BASICS OF MALWARE

hat is malware

- Can be loosely defined as “Malicious computer executable”
  - A bit flexible definition
  - Annoying software or program codes
- Running a code without user’s consent
  - “If you let somebody else execute code on your computer, then it is not your own computer”
- Not only virus or worm
  - Sometimes known as computer contaminant
- Should not be confused with defective software which contains harmful bugs

asons for increase

- Growing number and connectivity of computers
  - “everybody” is connected and dependant on computers
  - the number of attacks increase
  - attacks can be launched easily (automated attacks)
- Growing system complexity
  - unsafe programming languages
  - hiding code is easy
  - verification and validation is impossible
- Systems are easily extensible
  - mobile code, dynamically loadable modules
  - incremental evolution of systems

p 10 Malware

1. Packer.Malware.NSAnti.AD
2. Win32.Netsky.P@mm
3. Win32.Worm.Sohanad.NAW
4. Packer.Malware.NSAnti.AG
5. Trojan.Loader.N
6. Trojan.Dropper.Cutwail.F
7. Win32.Netsky.AA@mm
8. Win32.NetSky.D@mm
9. Packer.Malware.NSAnti.Z

- According to Sophos 86% of the reported attacks is spyware

pes of Malware

- Viruses and Worms
- Spyware and adware
- Bots, trojans and keyloggers
  - Backdoors and DoS attacks

uses and Worms

- Worms are the oldest one
  - First well-known worm was known as the Morris Worm
    - Used a BSD Unix flaw to propagate itself
- Viruses requires hosts
  - Word document, etc.
- Both can spread through e-mail
  - Melissa virus uses address books of the infected computers (1999)
- Because it is less beneficial to their creators, this oldest form of malware is dying out

yware and adware

- Growth of Internet helped spawn spyware
- Largely fueled by the prospect of monetary gain
- Not spreads like viruses, instead packaged with user installed software (mostly p2p programs)
- Least virulent forms causes sluggish systems, slow Web browsing, annoying pop-ups
- More dangerous spyware tracks browsing habits or sensitive information

ts and Trojans

- Bots makers infect multiple systems
  - Creates massive botnets that can be used to launch Distributed Denial of Service attacks
- Trojan is a way to secretly install a piece of malware on a system
  - It could be adware or a keylogger
  - It sneakes onto a system and delivers an unexpected and potentially devastating payload

ws and vulnerabilities

- **Homogeneity** – e.g. when all computers in a network run the same OS, if you can break that OS, you can break into any computer running it.
- **Defects** – most systems containing errors which may be exploited by malware.
- **Unconfirmed code** – code from a floppy disk, CD-ROM or USB device may be executed without the user's agreement.
- **Over-privileged users** – some systems allow all users to modify their internal structures.
- **Over-privileged code** – most popular systems allow code executed by a user all rights of that user.

VIRUSES

uses

- It is a piece of code that infect other programs by modifying them
  - Replicates its instructional code into other programs very much like its biological homophone
- It can also spread into programs in other computers by several ways
- It secretly executes when host program is run
- It is specific to particular software/hardware platform

etime of a virus

- Dormant phase
  - Idle, not all of them have this phase
- Propagation phase
  - Copies itself into other programs
- Triggering phase
  - Activated by a system event
- Execution phase
  - Runs its payload (part for malicious actions)

