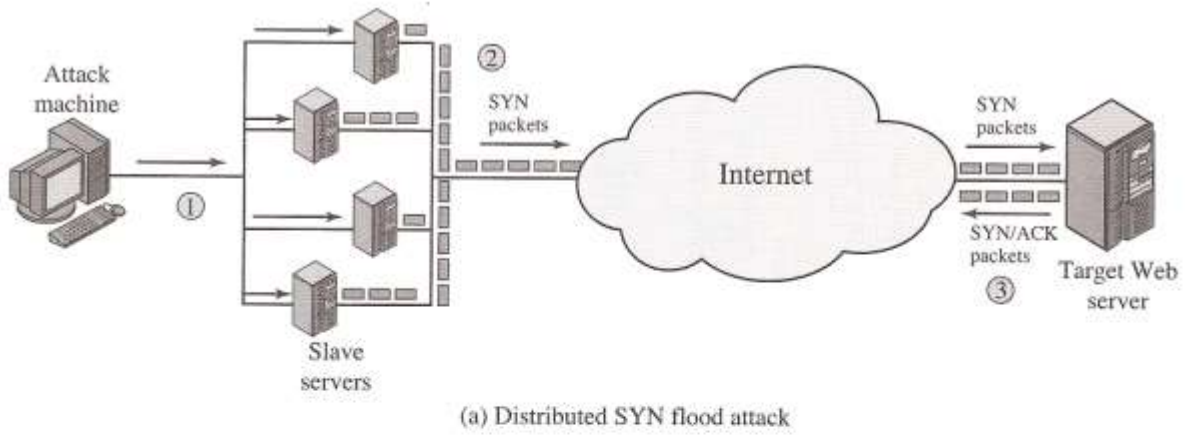
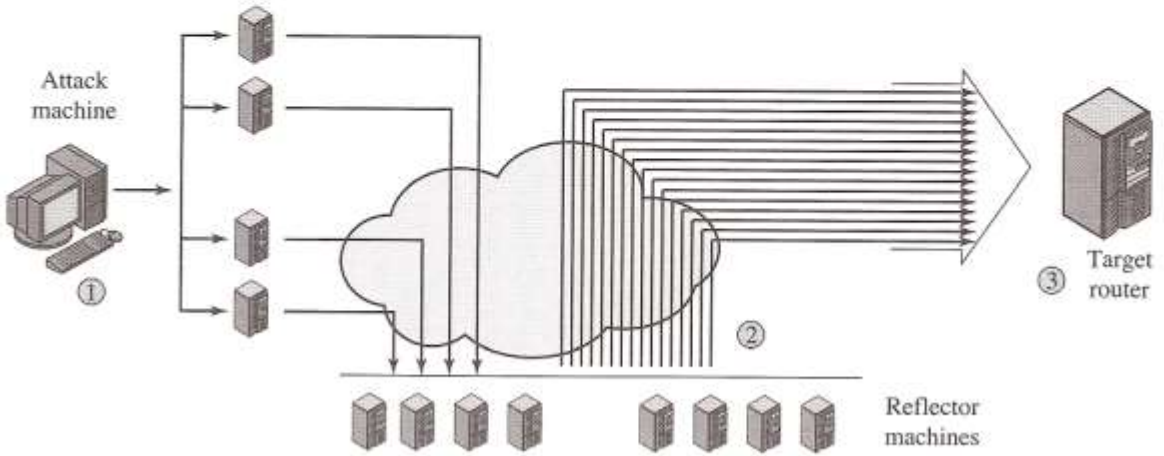


