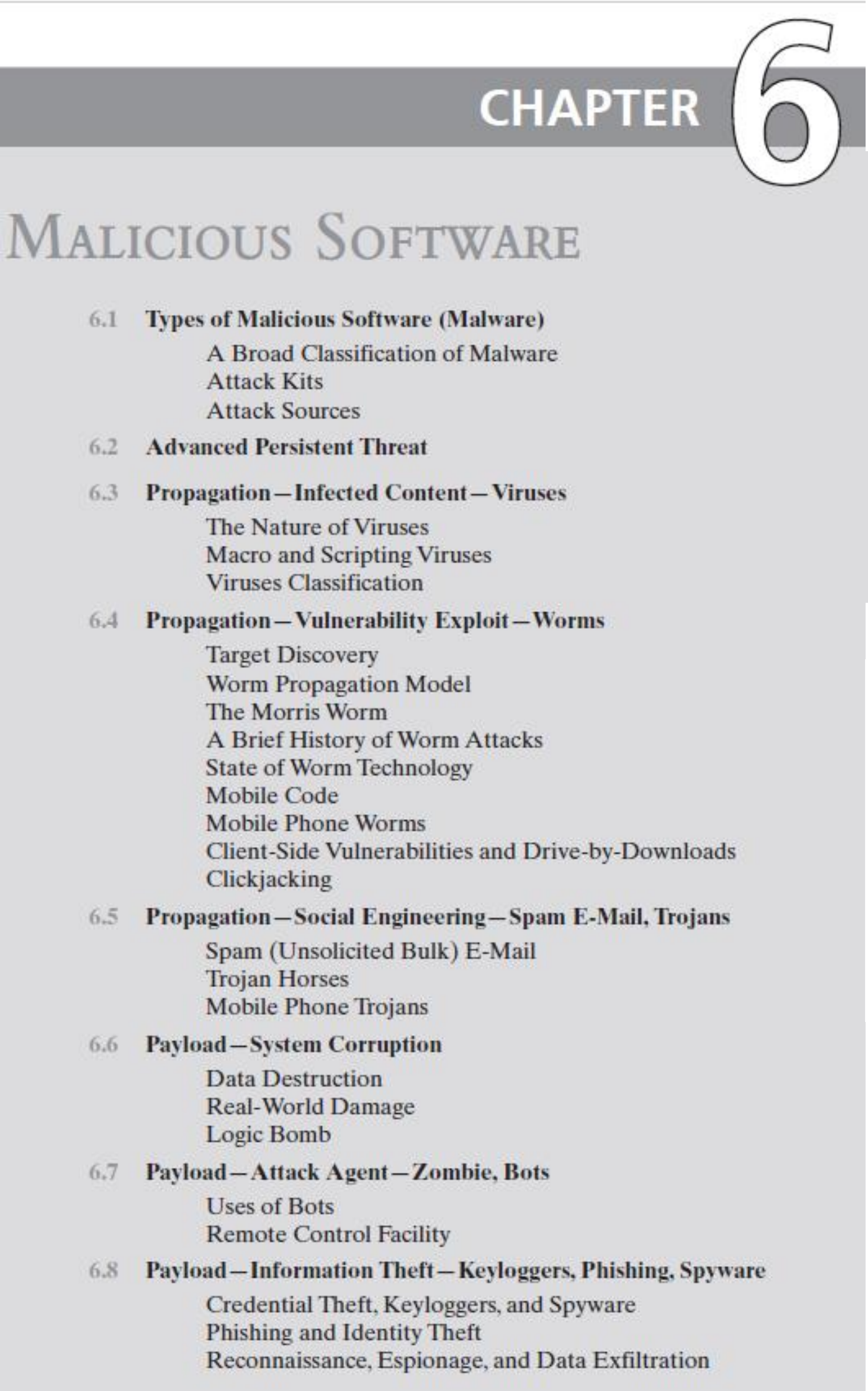
INFORMATION SECURITY FALL 2022

Week #10

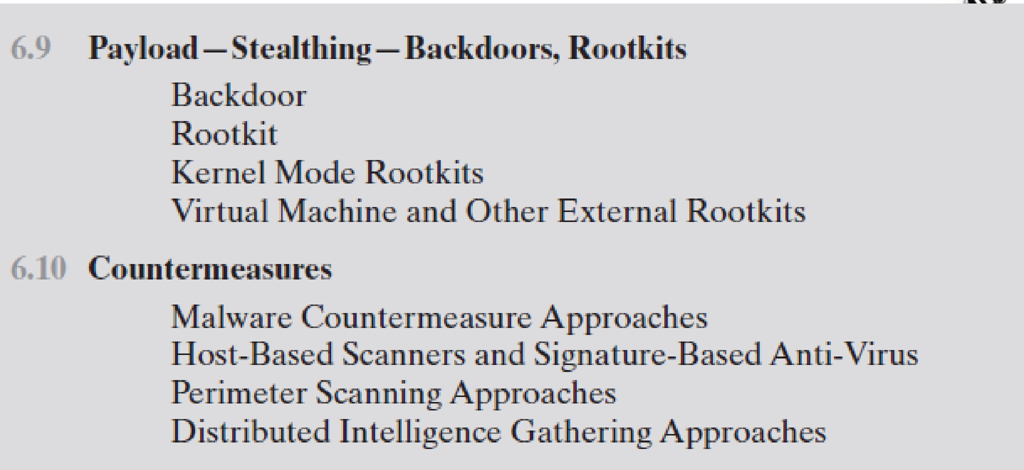
Lecture # 25, 26 and 27

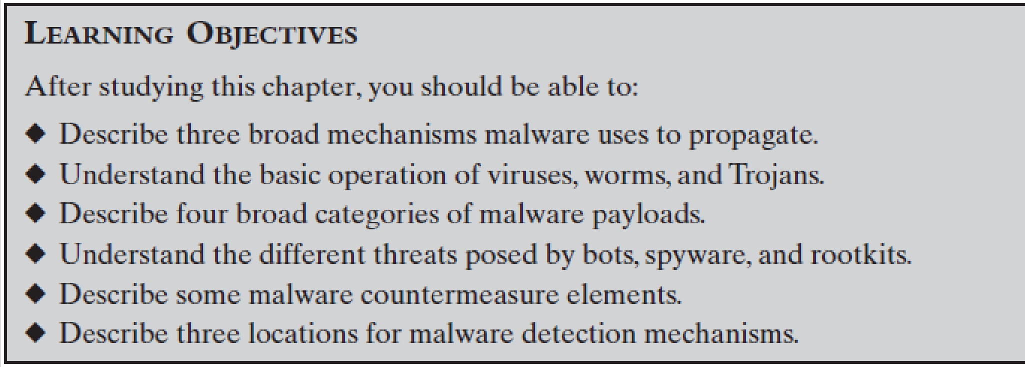
Dr. Aqsa Aslam



CHAPTER 6

Malicious Software





Learning Objectives

After studying this chapter, you should be able to:

- Describe three broad mechanisms malware uses to propagate.
- Understand the basic operation of viruses, worms, and Trojans.
- Describe four broad categories of malware payloads.
- Understand the different threats posed by bots, spyware, and rootkits.
- Describe some malware countermeasure elements.
- Describe three locations for malware detection mechanisms.

MALWARE

NIST 800-83 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."

