امنیت شبکه

گردآوری: محمدعلی عظیمی

بدافزار ها

Malware: Malicious Software

گردآوری: محمدعلی عظیمی

Network Security Essentials

Fourth Edition

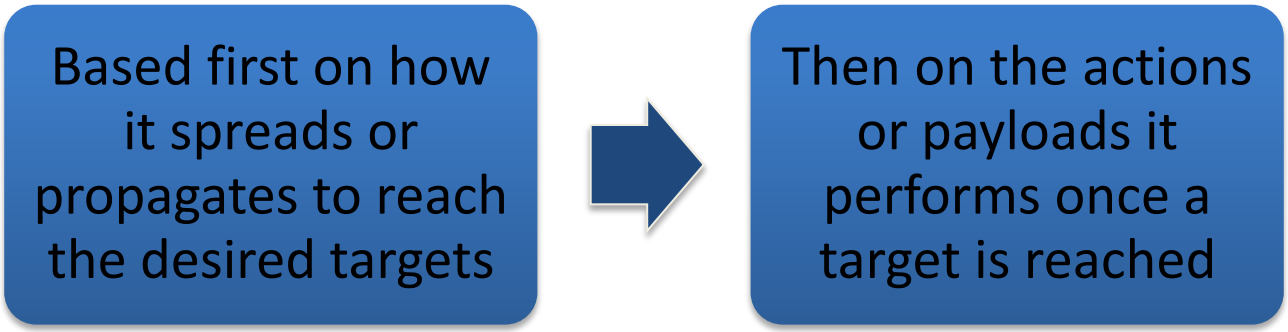
by William Stallings

Lecture slides by Lawrie Brown

Name	Description
Virus	Malware that, when executed, tries to replicate itself into other executable code; when it succeeds the code is said to be infected. When the infected code is executed, the virus also executes.
Worm	A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network.
Logic bomb	A program inserted into software by an intruder. A logic bomb lies dormant until a predefined condition is met; the program then triggers an unauthorized act.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program.
Backdoor (trapdoor)	Any mechanisms that bypasses a normal security check; it may allow unauthorized access to functionality.
Mobile code	Software (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
Exploits	Code specific to a single vulnerability or set of vulnerabilities.
Downloaders	Program that installs other items on a machine that is under attack. Usually, a downloader is sent in an e-mail.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Kit (virus generator)	Set of tools for generating new viruses automatically.
Spammer programs	Used to send large volumes of unwanted e-mail.
Flooders	Used to attack networked computer systems with a large volume of traffic to carry out a denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.
Zombie, bot	Program activated on an infected machine that is activated to launch attacks on other machines.
Spyware	Software that collects information from a computer and transmits it to another system.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.

A Broad classification of malware

- Can be classified into two broad categories:



- Propagation mechanisms:
  - Include infection of existing executable or interpreted content by viruses that is subsequently spread to other system
  - Exploit of software vulnerabilities either locally or over a network by worms or drive-by-downloads to allow the malware to replicate
  - Social engineering attacks that convince users to bypass security mechanisms to install trojans or to respond to phishing attacks

Broad classification (continued)

- Earlier approaches to malware classification distinguished between:
  - Those that need a host program, being parasitic code such as viruses
  - Those that are independent, self-contained programs run on the system such as worms, trojans, and bots
- Another distinction used was:
  - Malware that does not replicate, such as trojans and spam e-mail
  - Malware that does, including viruses and worms
- Payload actions performed by malware once it reaches a target system can include:
  - Corruption of system or data files
  - Theft of service in order to make the system a zombie agent of attack as part of a botnet
  - Theft of information from the system, especially of logins, passwords, or other personal details by keylogging or spyware programs
  - Stealthing where the malware hides its presence on the system from attempts to detect and block it
- Blended attack
  - Uses multiple methods of infection or propagation to maximize the speed of contagion and the severity of the attack

Attack kits

- Initially the development and deployment of malware required considerable technical skill by software authors
- This changed with the development of virus-creation toolkits in the early 1990s and more general attack kits in the 2000s
  - These toolkits are often known as *crimeware*
  - Include a variety of propagation mechanisms and payload modules that even novices can combine, select, and deploy
  - Can easily be customized with the latest discovered vulnerabilities in order to exploit the window of opportunity between the publication of a weakness and the deployment of patches to close it
  - These kits greatly enlarged the population of attackers able to deploy malware

