Chapter 6

Malicious Software

Malware

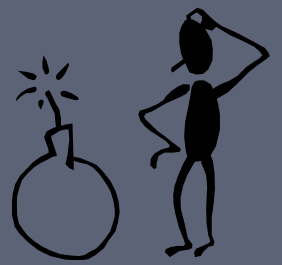
[SOUP13] defines malware as:

"a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim."

Name	Description
Advanced persistent threat	Cybercrime directed at business and political targets, using a wide variety of intrusion technologies and malware, applied persistently and effectively to specific targets over an extended period, often attributed to state-sponsored organizations.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.
Attack Kit	Set of tools for generating new malware automatically using a variety of supplied propagation and payload mechanisms.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Backdoor (trapdoor)	Any mechanisms that bypasses a normal security check; it may allow unauthorized access to functionality in a program, or onto a compromised system.
Downloaders	Code that installs other items on a machine that is under attack. It is normally included in the malware code first inserted on to a compromised system to then import a larger malware package.
Drive-by download	An attack using code in a compromised web site that exploits a browser vulnerability to attack a client system when the site is viewed.
Exploits	Code specific to a single vulnerability or set of vulnerabilities.
Flooders (DoS client)	Used to generate a large volume of data to attack networked computer systems, by carrying out some form of denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Logic bomb	Code inserted into malware by an intruder. A logic bomb lies dormant until a predefined condition is met; the code then triggers an unauthorized act.
Macro Virus	A type of virus that uses macro or scripting code, typically embedded in a document, and triggered when the document is viewed or edited, to run and replicate itself into other such documents.
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.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.
Spammer Programs	Used to send large volumes of unwanted e-mail.
Spyware	Software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data and/or network traffic; or by scanning files on the system for sensitive information.
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.
Virus	Malware that, when executed, tries to replicate itself into other executable machine or script 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, usually by exploiting software vulnerabilities in the target system.
Zombie, bot	Program activated on an infected machine that is activated to launch attacks on other machines.

Table 6.1 Malware Terminology

(Table can be found on page 201 in the textbook.)



Classification of Malware

Classified into two broad categories:

- Based first on how it spreads or propagates to reach the desired targets
- Then on the actions or payloads it performs once a target is reached

Also classified by:

- Those that need a host program (parasitic code such as viruses)
- Those that are independent, self-contained programs (worms, trojans, and bots)
- Malware that does not replicate (trojans and spam e-mail)
- Malware that does replicate (viruses and worms)

Types of Malicious Software (Malware)

Propagation mechanisms include:

- Infection of existing content by viruses that is subsequently spread to other systems
- Exploit of software vulnerabilities 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

Payload actions performed by malware once it reaches a target system can include:

- Corruption of system or data files
- Theft of service/make the system a zombie agent of attack as part of a botnet
- Theft of information from the system/keylogging
- Stealthing/hiding its presence on the system

Attack Kits

- Initially the development and deployment of malware required considerable technical skill by software authors
  - The development of virus-creation toolkits in the early 1990s and then more general attack kits in the 2000s greatly assisted in the development and deployment of malware
- Toolkits are often known as "crimeware"
  - Include a variety of propagation mechanisms and payload modules that even novices can deploy
  - Variants that can be generated by attackers using these toolkits creates a significant problem for those defending systems against them
- Widely used toolkits include:
  - Zeus
  - Blackhole
  - Sakura
  - Phoenix

Attack Sources

- Another significant malware development is the change from attackers being individuals often motivated to demonstrate their technical competence to their peers to more organized and dangerous attack sources such as:

- This has significantly changed the resources available and motivation behind the rise of malware and has led to development of a large underground economy involving the sale of attack kits, access to compromised hosts, and to stolen information

Advanced Persistent Threats (APTs)

- Well-resourced, persistent application of a wide variety of intrusion technologies and malware to selected targets (usually business or political)
- Typically attributed to state-sponsored organizations and criminal enterprises
- Differ from other types of attack by their careful target selection and stealthy intrusion efforts over extended periods
- High profile attacks include Aurora, RSA, APT1, and Stuxnet

APT Characteristics

Advanced

- Used by the attackers of a wide variety of intrusion technologies and malware including the development of custom malware if required
- The individual components may not necessarily be technically advanced but are carefully selected to suit the chosen target

Persistent

- Determined application of the attacks over an extended period against the chosen target in order to maximize the chance of success
- A variety of attacks may be progressively applied until the target is compromised

Threats

- Threats to the selected targets as a result of the organized, capable, and well-funded attackers intent to compromise the specifically chosen targets
- The active involvement of people in the process greatly raises the threat level from that due to automated attacks tools, and also the likelihood of successful attacks