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 condit
    holds; }

main :              main-progra
{ infect-executable;
if trigger-pulled then do-dam
goto next; }
next:
}
```

us structure

- The infected program will first run the virus code when invoked
- If the infection phase is fast, then it will be unrecognizable
- Infected version of a program is longer than the normal
  - A virus can compress the infected program to make its versions identical length

pes of viruses

- Parasitic virus
  - Traditional kind
- Memory-resident virus
  - Locates in memory, infects executing programs
- Boot sector virus
  - Infects MBR, spreads when system is booted
- Stealth virus
  - Compression technique, intercept logic in disk I/O routines
- Polymorphic virus
  - Makes detection by signature impossible by adding junk instructions, changing instruction order or using encryption
- Metamorphic virus
  - Similar to polymorphic virus, additionally changes its behaviour

acro viruses

- Platfrom independent
  - Any platform that supports office documents
- Infects Microsoft Word documents
- Easily spread by e-mails

ail viruses

- Eg. Melissa, sends mails with Word attachment
- Sends itself to everyone on the mail list in email package
- Does local damage
- In 1999, more powerful versions appeared
  - Executes when mail is read
- Strengthens the propagation phase of virus

GRAYWARE

ayware

- Applications that are installed on a user's computer to track and/or report certain information back to some external source
- Usually installed and run without the permission of the user
- Behave in a manner that is annoying or undesirable
- Designed to harm the performance of computers

ayware

- Sources can come from
  - Downloading shareware, freeware or other forms of file sharing services
  - Opening infected e-mails
  - Clicking on pop-up advertising
  - Visiting frivolous or spoofed web sites
  - Installing Trojan applications

ayware

- Not necessarily malevolent
  - Web site developers use newer techniques to customize their web sites & obtain better results
- Ultimate goal of many of them
  - Tracking the usage patterns of visitors to offer more customized search results to result in higher sales

ayware

- More of an annoyance than a security threat
  - Slower performance
  - More pop-up advertising
  - Web browser home pages being directed to other sites
- If the hackers are not counted!

ayware

- Hackers use grayware to load and run programs that
  - Collect information
  - Track usage pattern
  - Invasion of privacy
  - Track keystrokes
  - Modify system settings
  - Inflict other kinds of damage

ayware -- Categories

- Spyware
  - Included with freeware
  - Does not notify the user of its existance or ask permission to install the components