Figure 9.11 Digital Immune System

Examples of Simple DDoS Attacks



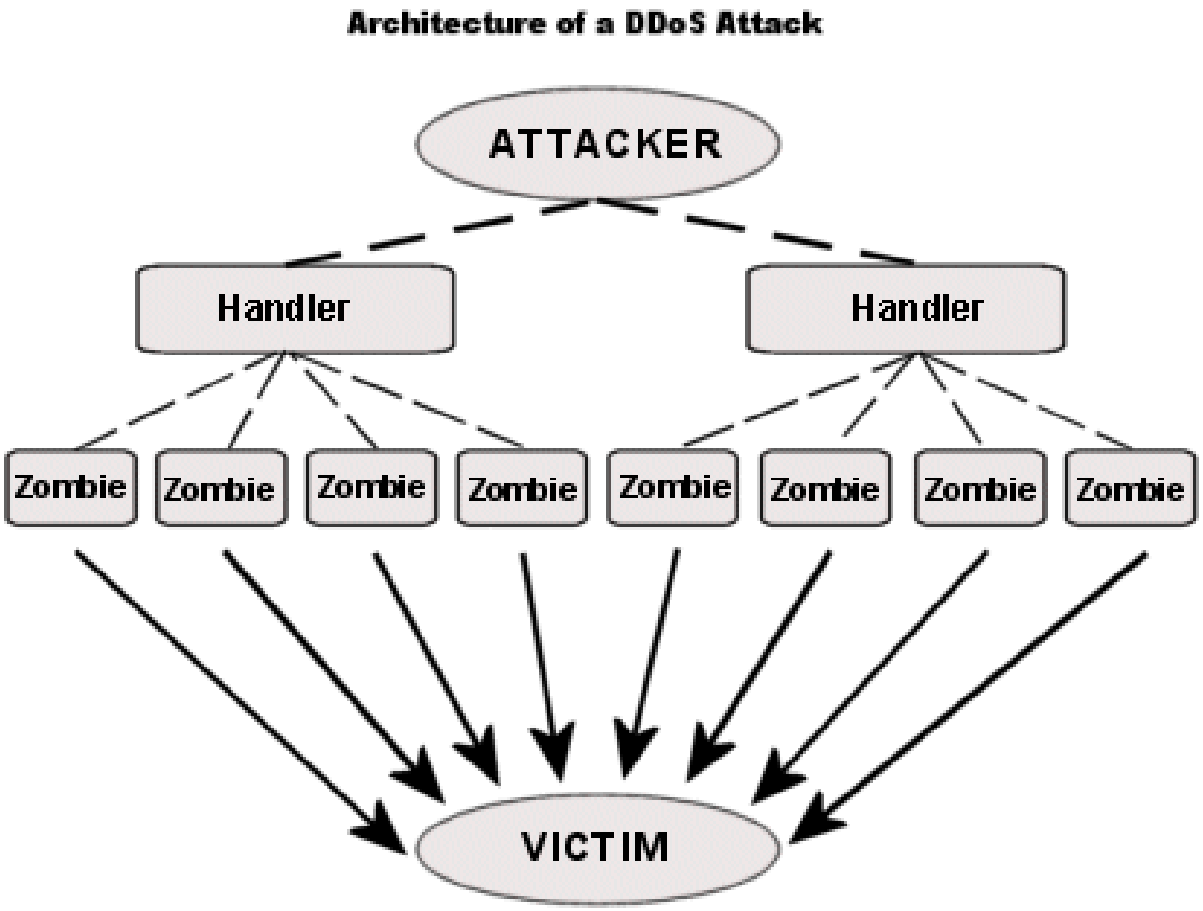
(a) Distributed SYN flood attack



(a) Distributed ICMP attack

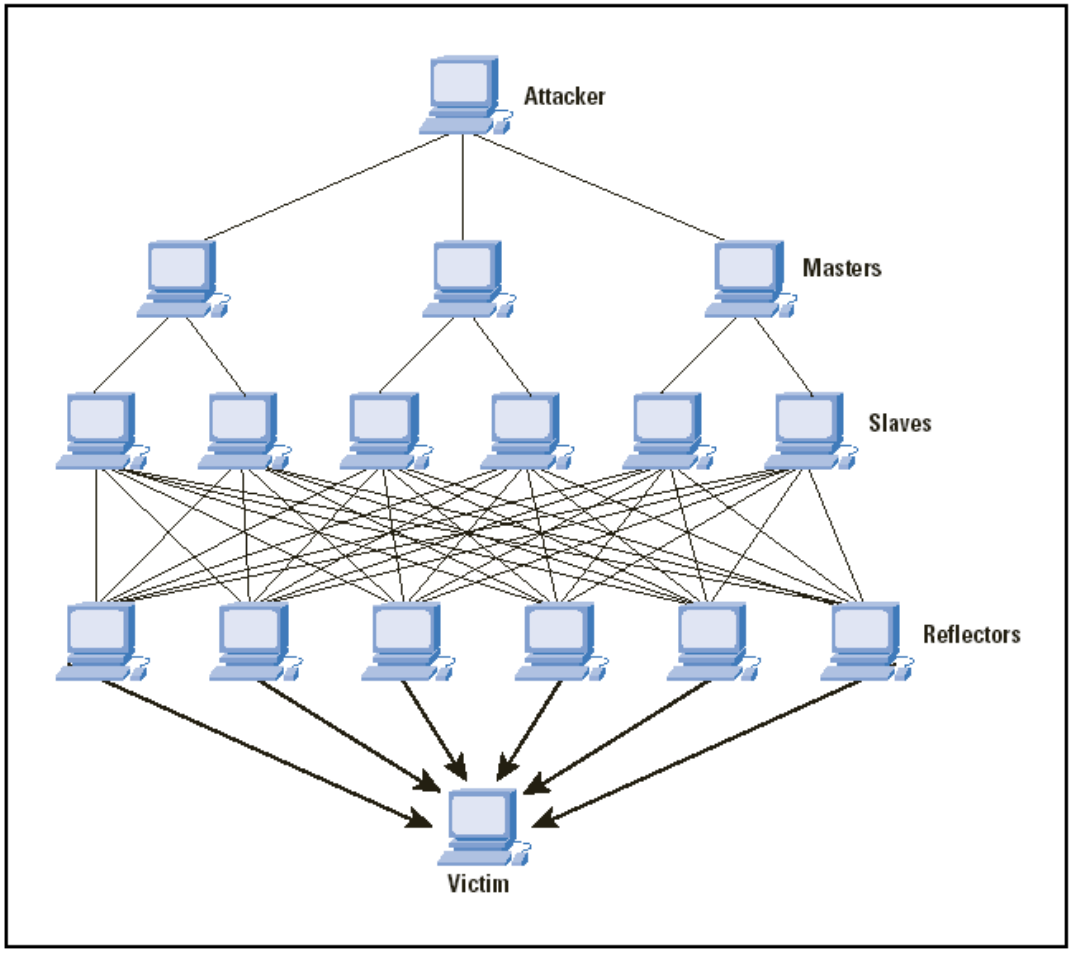
Figure 10.5 Examples of Simple DDoS Attacks