APT Attacks

- Aim:
  - Varies from theft of intellectual property or security and infrastructure related data to the physical disruption of infrastructure
- Techniques used:
  - Social engineering
  - Spear-phishing email
  - Drive-by-downloads from selected compromised websites likely to be visited by personnel in the target organization
- Intent:
  - To infect the target with sophisticated malware with multiple propagation mechanisms and payloads
  - Once they have gained initial access to systems in the target organization a further range of attack tools are used to maintain and extend their access

Viruses

- Piece of software that infects programs
  - Modifies them to include a copy of the virus
  - Replicates and goes on to infect other content
  - Easily spread through network environments
- When attached to an executable program a virus can do anything that the program is permitted to do
  - Executes secretly when the host program is run
- Specific to operating system and hardware
  - Takes advantage of their details and weaknesses

Virus Components

Infection mechanism

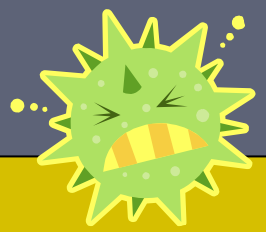
- Means by which a virus spreads or propagates
- Also referred to as the *infection vector*

Trigger

- Event or condition that determines when the payload is activated or delivered
- Sometimes known as a *logic bomb*

Payload

- What the virus does (besides spreading)
- May involve damage or benign but noticeable activity



Virus Phases

Dormant phase

Virus is idle	Will eventually be activated by some event	Not all viruses have this stage

Triggering phase

Virus is activated to perform the function for which it was intended	Can be caused by a variety of system events

Propagation phase

Virus places a copy of itself into other programs or into certain system areas on the disk	May not be identical to the propagating version	Each infected program will now contain a clone of the virus which will itself enter a propagation phase

Execution phase

Function is performed	May be harmless or damaging

Virus Structure

```
program V
1234567;

procedure attach-to-program;
begin
   repeat
        file := get-random-program;
   until first-program-line ≠ 1234567;
   prepend V to file;
end;

procedure execute-payload;
begin
   (* perform payload actions *)
end;

procedure trigger-condition;
begin
   (* return true if trigger condition is true *)
end;

begin (* main action block *)
   attach-to-program;
   if trigger-condition then execute-payload;
   goto main;
end;
```

(a) A simple virus

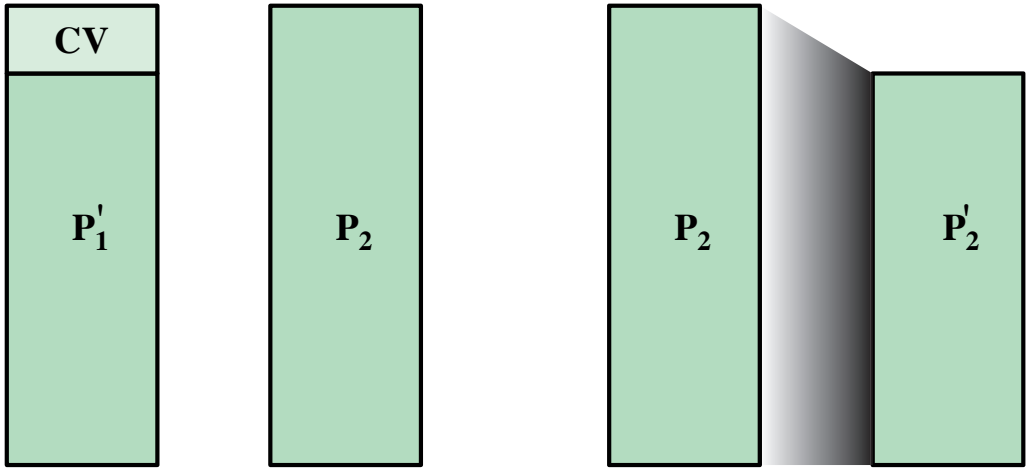
```
program CV
1234567;

procedure attach-to-program;
begin
   repeat
        file := get-random-program;
   until first-program-line ≠ 1234567;
   compress file;    (* t1 *)
   prepend CV to file;   (* t2 *)
end;

begin (* main action block *)
   attach-to-program;
   uncompress rest of this file into tempfile;   (* t3 *)
   execute tempfile;   (* t4 *)
end;
```