  - Designed to track & analyze a user's activity
    - Web browsing habits
    - Primarily for market purposes
  - Tracked information is sent back to the originator's Web site
  - Responsible for performance related issues

ayware -- Categories

- Adware
  - Embedded in freeware applications that users can donwload & install at no cost
    - By accepting the 'End User Licence Agreement'
  - Used to load pop-up browser windows to deliver advertisements
  - Considered to be invasive

ayware -- Categories

- Dialers
  - Used to control the PC's modem
    - To make long distance calls
    - To call premium 900 numbers to create revenue for the theaf
- Gaming
  - Installed to provide joke or nuisance games

ayware -- Categories

- Joke
  - Used to change system settings but do not damage the system
    - Changing the system cursor
    - Changing Windows' background image
- Peer-to-peer
  - Installed to perform file exchanges
  - Used to illegally swap music, movies, etc.

ayware -- Categories

- Key Logger
  - One of the most dangerous applications
  - Installed to capture the keystrokes
    - User & password information
    - Credit card numbers
    - E-mail, chat, instant messages, etc.
- Hijacker
  - Manipulates the Web browser or other settings to change the user's favorite or bookmarked sites, start pages or menu options
  - Some can also manipulate DNS settings

ayware -- Categories

- Plugins
  - Designed to add additional programs or features to an existing application in an attempt to control, record and send browsing preferences or other information back to an external destination
- Network Management
  - Designed to be installed to for malicious purposes
  - Used to change network settings, disrupt network security

ayware -- Categories

- Remote Administration Tools
  - Allow an external user to remotely gain access, change or monitor a computer on a network
- Browser Helper Object (BHO)
  - DLL files that are often installed as part of a software application to allow program to control the behaviour of Internet Explorer
  - Can track surfing habits

ayware -- Categories

- Toolbar
  - Installed to modify the computer's existing toolbar features
  - Can be used to monitor web habits, send information back to the developer or change the functionality of the host
- Download
  - Installed to allow other software to be downloaded & installed without the user's knowledge
  - Usually run during the startup

ayware -- Symptoms

- Slower computer performance
  - Takes more CPU & memory resources
  - Can be identified from Windows Task Manager
    - Usually unkown applications to users
- Send & receive lights on modem or the network icons on the task bar are flashing even though you are not performing any online process

ayware -- Symptoms