MALWARE

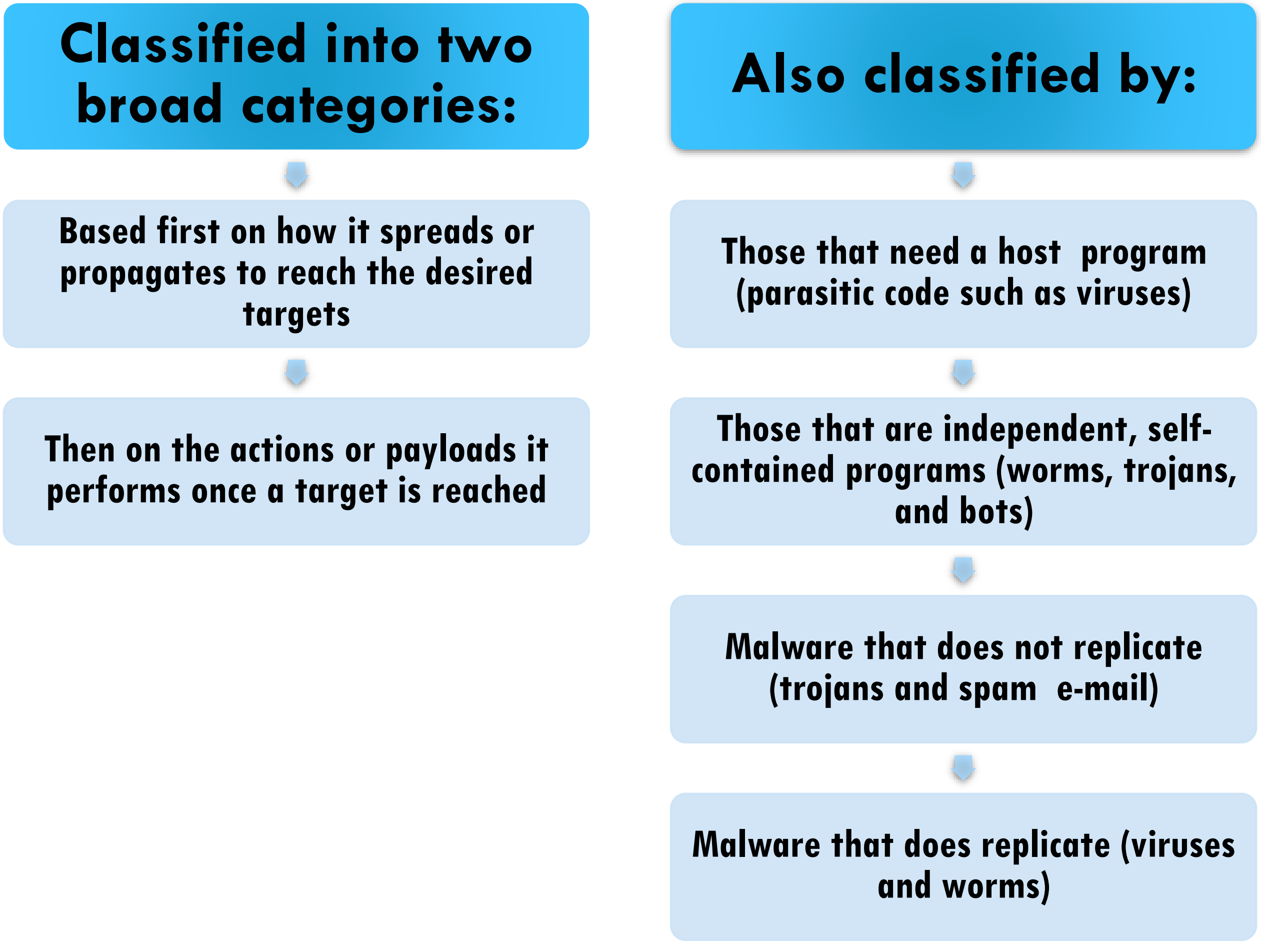
Threat malware poses to

- Application programs,
- Utility programs (such as editors and compilers)
- Kernel-level programs

Malware also use on

- Compromised or malicious websites and servers, or
- In especially crafted spam e-mails or other messages
  - Which aim to trick users into revealing sensitive personal information.

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)

Malware classification is based on:

1. How it spreads or propagates to reach the desired targets
2. On the actions or payloads, it performs once a target is reached

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

TYPES OF MALICIOUS SOFTWARE (MALWARE)