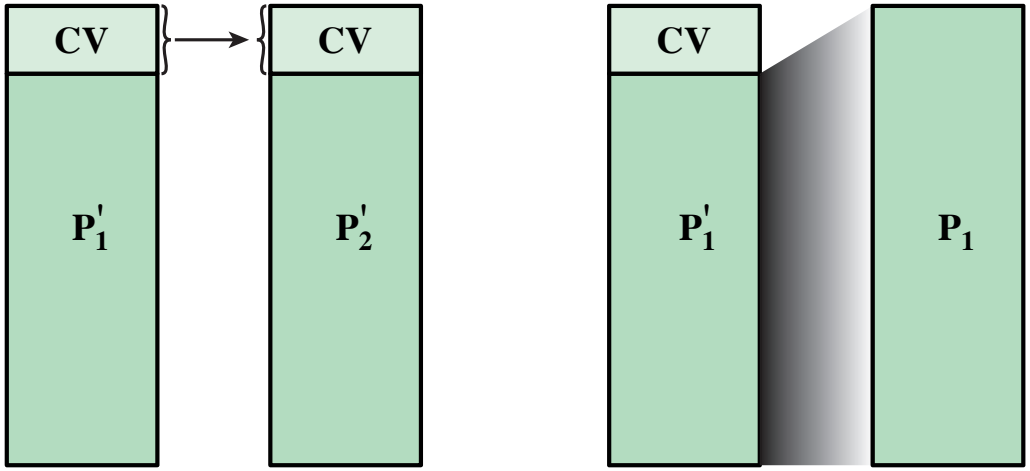
(b) A compression virus

Figure 6.1 Example Virus Logic



t_0: P_1' is infected version of P_1; P_2 is clean

t_1: P_2 is compressed into P_2'



t_2: CV attaches itself to P_2'

t_3: P_1' is decompressed into the original program P_1

Figure 6.2 A Compression Virus

Virus Classifications

Classification by target

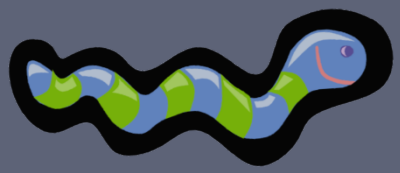
- Boot sector infector
  - Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus
- File infector
  - Infects files that the operating system or shell considers to be executable
- Macro virus
  - Infects files with macro or scripting code that is interpreted by an application
- Multipartite virus
  - Infects files in multiple ways

Classification by concealment strategy

- Encrypted virus
  - A portion of the virus creates a random encryption key and encrypts the remainder of the virus
- Stealth virus
  - A form of virus explicitly designed to hide itself from detection by anti-virus software
- Polymorphic virus
  - A virus that mutates with every infection
- Metamorphic virus
  - A virus that mutates and rewrites itself completely at each iteration and may change behavior as well as appearance

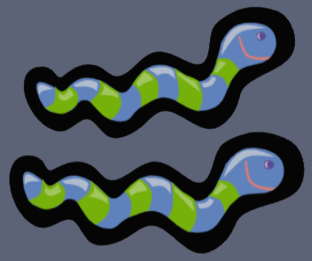
Macro and Scripting Viruses

- Very common in mid-1990s
  - Platform independent
  - Infect documents (not executable portions of code)
  - Easily spread
- Exploit macro capability of MS Office applications
  - More recent releases of products include protection
- Various anti-virus programs have been developed so these are no longer the predominant virus threat



Worms

- Program that actively seeks out more machines to infect and each infected machine serves as an automated launching pad for attacks on other machines
- Exploits software vulnerabilities in client or server programs
- Can use network connections to spread from system to system
- Spreads through shared media (USB drives, CD, DVD data disks)
- E-mail worms spread in macro or script code included in attachments and instant messenger file transfers
- Upon activation the worm may replicate and propagate again
- Usually carries some form of payload
- First known implementation was done in Xerox Palo Alto Labs in the early 1980s



Worm Replication

Electronic mail or instant messenger facility	• Worm e-mails a copy of itself to other systems • Sends itself as an attachment via an instant message service
File sharing	• Creates a copy of itself or infects a file as a virus on removable media
Remote execution capability	• Worm executes a copy of itself on another system
Remote file access or transfer capability	• Worm uses a remote file access or transfer service to copy itself from one system to the other
Remote login capability	• Worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other

Target Discovery

- Scanning (or fingerprinting)
  - First function in the propagation phase for a network worm
  - Searches for other systems to infect

Scanning strategies that a worm can use:

- Random
  - Each compromised host probes random addresses in the IP address space using a different seed
  - This produces a high volume of Internet traffic which may cause generalized disruption even before the actual attack is launched
- Hit-list
  - The attacker first compiles a long list of potential vulnerable machines
  - Once the list is compiled the attacker begins infecting machines on the list
  - Each infected machine is provided with a portion of the list to scan
  - This results in a very short scanning period which may make it difficult to detect that infection is taking place
- Topological
  - This method uses information contained on an infected victim machine to find more hosts to scan
- Local subnet
  - If a host can be infected behind a firewall that host then looks for targets in its own local network
  - The host uses the subnet address structure to find other hosts that would otherwise be protected by the firewall