- Computer displays pop-up messages & advertisements when not connected to Internet or when not running the browser
- Change in home page
- Change in search engine settings
- Change in bookmarks
- Change in toolbars or new installed options
  - Attempt to remove those fail

ayware -- Symptoms

- Increase in phone bills
- Stop in anti-virus program, anti-spyware program or any other security related program
- Receival of warnings of missing application files
  - Replacement does not work

ayware -- Protection

- User Education
  - Educating employees regarding the nature & dangers of grayware
  - Establishing policies that prohibit downloading & installing applications that are not approved
  - If the dowload & installation is allowed, 'End User License Agreement' should be read carefully
  - Increase the security settings on the Web browser
  - Configuration of e-mail programs as not to automatically download things
    - Turn of auto-preview

ayware -- Protection

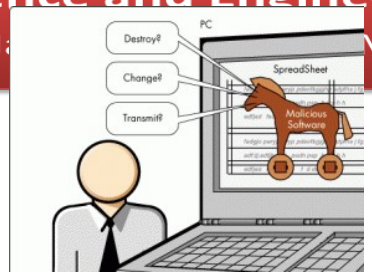
- Host-based Anti-spyware Programs
  - Client based software applications that spot, remove and block spyware
  - Functions similarly to antivirus programs
  - Difficulty: overhead of installing & maintaining client software applications on all corporate PCs
    - Resources to purchase & install software and to perform routine upgrades on each computer
  - Danger: can be disabled by the end user or by other malicious application

ayware -- Protection

- Network-based Grayware Protection
  - Through a network gateway approach
  - Install the grayware detection on a perimeter security appliance
  - Centralizes the intelligence at the ingress point
  - Lowers the overhead of installing, maintaining and keeping it up-to-date
  - Drawback
    - What happens when the user leaves the office?

TROJAN HORSE

Trojan Horse



- Is another type of proper looking software
  - But performs another action such as viruses
- Usually encoded in a hidden payload
- Used in installation of backdoors
- It does not propagate itself by self-replication
- Derived from the classical story of Trojan Horse

me examples

- Adding code to UNIX login command
  - Enables acception of encrypted password, or a particular known password
- C compiler can be modified to automatically generate rogue code
- Waterfall.scr is a free waterfall screensaver (!)
  - Unloads hidden programs, commands, scripts

pes of Trojan Horse

- Remote Access
- Data Destruction
- Downloader
- Server Trojan (Proxy, FTP, IRC, Email, HTTP/HTTPS, etc.)
- Security software disabler
- Denial-of-Service attack (DoS)

mages of Trojan Horse (1)

- Erasing or overwriting data on a computer
- Encrypting files in a cryptoviral extortion attack
  - Attacker encrypts the victim's files and the user must pay the malware author to receive the needed session key