DDoS


Architecture of a DDoS Attack
ATTACKER
Handler
Handler
Zombie
Zombie
Zombie
Zombie
Zombie
Zombie
Zombie
Zombie
VICTIM

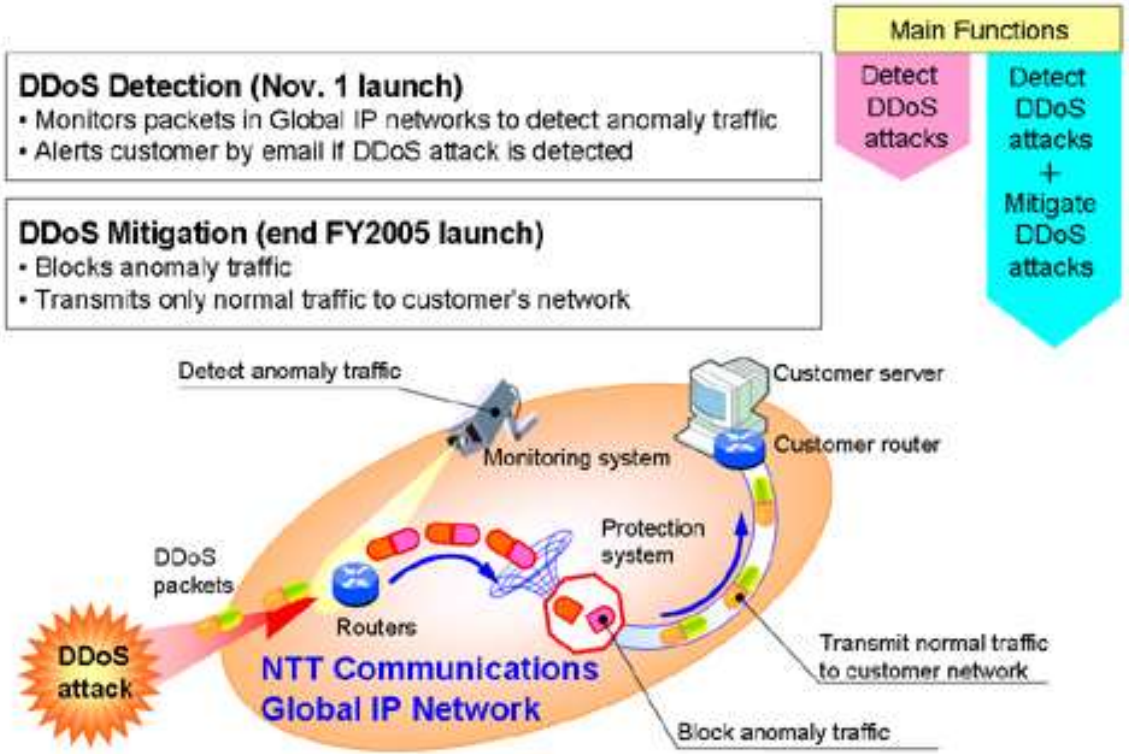
DDoS

Figure 5: A DRDoS Attack



Prevention of DDoS Attack

Attachment: NTT Com's New DDoS Countermeasures



Summary

- Malicious software is software that is intentionally included or inserted in a system for a harmful purpose
- A virus is a piece of software that can “infect” other program by modifying them
- A worm is a program that can replicate itself and send copies from computer to computer across network connections
- DoS attack is an attempt to attempt to prevent legitimate users of a service from using that service
- DDoS is launched from multiple coordinated sources