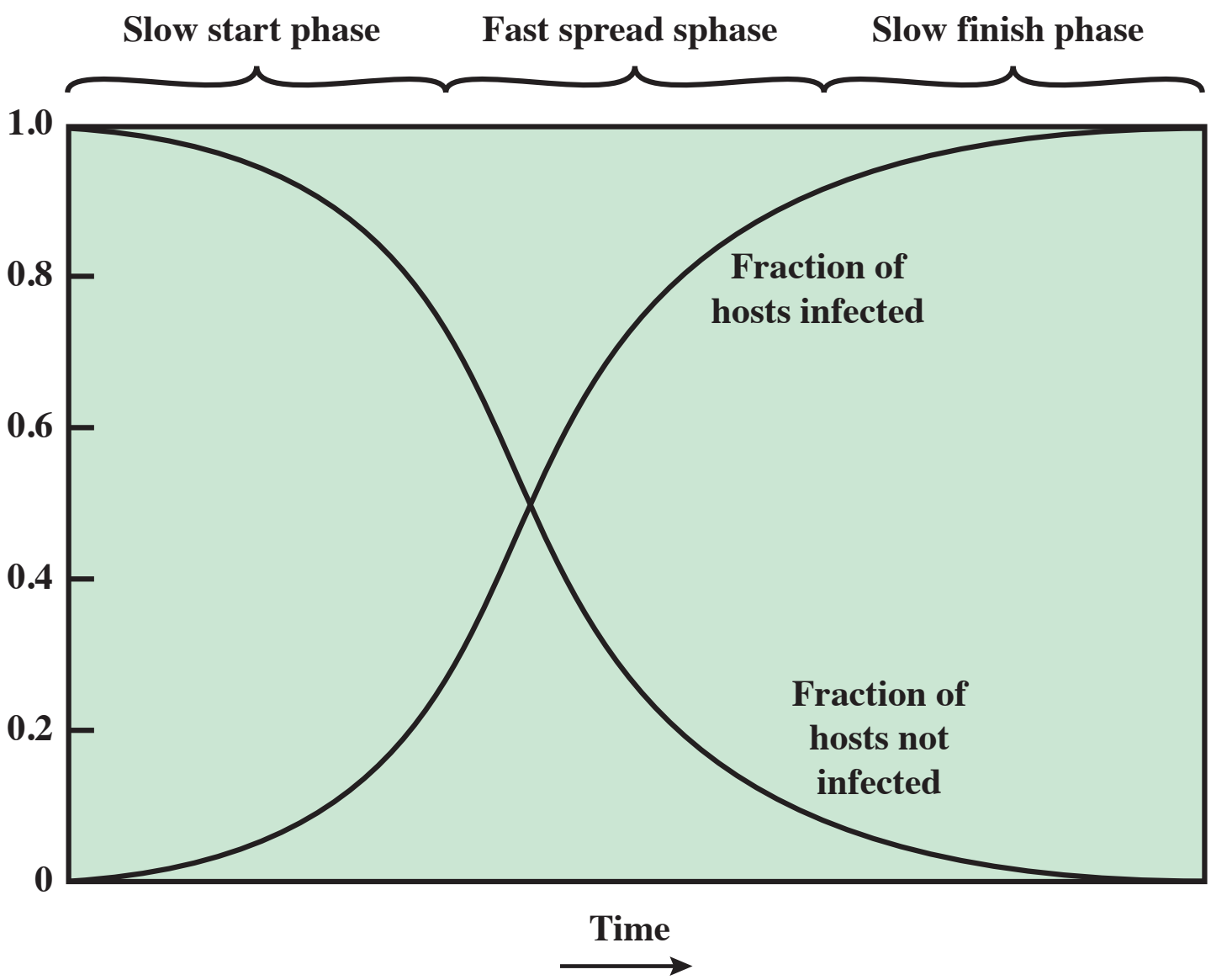
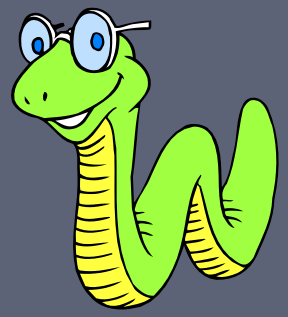