- Corrupting files in a subtle way
- Upload and download files
- Copying fake links, which lead to false websites, chats, or other account based websites, showing any local account name on the computer falsely engaging in untrue context
- Allowing remote access to the victim's computer.
- Spreading other malware, such as viruses
  - called a 'dropper' or 'vector'

mages of Trojan Horse (2)

- Setting up networks of zombie computers in order to launch DDoS attacks or send spam
- Spying on the user of a computer and covertly reporting data like browsing habits to other people
- Making screenshots
- Logging keystrokes to steal information such as passwords and credit card numbers
- Phishing for bank or other account details
- Installing a backdoor on a computer system
- Opening and closing CD-ROM tray Playing sounds, videos or displaying images.

mages of Trojan Horse (3)

- Calling using the modem to expensive numbers, thus causing massive phone bills.
- Harvesting e-mail addresses and using them for spam
- Restarting the computer whenever the infected program is started
- Deactivating or interfering with anti-virus and firewall programs
- Deactivating or interfering with other competing forms of malware
- Randomly shutting off the computer

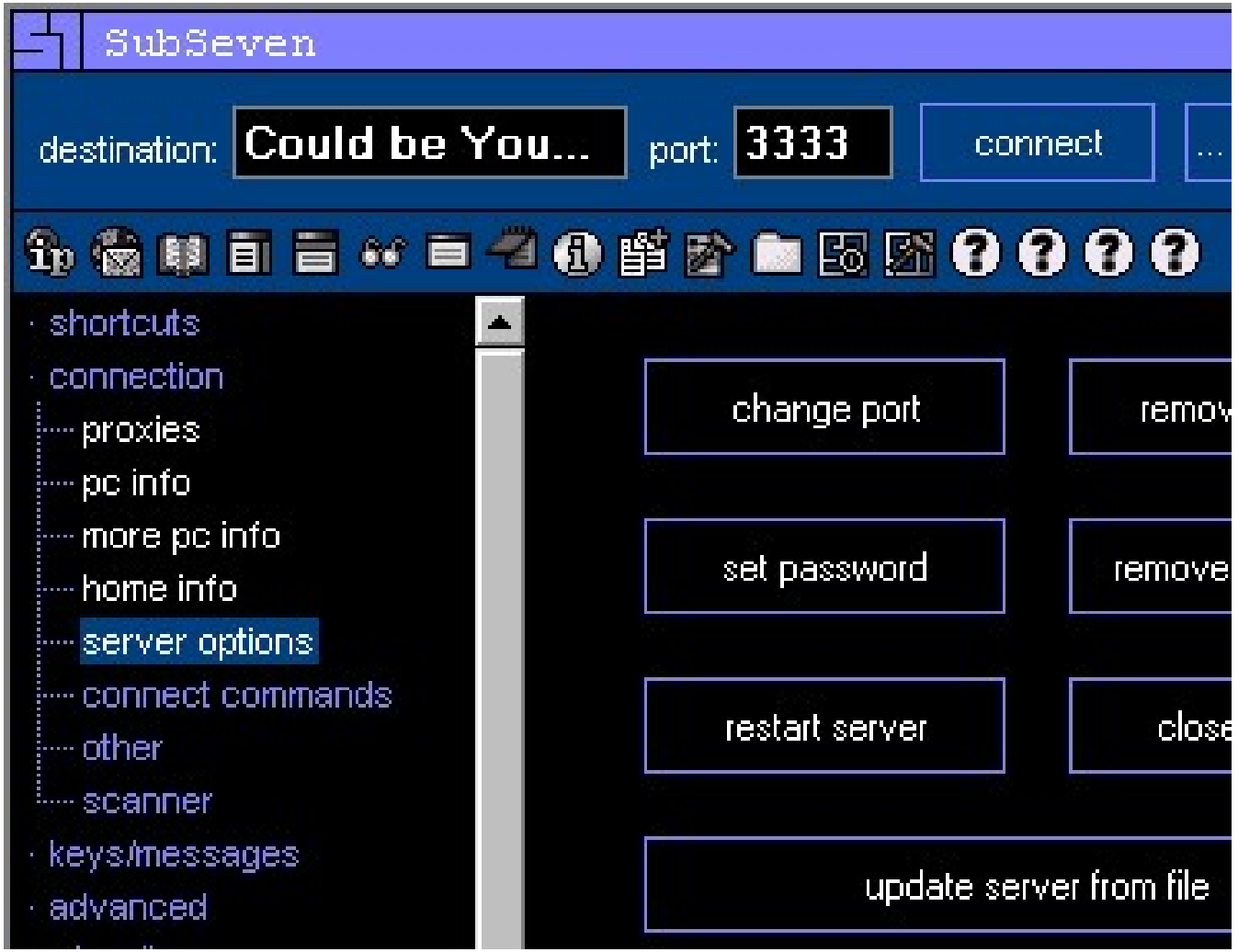
ckdoor (1)

- Bypassing actual authentication, securing remote access to a computer, obtaining access to plaintext
  - But remains undetected
- May be an installed program (e.g. Back Orifice) and modification to an existing program
- Threat is surfaced with development of multi-user and network based systems

ckdoor (2)

- Hard coded user and password combination
- Backdoors can be created by modification of source codes
  - Or modification of the compiler
- Computers infected by Sobig and Mydoom are a potential for spammers to send junk email
- Symmetric and asymmetric backdoors

mer 101 (Backdoor)



WORMS

orms

- It is a self-contained program and does not need human intervention unlike e-mail virus
- Replicates and sends copies of itself from computer to computer
- Performs disruptive or destructive actions
- May change its process name to system processes

w does it replicate?

- Electronic mail facility
- Remote execution capability
- Remote login capability

etime of a worm

- Dormant phase
- Propagation phase
  - Search for other systems by looking up host tables, repositories of remote system addresses
  - Connect to remote system
  - Copy itself to remote system and make it run
- Triggering phase
- Execution phase

me examples

- Morris worm
- Code Red

orris worm

- Released in 1998 by Robert Morris
- Designed for UNIX systems
- Propagation techniques
  - Examine system tables (list of other machines trusted by this one), mail forwarding files, remote account access permission tables