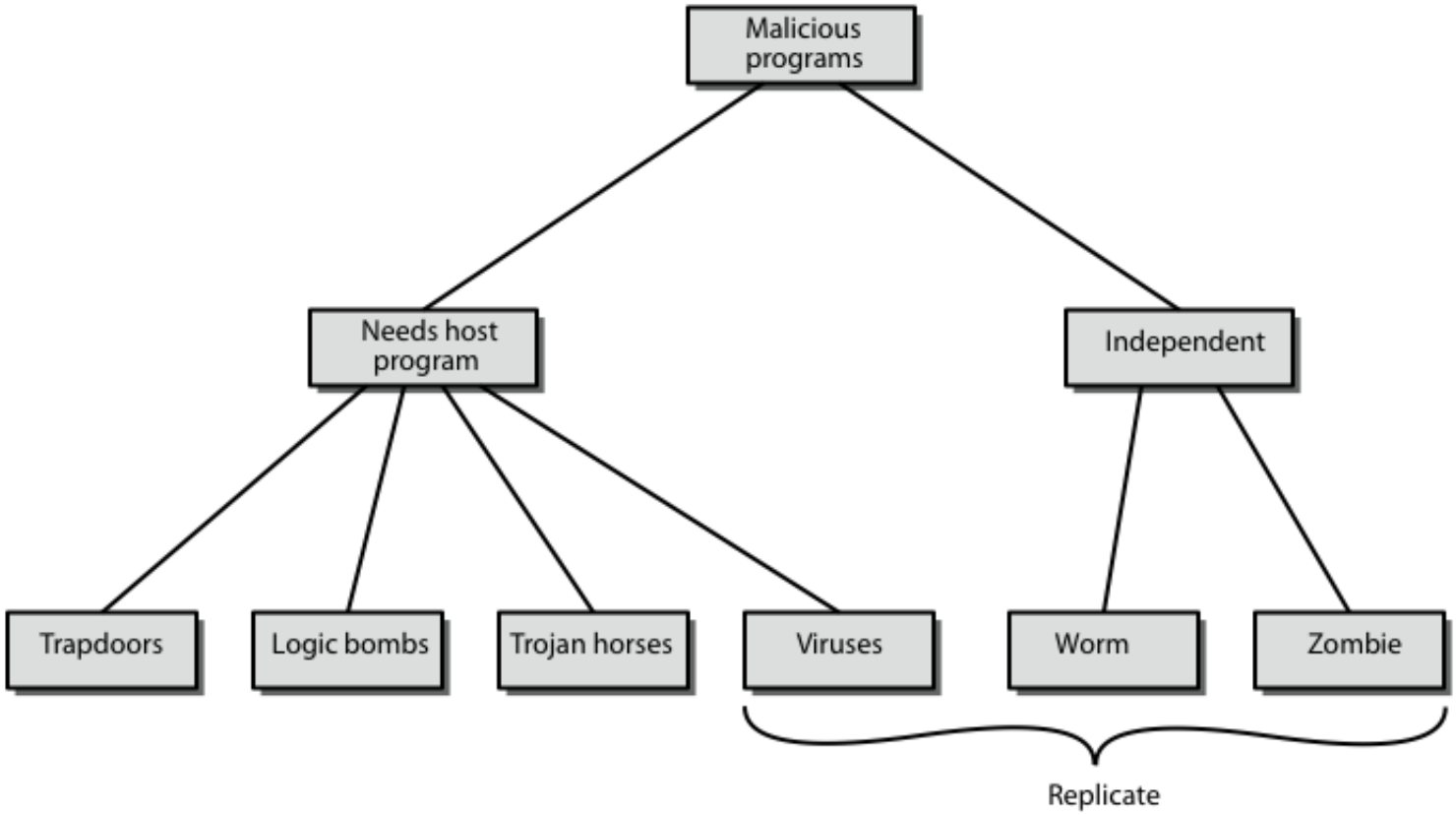
Attack sources

- Another significant malware development over the last couple of decades is the change from attackers being individuals to more organized and dangerous attack sources
  - These include politically motivated attackers, criminals, organized crime, organizations that sell their services to companies and nations, and national government agencies
- This has significantly changed the resources available and motivation behind the rise of malware leading to development of a large underground economy involving the sale of attack kits, access to compromised hosts, and to stolen information

Viruses and Other Malicious Content

- computer viruses have got a lot of publicity
- one of a family of **malicious software**
- effects usually obvious
- have figured in news reports, fiction, movies (often exaggerated)
- getting more attention than deserve
- are a concern though

Malicious Software



Backdoor or Trapdoor

- secret entry point into a program
- allows those who know access bypassing usual security procedures
- have been commonly used by developers
- a threat when left in production programs allowing exploited by attackers
- very hard to block in O/S
- requires good s/w development & update

Logic Bomb

- one of oldest types of malicious software
- code embedded in legitimate program
- activated when specified conditions met
  - eg presence/absence of some file
  - particular date/time
  - particular user
- when triggered typically damage system
  - modify/delete files/disks, halt machine, etc

Trojan Horse

- program with hidden side-effects
- which is usually superficially attractive
  - eg game, s/w upgrade etc
- when run performs some additional tasks
  - allows attacker to indirectly gain access they do not have directly
- often used to propagate a virus/worm or install a backdoor
- or simply to destroy data

Mobile Code

- program/script/macro that runs unchanged
  - on heterogeneous collection of platforms
  - on large homogeneous collection (Windows)
- transmitted from remote system to local system & then executed on local system
- often to inject virus, worm, or Trojan horse
- or to perform own exploits
  - unauthorized data access, root compromise

Multiple-Threat Malware

- malware may operate in multiple ways
- **multipartite** virus infects in multiple ways
  - eg. multiple file types
- **blended** attack uses multiple methods of infection or transmission
  - to maximize speed of contagion and severity
  - may include multiple types of malware
  - eg. Nimda has worm, virus, mobile code
  - can also use IM & P2P

Viruses

- piece of software that infects programs
  - modifying them to include a copy of the virus
  - so it executes secretly when host program is run
- specific to operating system and hardware
  - taking advantage of their details and weaknesses
- a typical virus goes through phases of:
  - dormant
  - propagation
  - triggering
  - execution

Virus Structure

- components:
  - infection mechanism - enables replication
  - trigger - event that makes payload activate
  - payload - what it does, malicious or benign
- prepended / postpended / embedded
- when infected program invoked, executes virus code then original program code
- can block initial infection (difficult)
- or propogation (with access controls)

Virus Classification

- boot sector
- file infector
- macro virus
- encrypted virus
- stealth virus
- polymorphic virus
- metamorphic virus

Macro Virus

- became very common in mid-1990s since
  - platform independent
  - infect documents
  - easily spread
- exploit macro capability of office apps
  - executable program embedded in office doc
  - often a form of Basic
- more recent releases include protection
- recognized by many anti-virus programs

E-Mail Viruses

- more recent development
- e.g. Melissa
  - exploits MS Word macro in attached doc
  - if attachment opened, macro activates
  - sends email to all on users address list
  - and does local damage
- then saw versions triggered reading email
- hence much faster propagation

Virus Countermeasures

- prevention - ideal solution but difficult
- realistically need:
  - detection
  - identification
  - removal
- if detect but can't identify or remove, must discard and replace infected program