Figure 6.3 Worm Propagation Model

Morris Worm



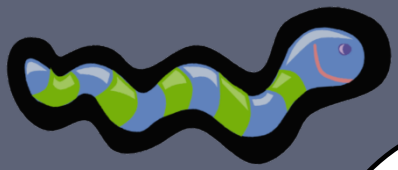
- Earliest significant worm infection
- Released by Robert Morris in 1988
- Designed to spread on UNIX systems
  - Attempted to crack local password file to use login/password to logon to other systems
  - Exploited a bug in the finger protocol which reports the whereabouts of a remote user
  - Exploited a trapdoor in the debug option of the remote process that receives and sends mail
- Successful attacks achieved communication with the operating system command interpreter
  - Sent interpreter a bootstrap program to copy worm over

Recent Worm Attacks

Melissa	1998	e-mail worm first to include virus, worm and Trojan in one package
Code Red	July 2001	exploited Microsoft IIS bug probes random IP addresses consumes significant Internet capacity when active
Code Red II	August 2001	also targeted Microsoft IIS installs a backdoor for access
Nimda	September 2001	had worm, virus and mobile code characteristics spread using e-mail, Windows shares, Web servers, Web clients, backdoors
SQL Slammer	Early 2003	exploited a buffer overflow vulnerability in SQL server compact and spread rapidly
Sobig.F	Late 2003	exploited open proxy servers to turn infected machines into spam engines
Mydoom	2004	mass-mailing e-mail worm installed a backdoor in infected machines
Warezov	2006	creates executables in system directories sends itself as an e-mail attachment can disable security related products
Conficker (Downadup)	November 2008	exploits a Windows buffer overflow vulnerability most widespread infection since SQL Slammer
Stuxnet	2010	restricted rate of spread to reduce chance of detection targeted industrial control systems

Worm Propagation

- It took the Brain virus month to infect a few thousand computers in 1986.
- It took three days for Melissa to infect over 100,000 computers in 1998.
- Code Red infected nearly 360,000 servers in 14 hours in 2001.
- The Slammer was extremely compact and spread rapidly, infecting 90% of vulnerable hosts within 10 minutes in 2003.
- Sobig.F reportedly accounted for one in every 17 messages and produced more than one million copies of itself within the first 24 hours in 2003.
- Mydoom replicated up to 1,000 times per minute and reportedly flooded the Internet with 100 million infected messages in 36 hours in 2004.
- Conficker estimated number of infections ranged from almost 9 million to 15 million in 2009 (source: wikipedia).



Worm Technology

- Multiplatform
- Multi-exploit
- Ultrafast spreading
- Polymorphic
- Metamorphic

Mobile Code

- Programs that can be shipped unchanged to a variety of platforms
- Transmitted from a remote system to a local system and then executed on the local system
- Often acts as a mechanism for a virus, worm, or Trojan horse
- Takes advantage of vulnerabilities to perform its own exploits
- Popular vehicles include Java applets, ActiveX, JavaScript and VBScript

Mobile Phone Worms

- First discovery was Cabir worm in 2004
- Then Lasco and CommWarrior in 2005
- Communicate through Bluetooth wireless connections or MMS
- Target is the smartphone
- Can completely disable the phone, delete data on the phone, or force the device to send costly messages
- CommWarrior replicates by means of Bluetooth to other phones, sends itself as an MMS file to contacts and as an auto reply to incoming text messages

Drive-By-Downloads

- Exploits browser vulnerabilities to download and installs malware on the system when the user views a Web page controlled by the attacker
- In most cases does not actively propagate
- Spreads when users visit the malicious Web page

Clickjacking

- Also known as a user-interface (UI) redress attack
- Using a similar technique, keystrokes can also be hijacked
  - A user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker
- https://youtu.be/gCLU7YUXUAY

- Vulnerability used by an attacker to collect an infected user's clicks
  - The attacker can force the user to do a variety of things from adjusting the user's computer setters to unwittingly sending the user to Web sites that might have malicious code
  - By taking advantage of Adobe Flash or JavaScript an attacker could even place a button under or over a legitimate button making it difficult for users to detect
  - A typical attack uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page
  - The attacker is hijacking clicks meant for one page and routing them to another page

Social Engineering

- "Tricking" users to assist in the compromise of their own systems

Spam

- Unsolicited bulk e-mail
- Significant carrier of malware
- Used for phishing attacks

Trojan horse

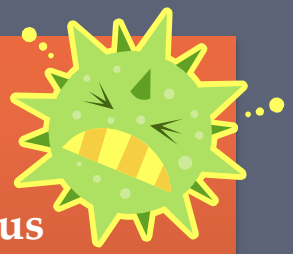
- Program or utility containing harmful hidden code
- Used to accomplish functions that the attacker could not accomplish directly

Mobile phone trojans

- First appeared in 2004 (Skuller)
- Target is the smartphone

Payload
System Corruption

Chernobyl virus



- First seen in 1998
- Windows 95 and 98 virus
- Infects executable files and corrupts the entire file system when a trigger date is reached