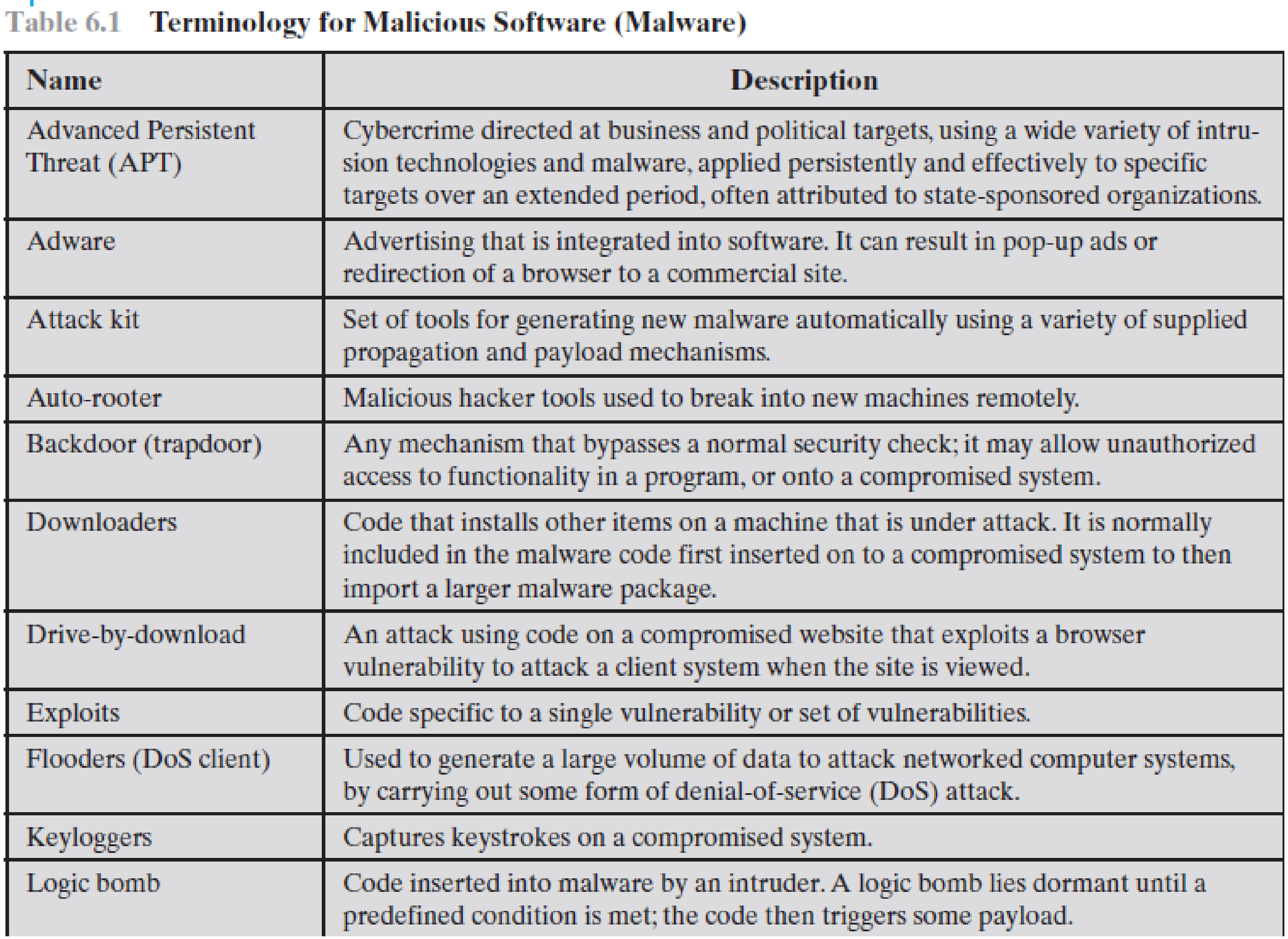
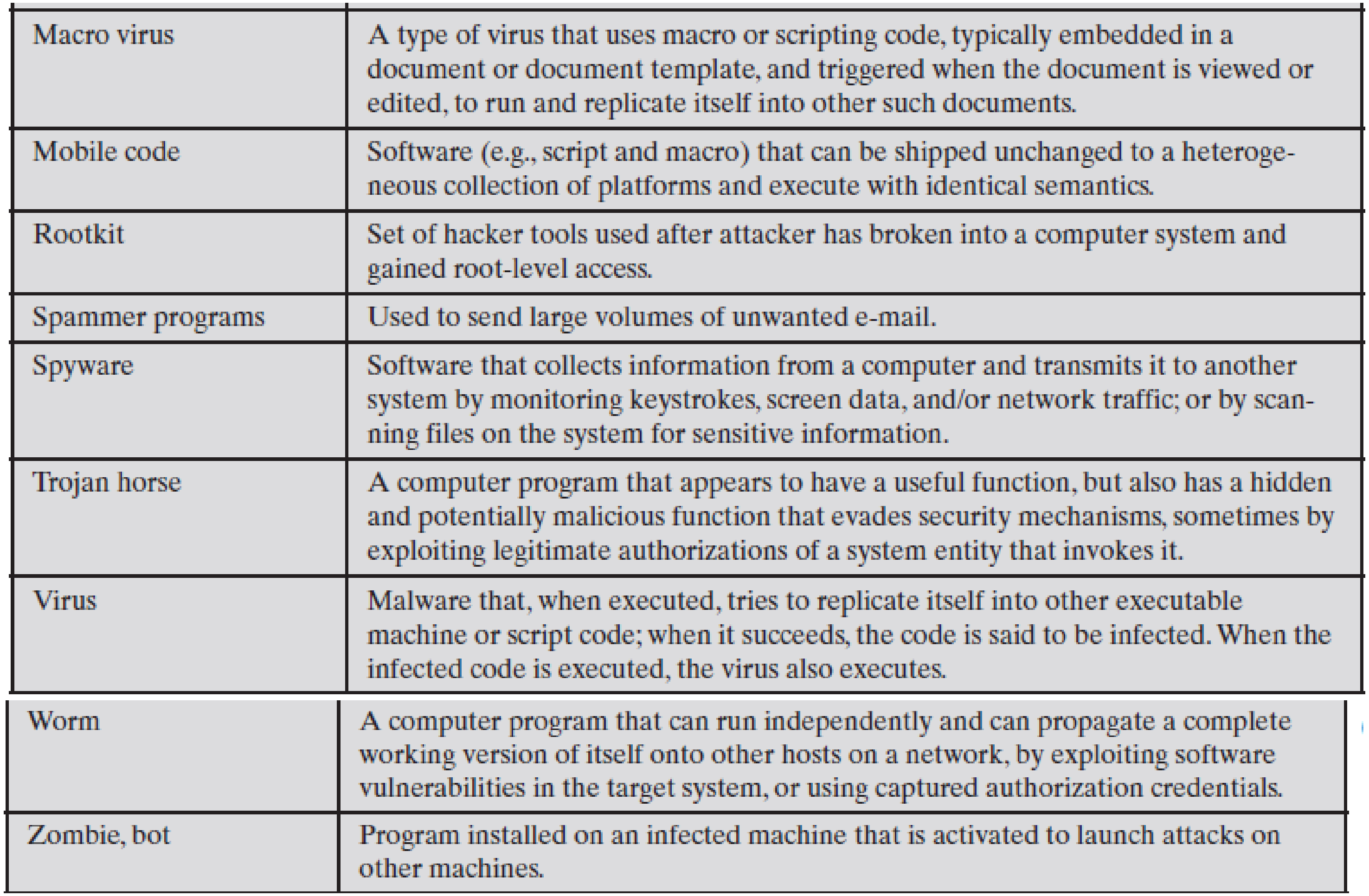


Table 6.1 **Terminology for Malicious Software (Malware)**

Name	Description
Advanced Persistent Threat (APT)	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 mechanism 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 on a compromised website 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 some payload.



Macro virus	A type of virus that uses macro or scripting code, typically embedded in a document or document template, and triggered when the document is viewed or edited, to run and replicate itself into other such documents.
Mobile code	Software (e.g., script and macro) 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 it.
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, by exploiting software vulnerabilities in the target system, or using captured authorization credentials.
Zombie, bot	Program installed on an infected machine that is activated to launch attacks on other machines.