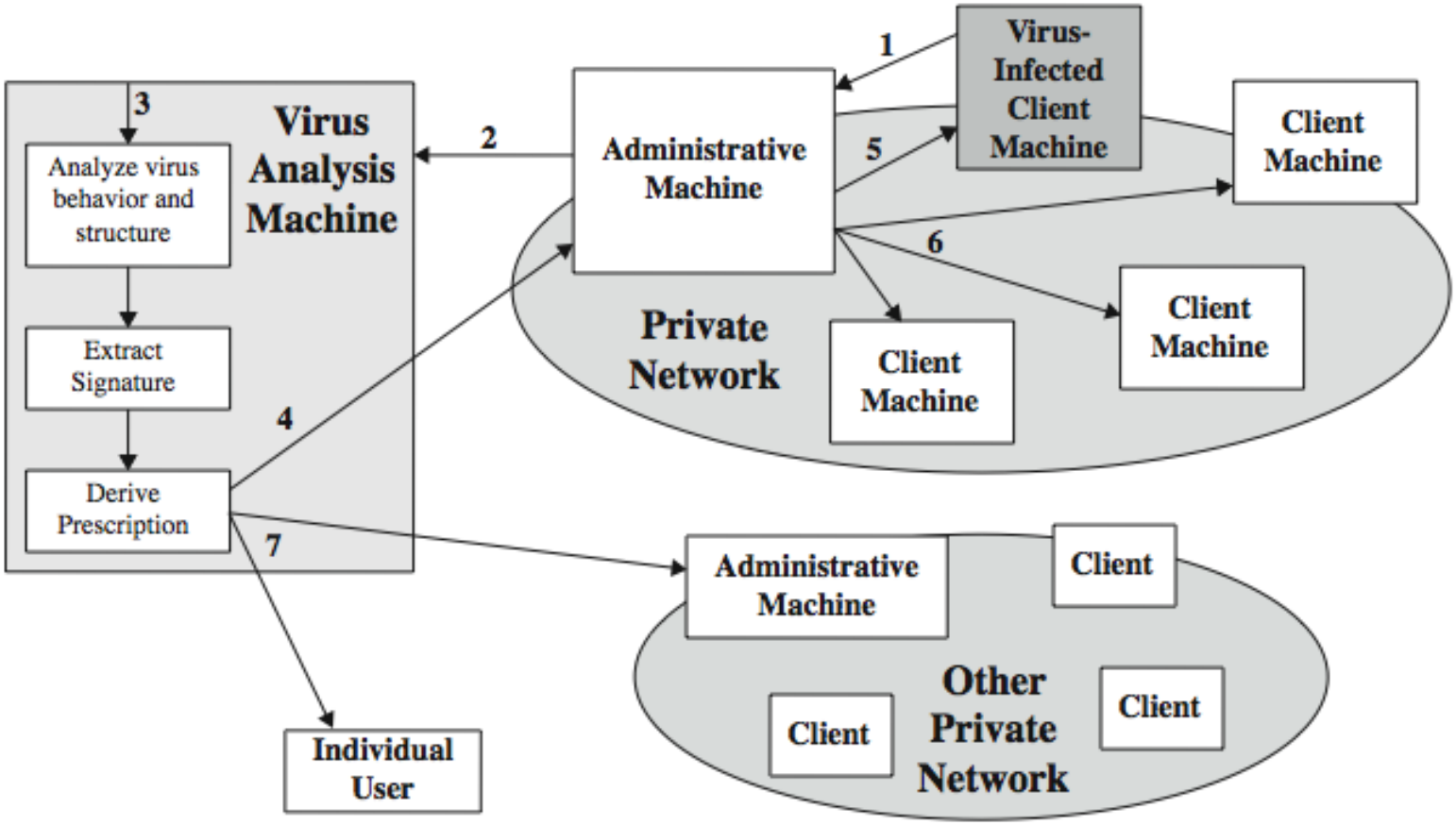
Anti-Virus Evolution

- virus & antivirus tech have both evolved
- early viruses simple code, easily removed
- as become more complex, so must the countermeasures
- generations
  - first - signature scanners
  - second - heuristics
  - third - identify actions
  - fourth - combination packages

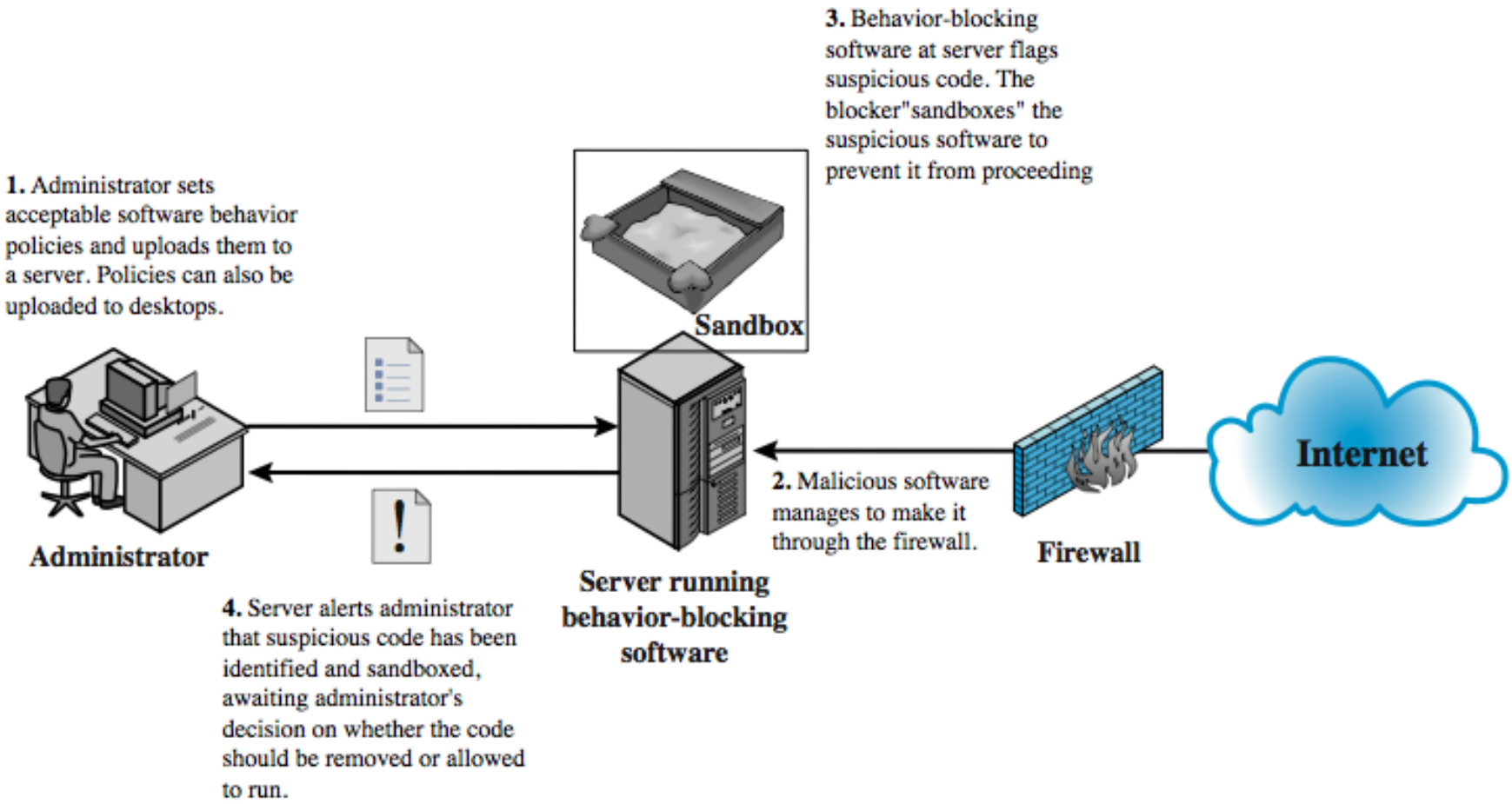
Generic Decryption

- runs executable files through GD scanner:
  - CPU emulator to interpret instructions
  - virus scanner to check known virus signatures
  - emulation control module to manage process
- lets virus decrypt itself in interpreter
- periodically scan for virus signatures
- issue is long to interpret and scan
  - tradeoff chance of detection vs time delay