Klez

- Mass mailing worm infecting Windows 95 to XP systems
- On trigger date causes files on the hard drive to become empty

Ransomware

- Encrypts the user's data and demands payment in order to access the key needed to recover the information
- PC Cyborg Trojan (1989)
- Gpcode Trojan (2006

Payload
System Corruption

- Real-world damage
  - Causes damage to physical equipment
    - Chernobyl virus rewrites BIOS code
  - Stuxnet worm
    - Targets specific industrial control system software
  - There are concerns about using sophisticated targeted malware for industrial sabotage
- Logic bomb
  - Code embedded in the malware that is set to "explode" when certain conditions are met

Payload – Attack Agents Bots

- Takes over another Internet attached computer and uses that computer to launch or manage attacks
- *Botnet* - collection of bots capable of acting in a coordinated manner
- Uses:
  - Distributed denial-of-service (DDoS) attacks
  - Spamming
  - Sniffing traffic
  - Keylogging
  - Spreading new malware
  - Installing advertisement add-ons and browser helper objects (BHOs)
  - Attacking IRC chat networks
  - Manipulating online polls/games

Remote Control Facility

- Distinguishes a bot from a worm
  - Worm propagates itself and activates itself
  - Bot is initially controlled from some central facility
- Typical means of implementing the remote control facility is on an IRC server
  - Bots join a specific channel on this server and treat incoming messages as commands
  - More recent botnets use covert communication channels via protocols such as HTTP
  - Distributed control mechanisms use peer-to-peer protocols to avoid a single point of failure

Payload – Information Theft Keyloggers and Spyware

Keylogger

- Captures keystrokes to allow attacker to monitor sensitive information
- Typically uses some form of filtering mechanism that only returns information close to keywords ("login", "password")

Spyware

- Subverts the compromised machine to allow monitoring of a wide range of activity on the system
  - Monitoring history and content of browsing activity
  - Redirecting certain Web page requests to fake sites
  - Dynamically modifying data exchanged between the browser and certain Web sites of interest

Payload – Information Theft Phishing

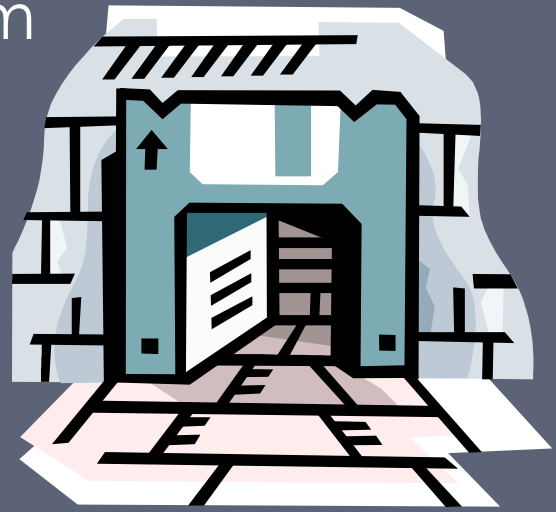
- Exploits social engineering to leverage the user's trust by masquerading as communication from a trusted source
  - Include a URL in a spam e-mail that links to a fake Web site that mimics the login page of a banking, gaming, or similar site
  - Suggests that urgent action is required by the user to authenticate their account
  - Attacker exploits the account using the captured credentials
- Spear-phishing
  - Recipients are carefully researched by the attacker
  - E-mail is crafted to specifically suit its recipient, often quoting a range of information to convince them of its authenticity

Worm Countermeasures

- Considerable overlap in techniques for dealing with viruses and worms
- Once a worm is resident on a machine anti-virus software can be used to detect and possibly remove it
- Perimeter network activity and usage monitoring can form the basis of a worm defense
- Worm defense approaches include:
  - Signature-based worm scan filtering
  - Filter-based worm containment
  - Payload-classification-based worm containment
  - Threshold random walk (TRW) scan detection
  - Rate limiting
  - Rate halting

Payload – Stealthing Backdoor

- Also known as a *trapdoor*
- Secret entry point into a program allowing the attacker to gain access and bypass the security access procedures
- *Maintenance hook* is a backdoor used by Programmers to debug and test programs
- Difficult to implement operating system controls for backdoors in applications