orris worm

- Attempt to log on to remote host as legitimate user
  - Crack the local password file, use permutations of usernames inside, all words in local directory
- Exploited a bug in the finger protocol
  - Gets info about remote user
- Exploited a trapdoor in remote sendmail program
- If succeeded, gains access to remote shell ands sends a short bootstrap program and executes it

de Red

- Released in July of 2001
- Exploits a security hole in Microsoft IIS
- It locates in RAM memory
- It propagates by probing random IP addresses between 1st and 19th of any month
  - Infected 360,000 servers in second reactivation
- It initiates DoS attack to a US government site and disrupts local service

de Red II

- New version installs a backdoor allowing master hacker to use host computer as a zombie

te of worm technology

- Multiplatform
  - Execute in different platforms
- Multiexploit
  - Use variety of exploits in web servers, browsers, etc.
- Ultrafast spreading
  - Prior Internet scan for vulnerable machines
- Polymorphic
  - Use functionality equivalent instructions and encryption
- Metamorphic
  - Change behavioural patterns
- Transport vehicles
  - Spread other malware tools
- Zero-day exploit
  - Use newly discovered exploits

SPAM

am

- Abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages
- Remains economically viable
  - Advertisers have no operating cost beyond the management of their mailing lists
  - Difficult to hold senders accountable for their mass mailings

amming in Different Media

- E-mail Spam
  - Unsolicated bulk e-mail (UBE)
  - Unsolicated commercial e-mail (UCE)
  - Practice of sending unwanted e-mail messages
  - Sent via ‘zombie networks’, networks of virus- or worm-infected PCs
  - Many modern worms install a backdoor which allows the spammer access to the computer

amming in Different Media

- Instant messaging & Chat room Spam
  - Requires scriptable software & the recepients' IM usernames
- Chat Spam
  - Can occur in any live chat environment
  - Consists of repeating the same word/sentences many times to get attention or to interfere with normal operations
- Newsgroup & Forum Spam

amming in Different Media

- Mobile Phone Spam
- Online Game Messaging Spam
- Spam Targeting Search Engines
  - Spamdexing
  - Practice on the WWW of modifying HTML pages to increase the chances of them being placed high on search engine relevancy lists
- Blog, Wiki & Guestbook Spam
- Spam Targeting Video Sharing Sites

Distributed Denial of Service Attack (DDoS)

tributed Denial of Service Attack (DDoS)

- DDoS attacks make computer systems inaccessible by flooding servers, networks and end-user computers
- In a DDoS attack a large number of compromised hosts are amassed