MALWARE

While early malware tended to use a single means of propagation to deliver a single payload, as it evolved, we see a growth of blended malware that incorporates a range of both propagation mechanisms and payloads that increase its ability to spread, hide, and perform a range of actions on targets.

*A **blended attack** uses multiple methods of infection or propagation to maximize the speed of contagion and the severity of the attack. Some malware even support an update mechanism that allows it to change the range of propagation and payload mechanisms utilized once it is deployed*

ATTACKS 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 later of more general attack kits in the 2000s.

These toolkits, often known **as crimeware**

- Now include a variety of propagation mechanisms and payload modules that even novices can combine, select, and deploy
- They can also easily be customized with the latest discovered vulnerabilities in order to exploit the window of opportunity between the publication of a weakness and the widespread deployment of patches to close it.

These kits greatly enlarged the population of attackers able to deploy malware.

- The sheer number of new variants that can be generated by attackers using these toolkits creates a significant problem for those defending systems against them.

The **Zeus crimeware toolkit** is a prominent example of such an attack kit

- Which was used to generate a wide range of very effective, stealthed malware
  - That facilitates a range of criminal activities, in particular capturing and exploiting banking credentials

ATTACKS SOURCES

- Another significant malware development over the last couple of decades is the change from attackers being individuals, often motivated to demonstrate their technical competence to their peers, to more organized and dangerous attack sources. These include:
  - *Politically motivated attackers,*
  - *Criminals,*
  - *Organized crime;*
  - *Organizations that sell their services to companies and nations*
  - *National government.*

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

ADVANCED PERSISTENT THREAT

- **Advanced Persistent Threats (APTs)** have risen to prominence in recent years
  - These are not a new type of malware, but rather the well-resourced, persistent application of a wide variety of intrusion technologies and malware to selected targets, usually business or political.
  - APTs are typically attributed to state-sponsored organizations, with some attacks likely from criminal enterprises as well.
  - APTs differ from other types of attack by their careful target selection, and persistent, often stealthy, intrusion efforts over extended periods.

- A number of high-profile attacks, including:
  - Aurora
  - RSA
  - APT1
  - Stuxnet

ADVANCED PERSISTENT THREAT

- They are named as a result of these characteristics:
  - **Advanced:** Use 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, and often stealthily, 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 attack.

PROPAGATION—INFECTED CONTENT—VIRUSES

- Piece of software that infects programs
    - **Modifies them to include a copy of the virus**
        - The modification includes injecting the original code with a routine to make copies of the virus code, which can then goon to infect other content
    - **Replicates and goes on to infect other content**
        - Virus becomes embedded in a program, or carrier of executable content, on a computer. whenever the infected computer comes into contact with an uninfected piece of code, a fresh copy of the virus passes into the new location.
    - **Easily spread through network environments**

- A virus that attaches to an executable program can do anything that the program is permitted to do.
    - *It executes secretly when the host program is run.*
    - *Once the virus code is executing, it can perform any function (e.g., erasing files and program etc*
    - *Examples of viruses include* ***Creeper, Blaster, Slammer, etc.***

VIRUS COMPONENTS

Many *contemporary types* of malware also include one or more variants of each of these 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

During its lifetime, a typical virus goes through the following four phases:

Dormant phase:

- The virus is idle.
- The virus will eventually be activated by some event
  - such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit.)
- Not all viruses have this stage.

Propagation phase:

- The virus places a copy of itself into other programs or into certain system areas on the disk.
- The copy may not be identical to the propagating version; viruses often morph to evade detection.
- Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.

Triggering phase:

- The virus is activated to perform the function for which it was intended.
- As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.

Execution phase:

- The function is performed.
- The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.

MACRO AND SCRIPTING VIRUSES

In the mid-1990s, macro or scripting code viruses became by far the most prevalent type of virus.

NISTIR 7298 (*Glossary of Key Information Security Terms*, May 2013) defines a ***macro virus as a virus that attaches itself to documents and uses the macro programming capabilities of the document's application to execute and propagate. Macro viruses infect scripting code used to support active content in a variety of user document types.***

MACRO AND SCRIPTING VIRUSES

Macro viruses are particularly threatening for a number of reasons:

1. A macro virus is platform independent. Many macro viruses infect active content in commonly used applications, such as macros in Microsoft Word documents or other Microsoft Office documents, or scripting code in Adobe PDF documents

2. Macro viruses infect documents, not executable portions of code. Most of the information introduced onto a computer system is in the form of documents rather than programs.

3. Macro viruses are easily spread, as the documents they exploit are shared in normal use. A very common method is by electronic mail, particularly since these documents can sometimes be opened automatically without prompting the user.

4. Because macro viruses infect user documents rather than system programs, traditional file system access controls are of limited use in preventing their spread, since users are expected to modify them.