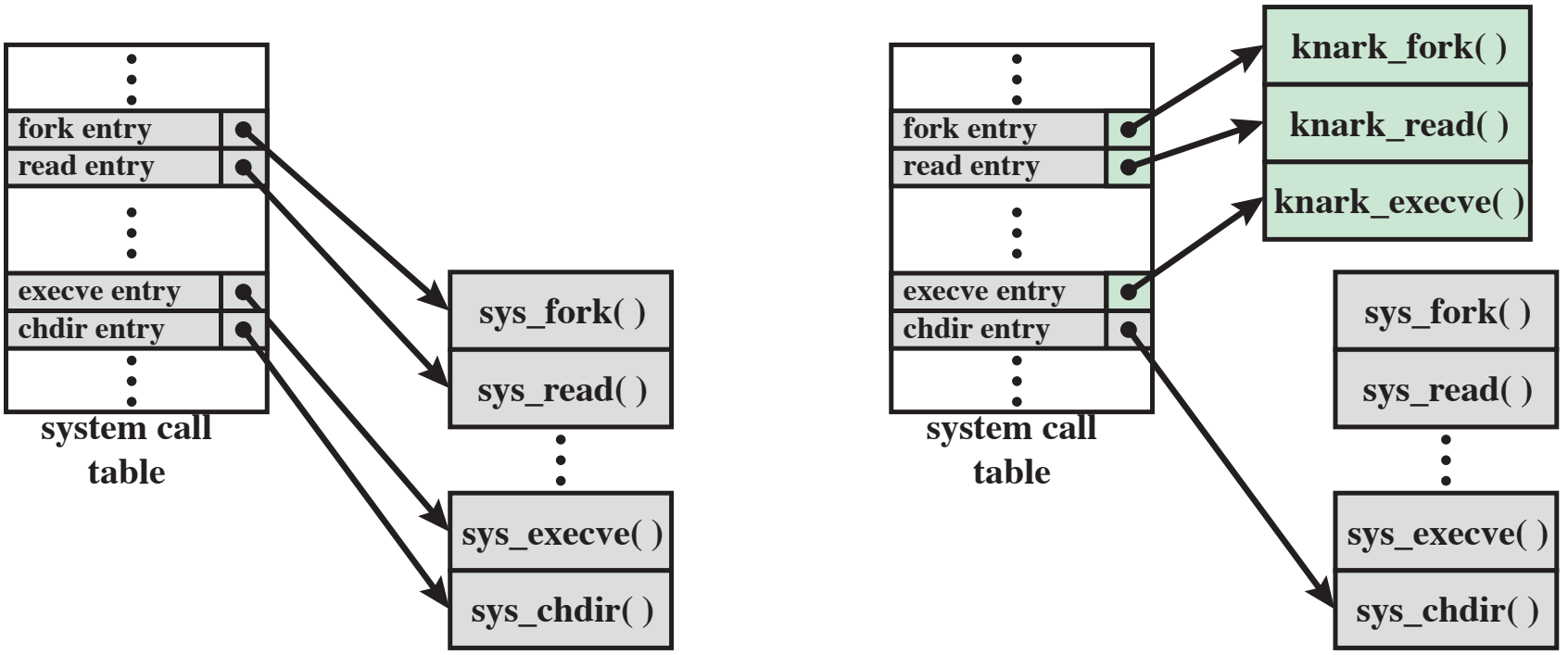


Payload - Stealthing Rootkit

- Set of hidden programs installed on a system to maintain covert access to that system
- Hides by subverting the mechanisms that monitor and report on the processes, files, and registries on a computer
- Gives administrator (or root) privileges to attacker
    - Can add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand

Rootkit Classification Characteristics

Persistent	Memory based	User mode
Kernel mode	Virtual machine based	External mode



(a) Normal kernel memory layout

(b) After nkark install

Figure 6.4 System Call Table Modification by Rootkit

Malware Countermeasure Approaches

- Ideal solution to the threat of malware is prevention

Four main elements of prevention:

- Policy
- Awareness
- Vulnerability mitigation
- Threat mitigation

- If prevention fails, technical mechanisms can be used to support the following threat mitigation options:
  - Detection
  - Identification
  - Removal

Generations of Anti-Virus Software

First generation: simple scanners

- Requires a malware signature to identify the malware
- Limited to the detection of known malware

Second generation: heuristic scanners

- Uses heuristic rules to search for probable malware instances
- Another approach is integrity checking

Third generation: activity traps

- Memory-resident programs that identify malware by its actions rather than its structure in an infected program

Fourth generation: full-featured protection

- Packages consisting of a variety of anti-virus techniques used in conjunction
- Include scanning and activity trap components and access control capability

Generic Decryption (GD)

- Enables the anti-virus program to easily detect complex polymorphic viruses and other malware while maintaining fast scanning speeds
- Executable files are run through a GD scanner which contains the following elements:
  - CPU emulator
  - Virus signature scanner
  - Emulation control module
- The most difficult design issue with a GD scanner is to determine how long to run each interpretation