- If an attack comes from a single machine, it is referred to as a DoS

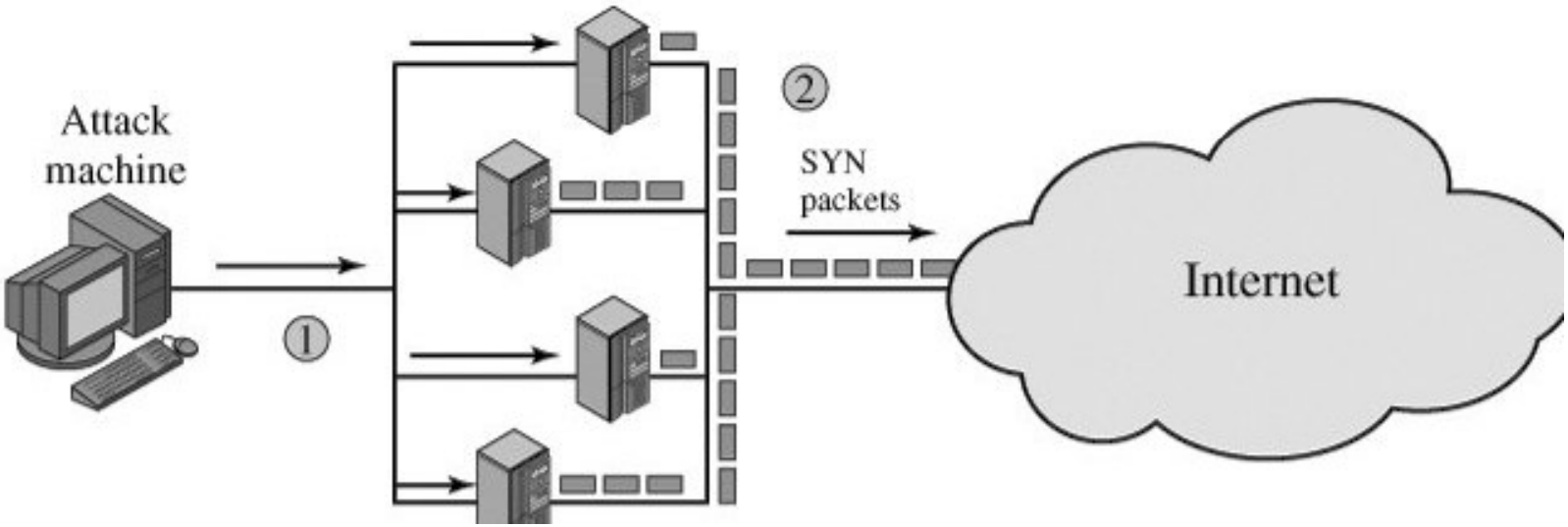
ack Description

- DDoS attack attempts to consume target's resources
- Consume operation is based on:
  - Internal Resource Attack
  - Consume of Data Transmission Resource

ernal Resource Attack

- Attacker takes control of multiple hosts, and instructs them to contact with target
- Slave hosts begin sending TCP/IP SYN packets with erronous return IP address information
  - SYN packets are requests to open TCP connections
- Server sends SYN/ACK response packets to these spurious IP addresses
- Data structure is consumed with “half open” connections

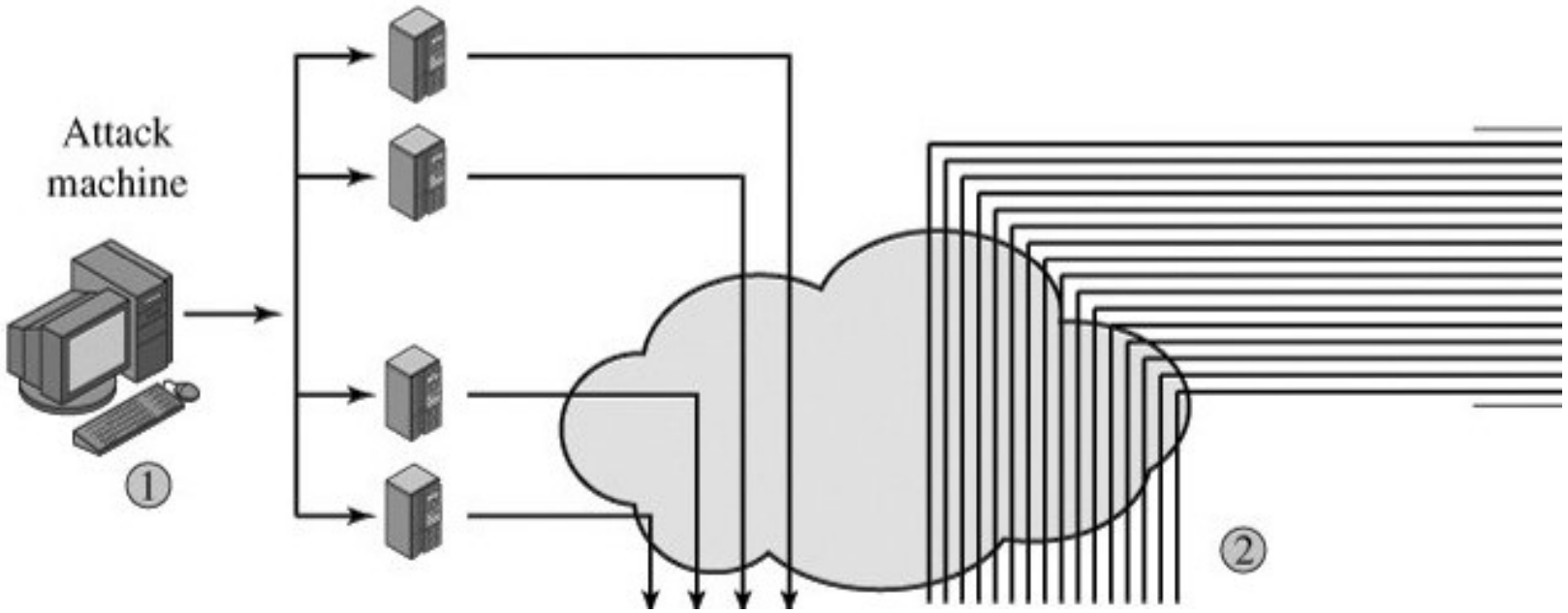
tributed SYN Flood Attacks



nsume of Data Transmission Resource

- Attacker takes control of hosts, intructs them to send ICMP ECHO packets with target's IP address, to a group of hosts
- Nodes that receive multiple requests and responds with sending echo reply packets
- Target's router is flooded, and leaves no data transmission capacity for legitimate traffic

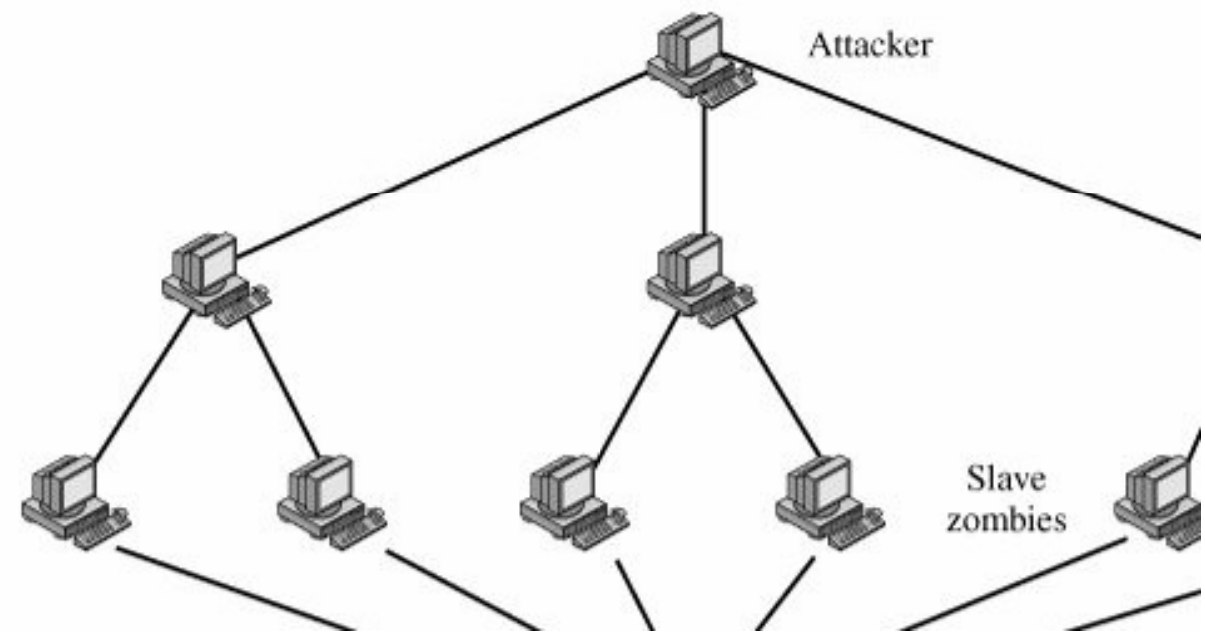
tributed ICMP Attack



ect DDoS Attack

- Attacker can implant zombie software
  - Master and slave zombies
- Attacker coordinates master zombies
  - They trigger slave zombies
- Why are two level zombies needed?
  - It makes more difficult to trace the attack back to its source

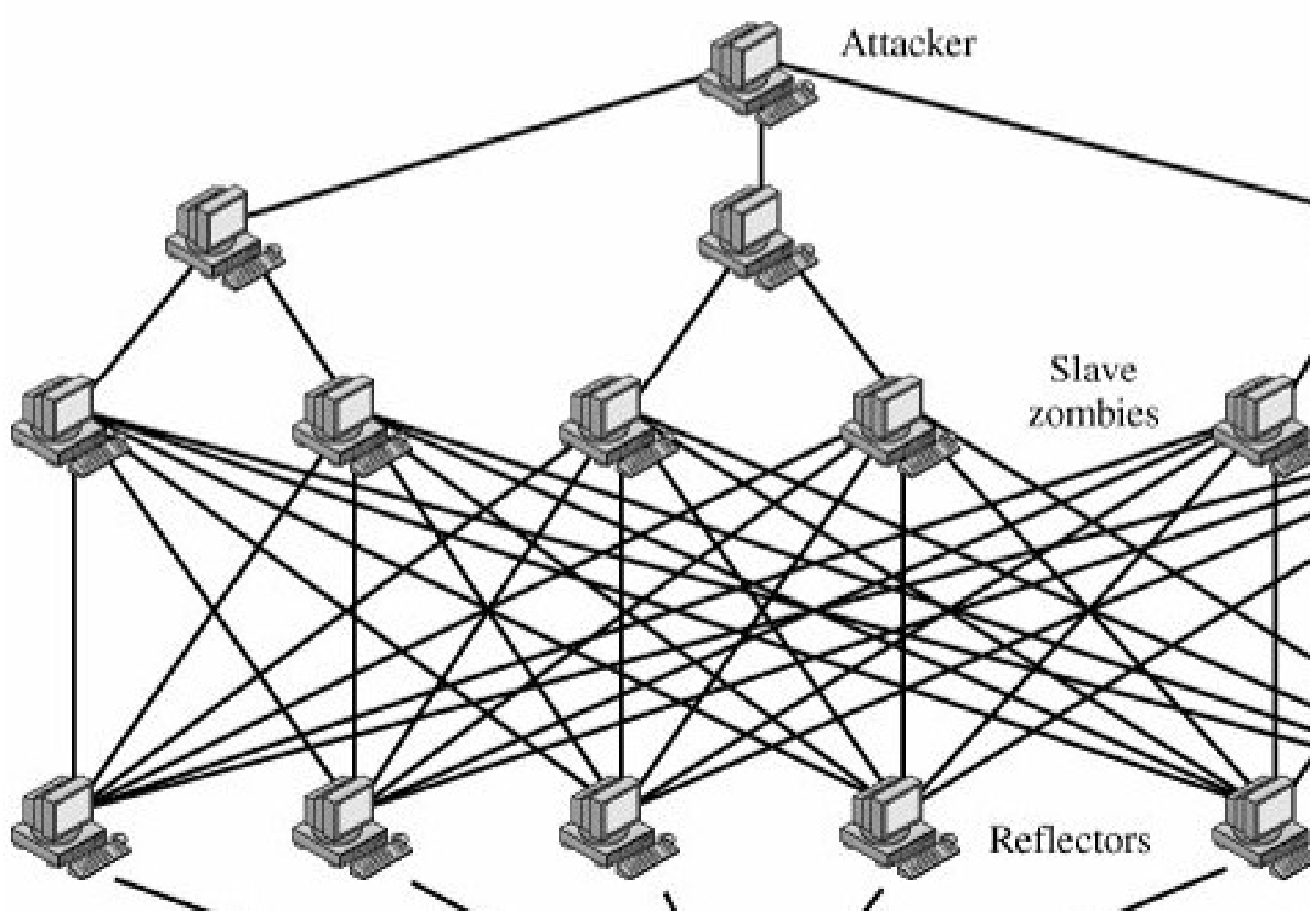
ect DDoS Attack



flector DDoS Attack

- This time slaves send packets to reflectors (uninfected machines)
- Source address of these packets are spoofed IP address of the target
- Reflectors response with packets directed to the target machine
- A reflector DDoS can easily involve more machines
- Hard to detect the source because attack comes from uninfected machines

flector DDoS Attack



w to find victims?

- Random
  - This may cause generalized disruption
- Hit-list
  - It results very short scanning period
- Topological
- Local subnet

oS Countermeasures

- Attack prevention and preemption
  - Enforcing policies for resource consumption
- Attack detection and filtering
  - Looking for suspicious patterns of behaviour
- Attack source traceback and identification
  - Does not yield results fast enough

MALWARE TO PROFIT

lware to Profit

- During 1980s and 1990s
  - Created as a form of vandalism or prank
- Recently
  - Written with a financial or profit motive
  - Choice of the author to monetize control over infected systems
    - Turn the control into a source of revenue
- Since 2003
  - Some redirect search engine results to paid advertisements

lware to Profit

- Another way
  - Directly use the infected computers to do work for the creator
  - Infected computers are used as proxies to send out spam messages or to targat anti-spam organizations with distributed DoS attacks