5. Macro viruses are much easier to write or to modify than traditional executable viruses

VIRUSES CLASSIFICATION

A virus classification by target includes the following categories

- **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 consider 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.
  - Typically, the multipartite virus is capable of infecting multiple types of files, so virus eradication must deal with all of the possible sites of infection.

VIRUSES CLASSIFICATION

A virus classification by concealment strategy includes the following categories:

- **Encrypted virus:** A form of virus that uses encryption to obscure it’s content. A portion of the virus creates a random encryption key and encrypts the remainder of the virus. The key is stored with the virus

- **Stealth virus:** A form of virus explicitly designed to hide itself from detection by anti-virus software. Thus, the entire virus, not just a payload, is hidden

- **Polymorphic virus:** A form of virus that creates copies during replication that are functionally equivalent but have distinctly different bit patterns, in order to defeat programs that scan for viruses. The portion of the virus that is responsible for generating keys and performing encryption/decryption is referred to as the *mutation engine*.

- **Metamorphic virus:** As with a polymorphic virus, a metamorphic virus mutates with every infection. The difference is that a metamorphic virus rewrites itself completely at each iteration, using multiple transformation techniques, increasing the difficulty of detection. Metamorphic viruses may change their behavior as well as their appearance.

PROPAGATION—VULNERABILITY EXPLOIT—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

WORM REPLICATION

- ❑ A worm typically uses the same phases as a computer virus:

1. Dormant
2. Propagation
3. Triggering
4. Execution

- ❑ The propagation phase generally performs the following functions:

1. Search for appropriate access mechanisms on other systems to infect by examining host tables, address books, buddy lists, trusted peers, and other similar repositories of remote system access details; **OR** by scanning possible target host addresses; **OR** by searching for suitable removable media devices to use.
2. Use the access mechanisms found to transfer a copy of itself to the remote system, and cause the copy to be run.

TARGET DISCOVERY

- The first function in the propagation phase for a network worm is for it to search for other systems to infect, a process known as **scanning** or fingerprinting.

  [MIRK04] lists the following types of network address scanning strategies that such a worm can use:

  - **Random:** Each compromised host probes random addresses in the IP address space, using a different seed. This technique 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. This can be a slow process done over a long period to avoid detection that an attack is underway. 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 strategy results in a very short scanning period, which may make it difficult to detect that infection is taking place.

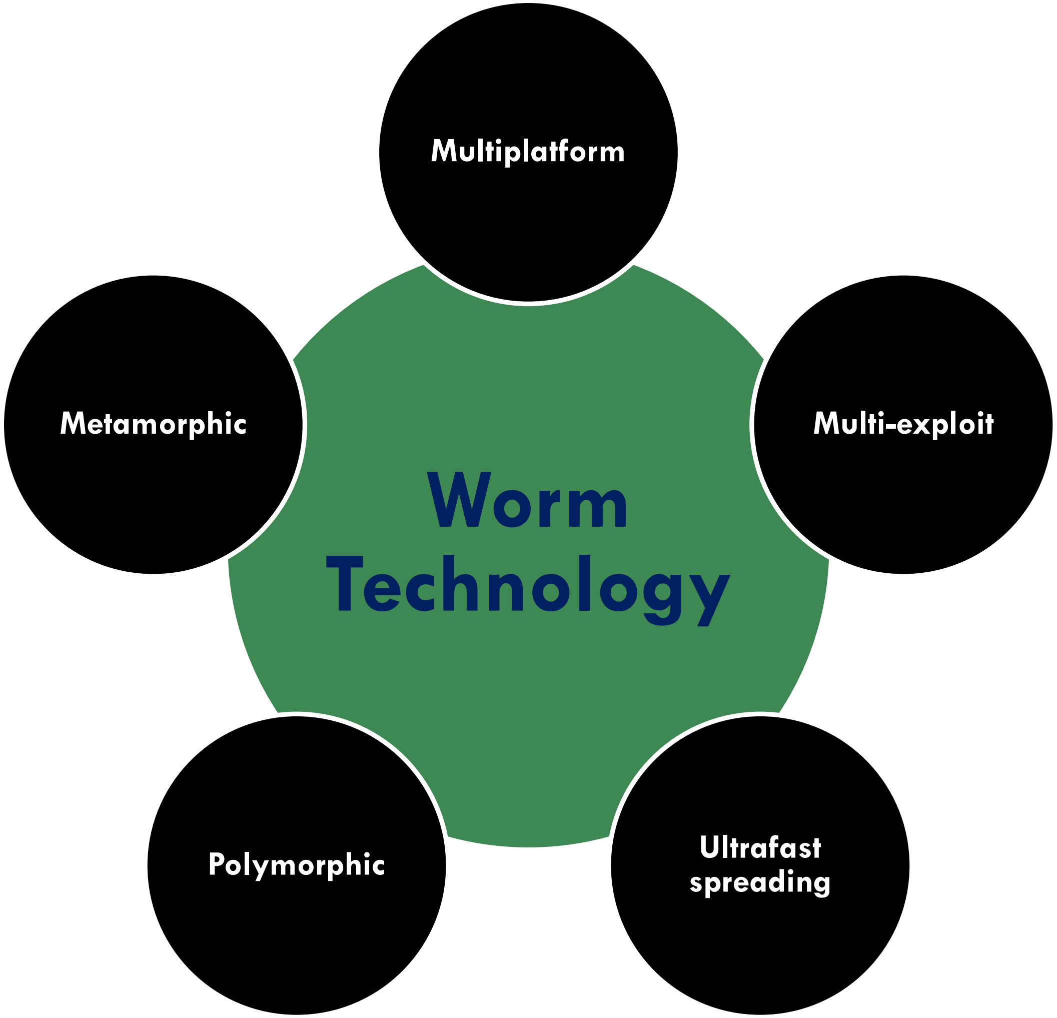
  - **Topological:** This method uses information contained on an infected victim machine to find more hosts to scan.