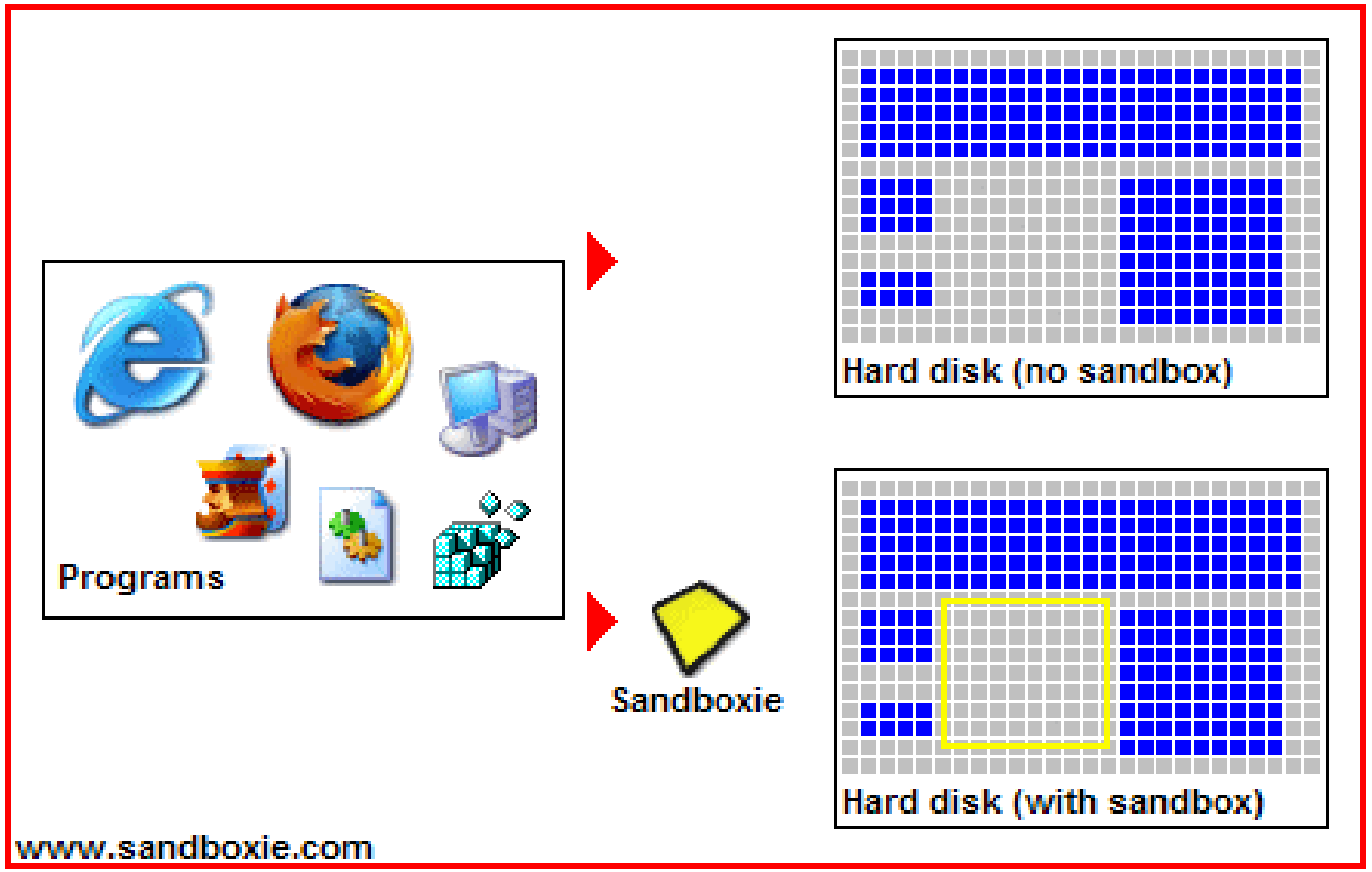
Digital Immune System



Behavior-Blocking Software



Sandboxing


Programs
Sandboxie
Hard disk (no sandbox)
Hard disk (with sandbox)
www.sandboxie.com