  - Advantage: anonymity

lware to Profit

- In order to coordinate the activity of many infected computers
  - Use of coordinating systems – botnets
- Botnets are also used to push ungraded malware to the infected systems
- Other than those
  - Stealing credit card number
  - Stealing passwords of the online games
  - Taking the control of the modem

VIRUS COUNTERMEASURES

us countermeasures

- Antivirus approaches
- Advanced antivirus techniques

tivirus approaches

- The best way is prevention
- Detection
- Identification
- Removal

nerations of antivirus software

- First generation
  - Simple scanners, requires virus signature, examines proram length
- Second generation
  - Heuristic scanners, looks for fragments of virus codes, decrypts the virus
  - Computes checksum
- Third generation
  - Examines virus actions, not structure
- Fourth generation
  - Conducts a combination of mentioned techniques
  - Includes access control capability

vanced antivirus techniques

- Generic Decryption
- Digital Immune Sytem
- Behaviour-Blocking Software

neric Decryption

- CPU emulator
- Virus signature scanner
- Emulation control module

gital Immune System

- Monitoring program in client machine discovers suspicious programs, signatures or behaviours, forwards program to administrative machine
- Administrative machine encrypts and sends it to central analysis machine
- Central analysis machine uses emulation technique identifies the virus and produces a prescription
- Prescription is sent back

haviour-blocking software

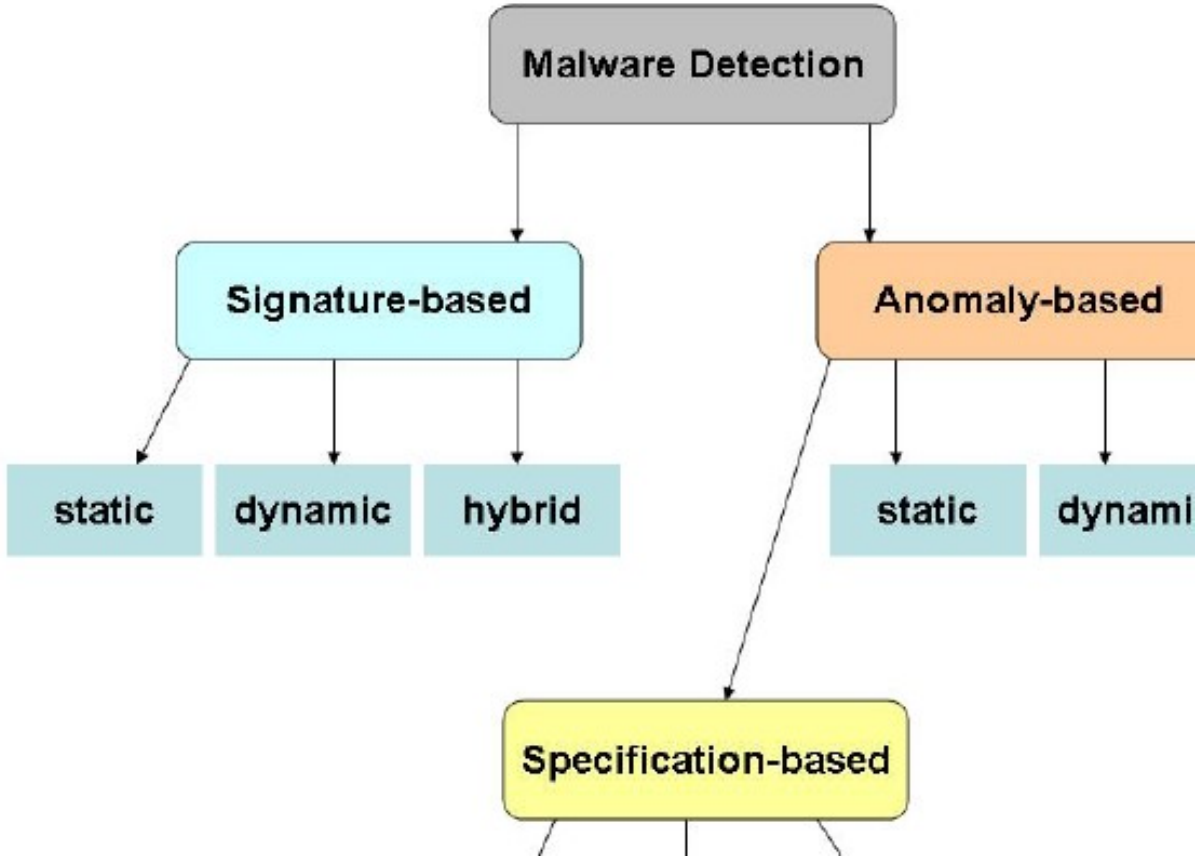
- It is integrated with OS
- Monitors suspicios behaviours such as file operations, disk operations, system settings, scripts in e-mails

MALWARE DETECTION

lware Detector

- Attemps to protect the system by detecting malicious behaviour
- May or may not reside on the same system it is trying to protect
- Performs its protection through the manifested malware detection techniques
- Take two inputs:
  - Its knowledge of malicious behaviour
  - Program under inspection

lware Detection Techniques



lware Detection Techniques

- Anomaly-based
  - Uses its knowledge of what constitutes normal behaviour to decide the maliciousness of a program
  - Specification-based detection: leverage a rule set of what is valid behaviour
- Signature-based
  - Uses its characterization of what is known to be malicious to decide the maliciousness of a program

lware Detection Techniques

- Specific approach is determined by how the technique gathers information to detect malware
- Static analysis
  - Before the program under inspection executes
    - i.e. Sequence of bytes
- Dynamic analysis
  - During or after program execution
    - i.e. Systems seen on the runtime stack