  - **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.

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

STATE OF WORM TECHNOLOGY



Worm Technology

Multiplatform

Multi-exploit

Ultrafast spreading

Polymorphic

Metamorphic

STATE OF WORM TECHNOLOGY

The state of the art in worm technology includes the following:

- **Multiplatform:** Newer worms are not limited to Windows machines but can attack a variety of platforms, especially the popular varieties of UNIX; or exploit macro or scripting languages supported in popular document types.
- **Multi-exploit:** New worms penetrate systems in a variety of ways, using exploits against Web servers, browsers, e-mail, file sharing, and other network-based applications; or via shared media.
- **Ultrafast spreading:** Exploit various techniques to optimize the rate of spread of a worm to maximize its likelihood of locating as many vulnerable machines as possible in a short time period.
- **Polymorphic:** To evade detection, skip past filters, and foil real-time analysis, worms adopt virus polymorphic techniques. Each copy of the worm has new code generated on the fly using functionally equivalent instructions and encryption techniques.
- **Metamorphic:** In addition to changing their appearance, metamorphic worms have a repertoire of behavior patterns that are unleashed at different stages of propagation.
- **Transport vehicles:** Because worms can rapidly compromise a large number of systems, they are ideal for spreading a wide variety of malicious payloads, such as distributed denial-of-service bots, rootkits, spam e-mail generators, and spyware.
- **Zero-day exploit:** To achieve maximum surprise and distribution, a worm should exploit an unknown vulnerability that is only discovered by the general network community when the worm is launched.

MOBILE CODE

- **NIST SP 800-28 defines mobile code as *"programs that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics"***
- 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
  - VBScript
- Most common ways of using mobile code for malicious operations on local system are:
  - Cross-site scripting
  - Interactive and dynamic Web sites
  - E-mail attachments
  - Downloads from untrusted sites or of untrusted software

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

CLIENT-SIDE VULNERABILITIES AND DRIVE-BY-DOWNLOADS

Exploits browser and plugin vulnerabilities so when the user views a webpage controlled by the attacker, it contains code that exploits the bug to download and install malware on the system without the user's knowledge or consent

In most cases the malware does not actively propagate as a worm does

Spreads when users visit the malicious Web page

WATERING-HOLE ATTACKS

- ○ A variant of drive-by-download used in highly targeted attacks
- ○ The attacker researches their intended victims to identify websites they are likely to visit, then scans these sites to identify those with vulnerabilities that allow their compromise
- ○ They then wait for one of their intended victims to visit one of the compromised sites
- ○ Attack code may even be written so that it will only infect systems belonging to the target organization and take no action for other visitors to the site
- ○ This greatly increases the likelihood of the site compromise remaining undetected

MALVERTISING

Places malware on websites without actually compromising them

The attacker pays for advertisements that are highly likely to be placed on their intended target websites and incorporate malware in them

Using these malicious ads, attackers can infect visitors to sites displaying them

The malware code may be dynamically generated to either reduce the chance of detection or to only infect specific systems

Has grown rapidly in recent years because they are easy to place on desired websites with few questions asked and are hard to track

Attackers can place these ads for as little as a few hours, when they expect their intended victims could be browsing the targeted websites, greatly reducing their visibility

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

- 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 settings 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

PROPAGATION — SOCIAL ENGINEERING— SPAM E-MAIL, TROJANS

- The final category of malware propagation we consider involves social engineering,

"tricking" users to assist in the compromise of their own systems or personal information.

- This can occur when a user views and responds to some SPAM e-mail, or permits the installation and execution of some Trojan horse program or scripting code.

Spam (Unsolicited Bulk) E-Mail

- With the explosive growth of the Internet over the last few decades, the widespread use of e-mail, and the extremely low cost required to send large volumes of e-mail, has come the rise of unsolicited bulk e-mail, commonly known as spam.
- A significant portion of spam e-mail content is just advertising, trying to convince the recipient to purchase some product online, such as pharmaceuticals, or used in scams, such as stock, fake trader scams, or money mule job ads. But spam is also a significant carrier of malware.
- The e-mail may have an attached document, which, if opened, may exploit a software vulnerability to install malware on the user's system **Or,** it may have an attached Trojan horse program or scripting code that, if run, also installs malware on the user's system.
- Spam may be used in a phishing attack, typically directing the user either to a fake website that mirrors some legitimate service, such as an online banking site, where it attempts to capture the user's login and password details; or to complete some form with sufficient personal details to allow the attacker to impersonate the user in an identity theft.