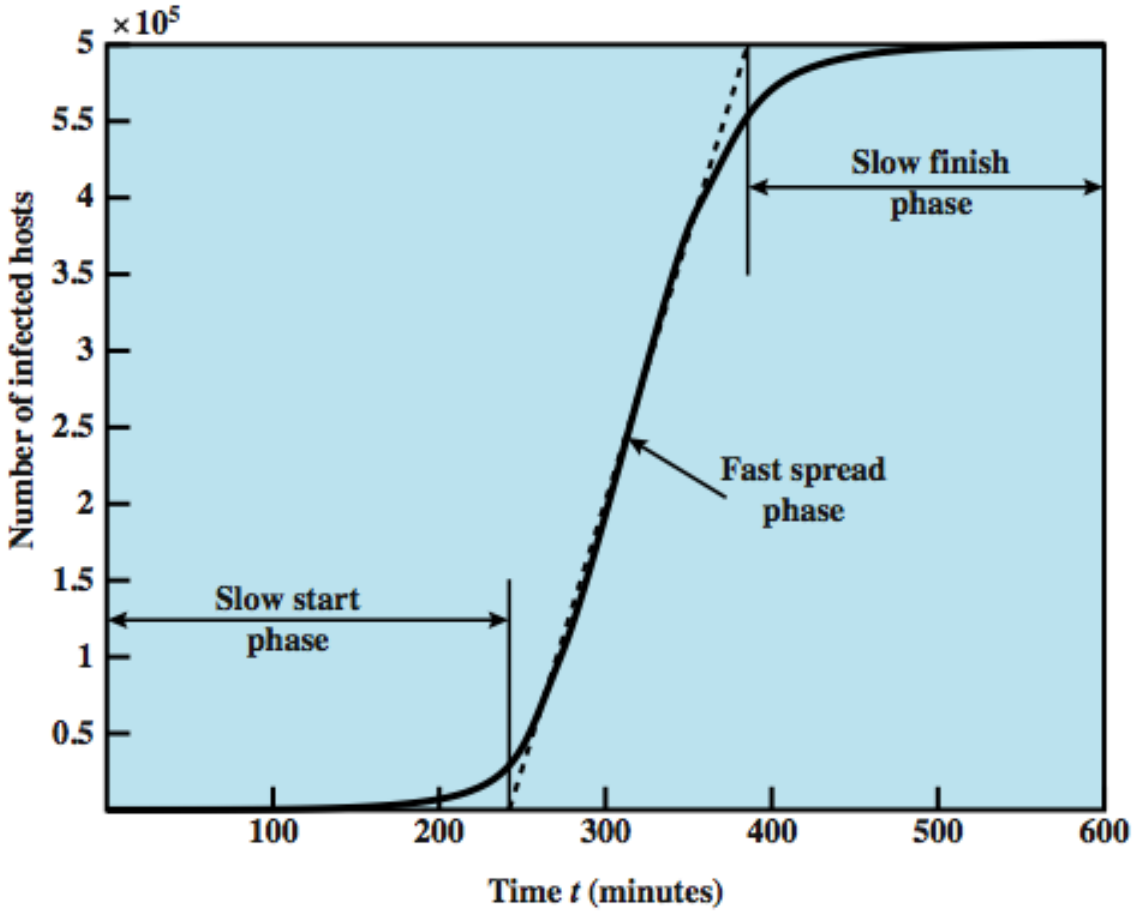
Worms

- replicating program that propagates over net
  - using email, remote exec, remote login
- has phases like a virus:
  - dormant, propagation, triggering, execution
  - propagation phase: searches for other systems, connects to it, copies self to it and runs
- may disguise itself as a system process
- concept seen in Brunner's "Shockwave Rider"
- implemented by Xerox Palo Alto labs in 1980's

Morris Worm

- one of best know worms
- released by Robert Morris in 1988
- various attacks on UNIX systems
  - cracking password file to use login/password to logon to other systems
  - exploiting a bug in the finger protocol
  - exploiting a bug in sendmail
- if succeed have remote shell access
  - sent bootstrap program to copy worm over

Worm Propagation Model



Recent Worm Attacks

- Code Red
  - July 2001 exploiting MS IIS bug
  - probes random IP address, does DDoS attack
- Code Red II variant includes backdoor
- SQL Slammer
  - early 2003, attacks MS SQL Server
- Mydoom
  - mass-mailing e-mail worm that appeared in 2004
  - installed remote access backdoor in infected systems
- Warezov family of worms
  - scan for e-mail addresses, send in attachment

Worm Technology

- multiplatform
- multi-exploit
- ultrafast spreading
- polymorphic
- metamorphic
- transport vehicles
- zero-day exploit

Mobile Phone Worms

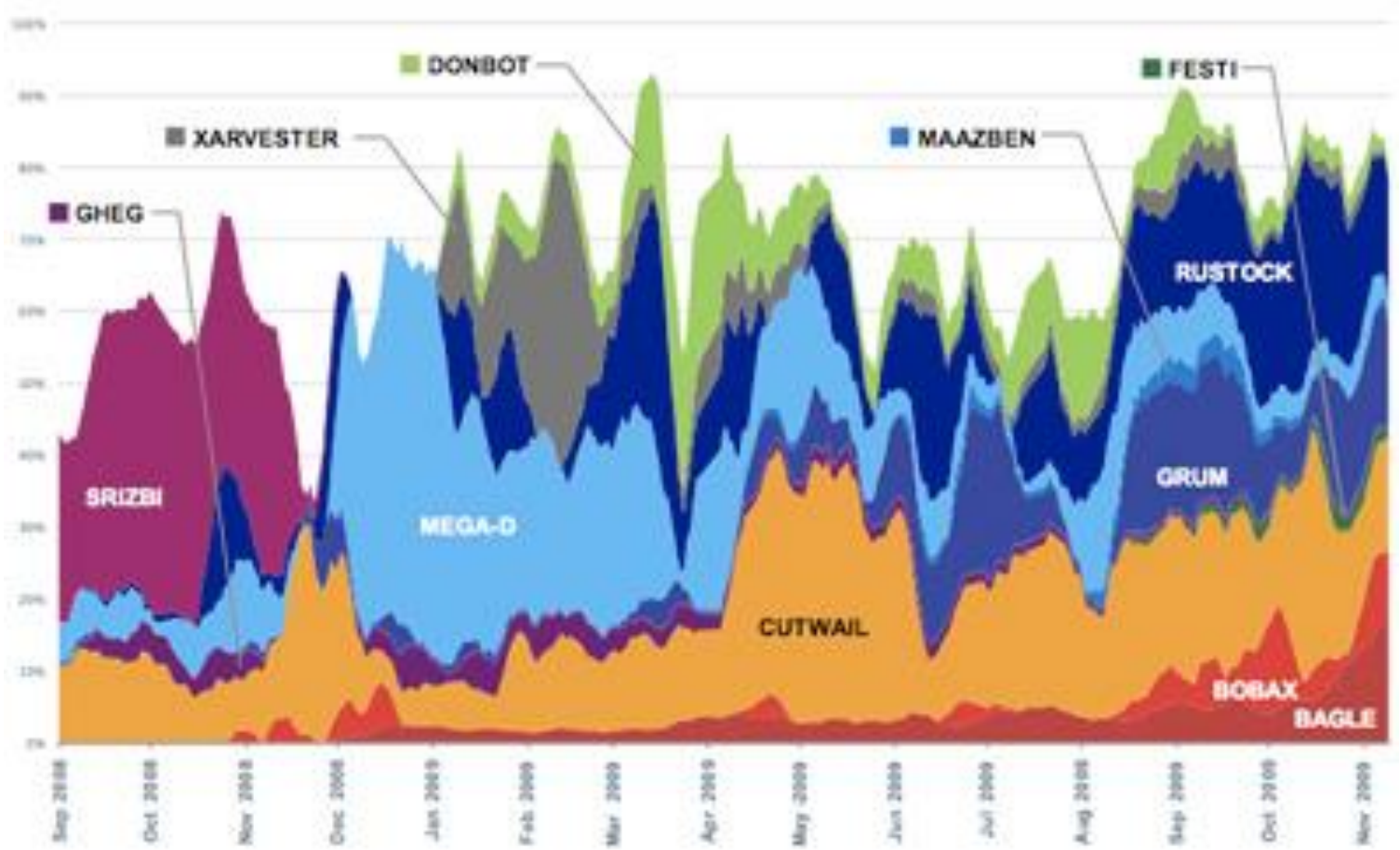
- first appeared on mobile phones in 2004
  - target smartphone which can install s/w
- they communicate via Bluetooth or MMS
- to disable phone, delete data on phone, or send premium-priced messages
- CommWarrior, launched in 2005
  - replicates using Bluetooth to nearby phones
  - and via MMS using address-book numbers