Host-Based Behavior-Blocking Software

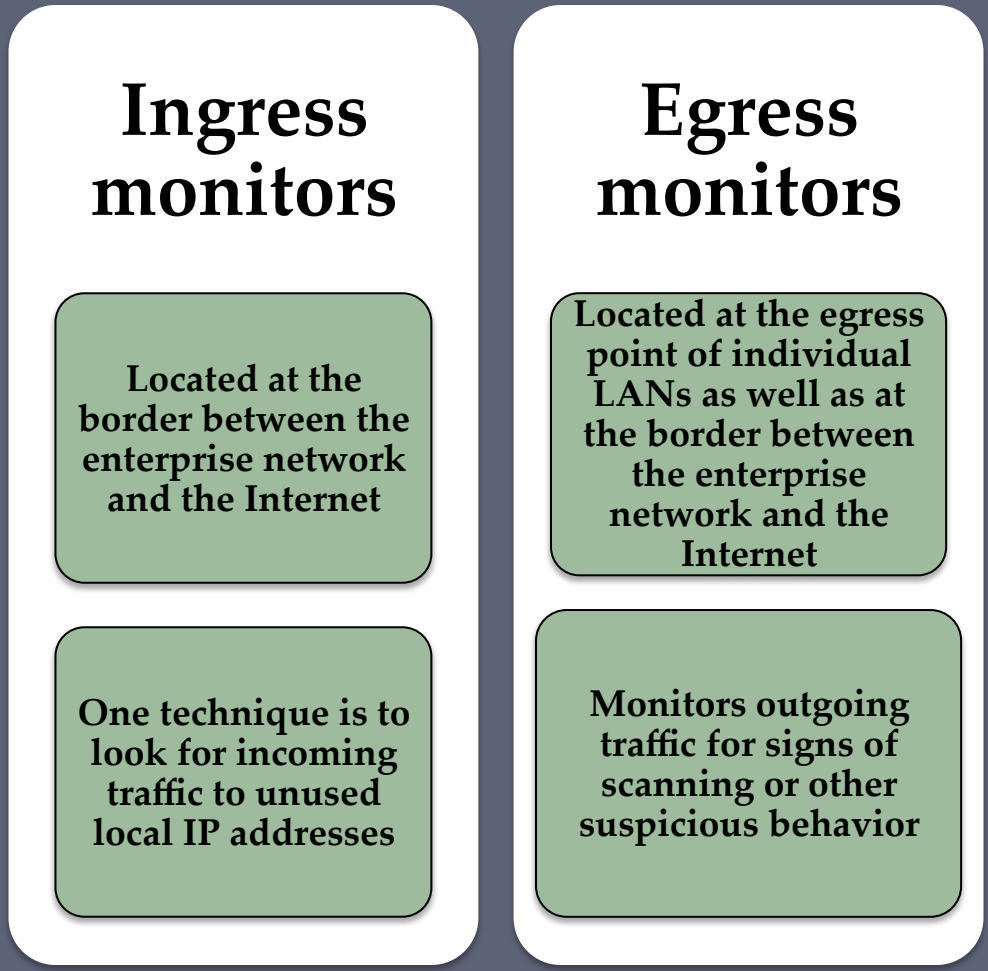
- Integrates with the operating system of a host computer and monitors program behavior in real time for malicious action
  - Blocks potentially malicious actions before they have a chance to affect the system
  - Blocks software in real time so it has an advantage over anti-virus detection techniques such as fingerprinting or heuristics

Limitations

- Because malicious code must run on the target machine before all its behaviors can be identified, it can cause harm before it has been detected and blocked

Perimeter Scanning Approaches

- Anti-virus software typically included in e-mail and Web proxy services running on an organization's firewall and IDS
- May also be included in the traffic analysis component of an IDS
- May include intrusion prevention measures, blocking the flow of any suspicious traffic
- Approach is limited to scanning malware



Two types of monitoring software

Malware Analysis

- Static malware analysis: code-based
  - Reverse-engineering the malware
  - Decompilers, disassemblers, debuggers
  - Tools: IDA pro, gdb, windbg,
- Dynamic malware analysis: behavior-based
  - What changes the malware does to a system? Who is it trying to communicate with?
  - Registry snapshot, file attributes, processes
  - Regshot, RemNUX, CaptureBAT

Summary

- Types of malicious software (malware)
- Advanced persistent threat
- Propagation
  - Infected content
    - viruses
  - Vulnerability exploit
    - worms
  - Social engineering
    - spam
    - e-mail
    - Trojans

- Payload
  - System corruption
  - Attack agent
    - Zombie
    - Bots
  - Information theft
    - Keyloggers
    - Phishing
    - Spyware
  - Stealthing
- Countermeasures