Botnets

- A **botnet** is a collection of internet-connected programs communicating with other similar programs in order to perform tasks. It could be used to send spam email or participate in DDoS attacks. The word botnet stems from the two words robot and network.
- Botnets sometimes comprise computers whose security defenses have been breached and control ceded to a 3rd party. Each such compromised device, known as a "bot", is created when a computer is penetrated by software from a *malware* (malicious software) distribution. The controller of a botnet is able to direct the activities of these compromised computers through communication channels.

Top Botnets

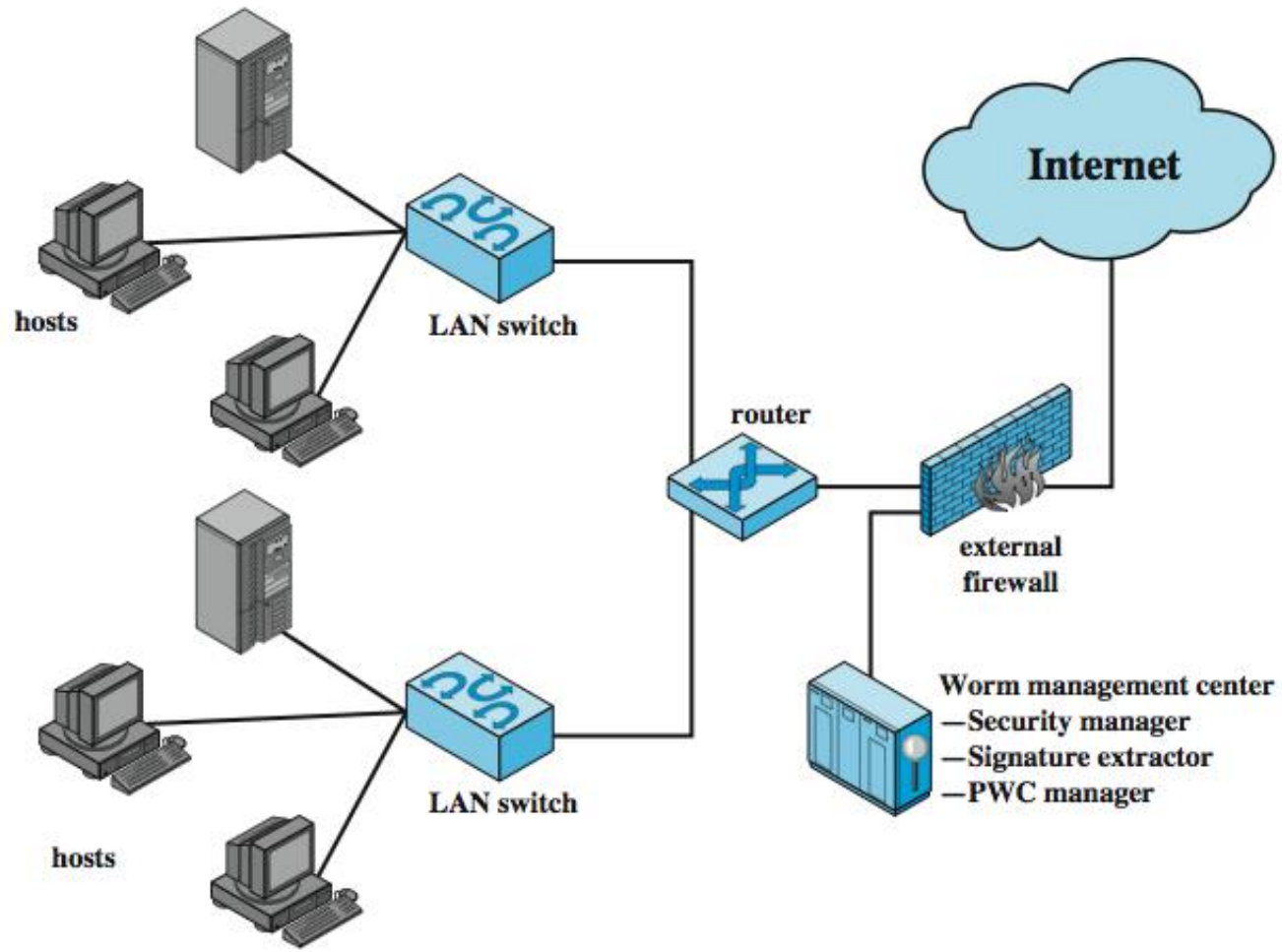
- http://www.net-security.org/



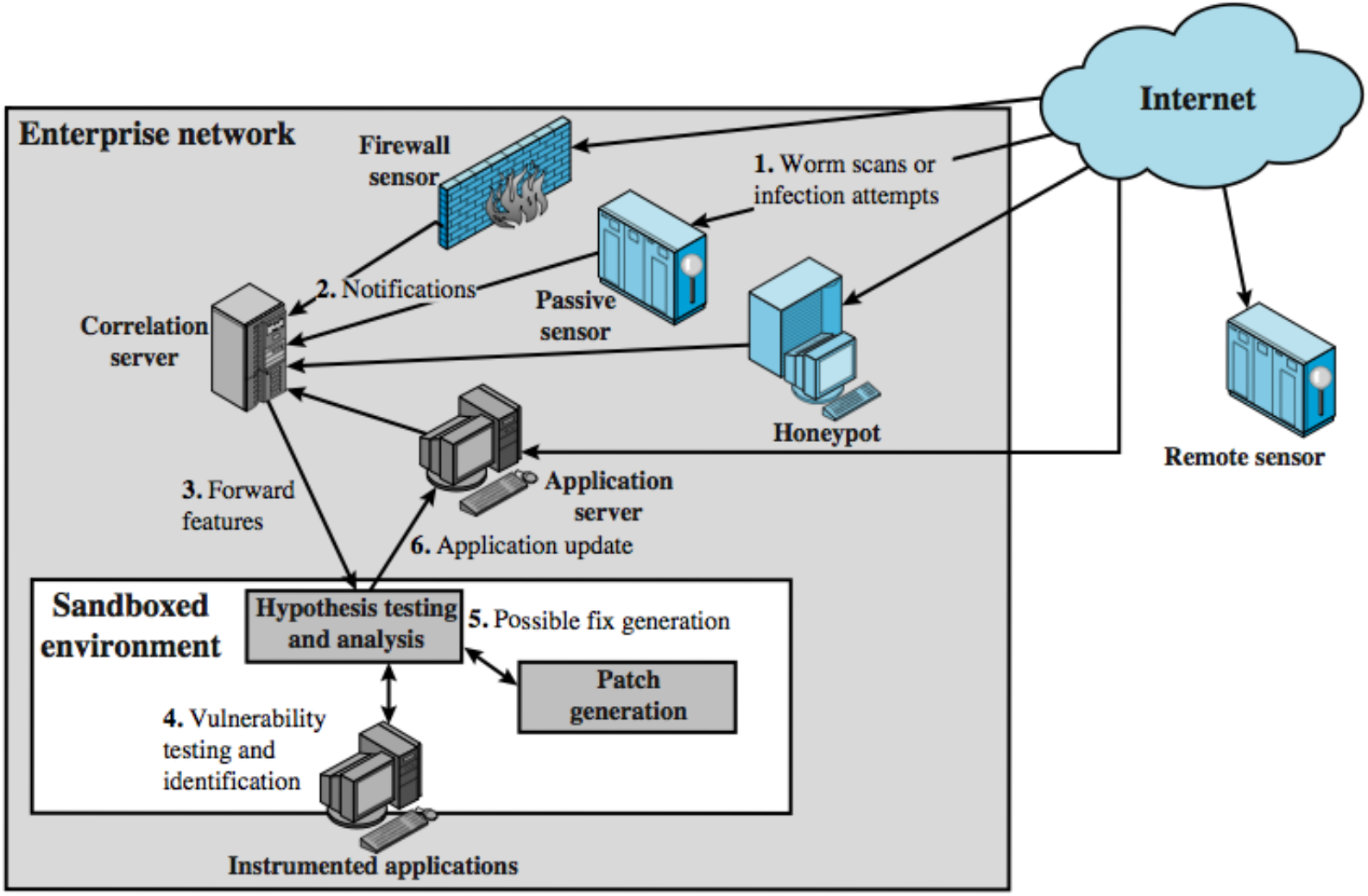
Worm Countermeasures

- overlaps with anti-virus techniques
- once worm on system A/V can detect
- worms also cause significant net activity
- worm defense approaches include:
  - signature-based worm scan filtering
  - filter-based worm containment
  - payload-classification-based worm containment
  - threshold random walk scan detection
  - rate limiting and rate halting

Proactive Worm Containment



Network Based Worm Defense



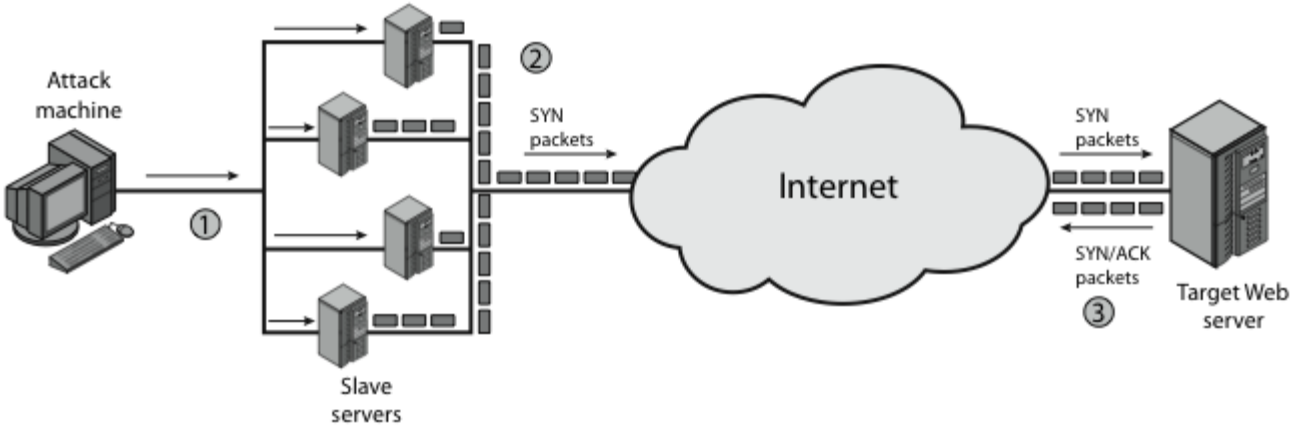
Honeypots Solutions

- Bubblegum Proxypot. An open proxy honeypot for deceiving and detecting spammers.
- Jackpot. An open relay honeypot, also aimed at spammers.
- BackOfficer Friendly: BOF is a free Windows based honeypot can listen on only 7 ports
- Bait-n-Switch. Not really a honeypot. Instead, a technology that directs all non-production or unauthorized traffic to your honeypots
- Bigeye. A low-interaction honeypot that emulates several servcies.
- HoneyWeb. Emulates different types of webservers. Can dynamicaly change itself based on the type of requests.
- Deception Toolkit: DTK was the first OpenSource honeypot, that emulates a variety of listening services. Its primary purpose is to deceive human attackers.
- LaBrea Tarpit: This OpenSource honeypot is unqiue in that it is designed to slow down or stop attacks by acting as a sticky honeypot
- Honeyd: This is a powerful, low-interaction OpenSource honeypot, to monitor millions of unused IPs, IP stack spoofing, and simulate hundreds of operating systems.

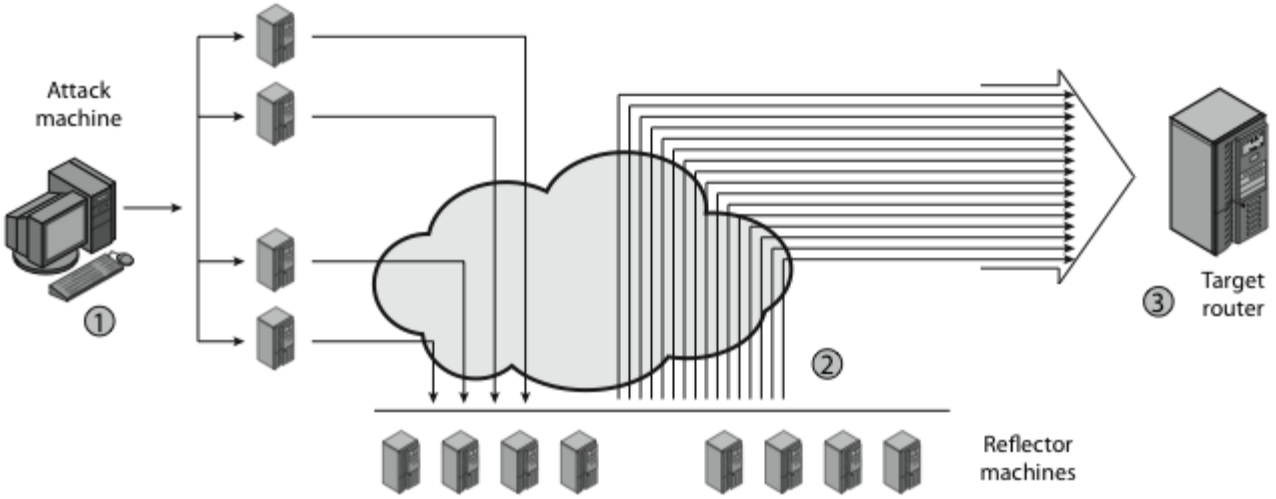
Distributed Denial of Service Attacks (DDoS)

- Distributed Denial of Service (DDoS) attacks form a significant security threat
- making networked systems unavailable
- by flooding with useless traffic
- using large numbers of “zombies”
- growing sophistication of attacks
- defense technologies struggling to cope

Distributed Denial of Service Attacks (DDoS)

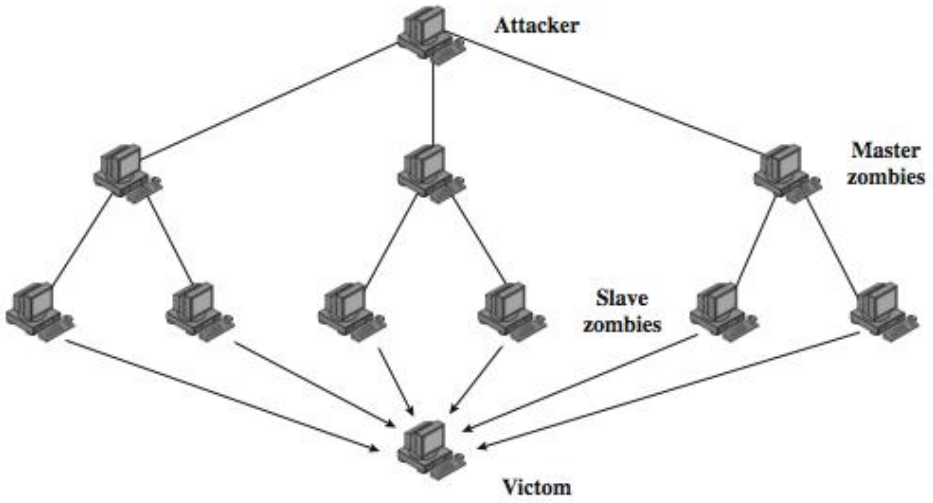


(a) Distributed SYN flood attack

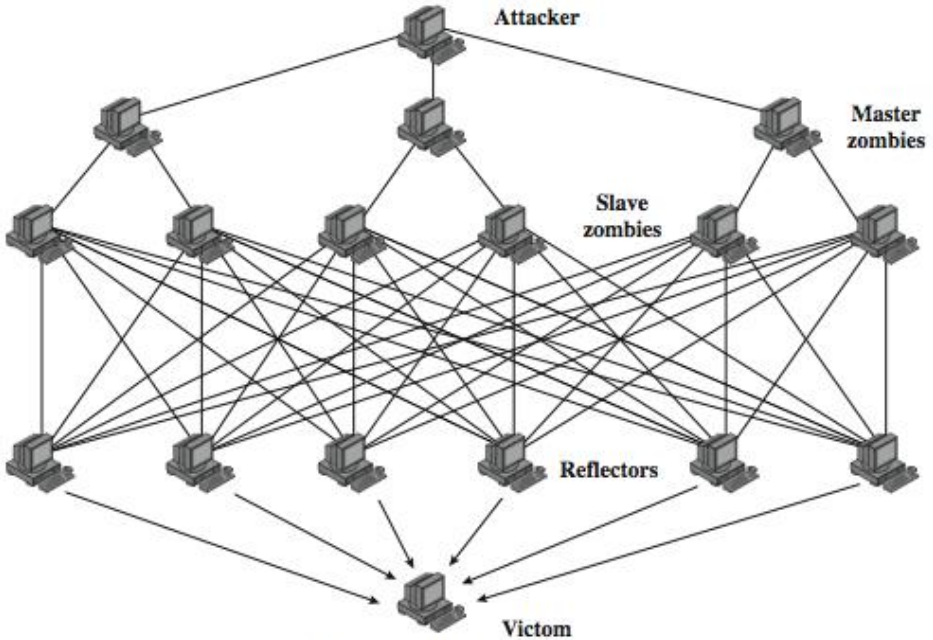


(a) Distributed ICMP attack

DDoS Flood Types



(a) Direct DDoS Attack



(b) Reflector DDoS Attack

Constructing an Attack Network

- must infect large number of zombies
- needs:

1. software to implement the DDoS attack
2. an unpatched vulnerability on many systems
3. scanning strategy to find vulnerable systems
   - random, hit-list, topological, local subnet

DDoS Countermeasures

- three broad lines of defense:
  1. attack prevention & preemption (before)
  2. attack detection & filtering (during)
  3. attack source traceback & ident (after)
- huge range of attack possibilities
- hence evolving countermeasures

Summary

- have considered:
  - various malicious programs
  - trapdoor, logic bomb, trojan horse, zombie
  - viruses
  - worms
  - distributed denial of service attacks