PROPAGATION — SOCIAL ENGINEERING— SPAM E-MAIL, TROJANS

Trojan Horses

- ***A Trojan is a useful, or apparently useful, program or utility containing hidden code that, when invoked, performs some unwanted or harmful function.***

- Trojan horse programs can be used to accomplish functions indirectly that the attacker could not accomplish directly.
  - ***For example, to gain access to sensitive, personal information stored in the files of a user, an attacker could create a Trojan horse program that, when executed, scans the user's files for the desired sensitive information and sends a copy of it to the attacker via a webform or e-mail or text message.***

- **Trojan horses fit into one of three models:**
  - Continuing to perform the function of the original program and additionally performing a separate malicious activity.
  - Continuing to perform the function of the original program but modifying the function to perform malicious activity (e.g., a Trojan horse version of a login program that collects passwords) **or** to disguise other malicious activity (e.g., a Trojan horse version of a process listing program that does not display certain processes that are malicious).
  - Performing a malicious function that completely replaces the function of the original program.

PROPAGATION — SOCIAL ENGINEERING— SPAM E-MAIL, TROJANS

Mobile Phone Trojan

- Mobile phone Trojans also first appeared in 2004 with the discovery of Skuller.
- As with mobile worms, the target is the smartphone, and the early mobile Trojans targeted Symbian phones.
- More recently, a significant number of Trojans have been detected that target Android phones and Apple iPhones. These Trojans are usually distributed via one or more of the app marketplaces for the target phone O/S.
- The rapid growth in smartphone sales and use, which increasingly contain valuable personal information, make them an attractive target for criminals and other attackers
- Recent examples include a phishing Trojan that tricks the user into entering their banking details, and ransomware that mimics Google’s design style to appear more legitimate and intimidating.
- More recently in 2015, XcodeGhost malware was discovered in a number of legitimate Apple Store apps.
- The apps were not intentionally designed to be malicious, but their developers used a compromised Xcode development system that covertly installed the malware as the apps were created [SYMA16].
- This is one of several examples of attackers exploiting the development or enterprise provisioning infrastructure to assist malware distribution.

PAYLOAD — SYSTEM CORRUPTION

- Once malware is active on the target system, the next concern is what actions it will take on this system.
  - That is, what payload does it carry? Some malware has a non-existent or non-functional payload. Its only purpose, either deliberate or due to accidental early release, is to spread.
  - More commonly, it carries one or more payloads that perform covert actions for the attacker.
- An early payload seen in a number of viruses and worms resulted in data destruction on the infected system when certain trigger conditions were met [WEAV03].
- A related payload is one that displays unwanted messages or content on the user's system when triggered. More seriously, another variant attempts to inflict real-world damage on the system. All of these actions target the integrity of the computer system's software or hardware, or of the user's data.
- ***These changes may not occur immediately, but only when specific trigger conditions are met that satisfy their logic-bomb code.***

PAYLOAD — SYSTEM CORRUPTION

Data Destruction and Ransomware

Chernobyl virus

- First seen in 1998
- Example of a destructive parasitic memory-resident Windows 95 and 98 virus
- *Infects executable files when they are opened and when a trigger date is reached, the virus deletes data on the infected system by overwriting the first megabyte of the hard drive with zeroes, resulting in massive corruption of the entire file system*

Klez

- Mass mailing worm infecting Windows 95 to XP systems
- First seen in October 2001
- *Spreads by e-mailing copies of itself to addresses found in the address book and in files on the system*
- *It can stop and delete some anti-virus programs running on the system*
- *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)
- *Mid-2006 a number of worms and Trojans appeared that used public-key cryptography with increasingly larger key sizes to encrypt data*
- *The user needed to pay a ransom, or to make a purchase from certain sites, in order to receive the key to decrypt this data*

RANSOMWARE

WannaCry

- Infected a large number of systems in many countries in May 2017
- When installed on infected systems, it encrypted a large number of files and then demanded a ransom payment in Bitcoins to recover them
- Recovery of this information was generally only possible if the organization had good backups and an appropriate incident response and disaster recovery plan
- Targets widened beyond personal computer systems to include mobile devices and Linux servers
- Tactics such as threatening to publish sensitive personal information, or to permanently destroy the encryption key after a short period of time, are sometimes used to increase the pressure on the victim to pay up

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**
  - A key component of data-corrupting malware is the logic bomb. The logic bomb is code embedded in the malware that is set to “explode” when certain conditions are met.
    - *Examples of conditions that can be used as triggers for a logic bomb are the presence or absence of certain files or devices on the system, a particular day of the week or date, a particular version or configuration of some software, or a particular user running the application. Once triggered, a bomb may alter or delete data or entire files, cause a machine to halt, or do some other damage.*

PAYLOAD – ATTACK AGENTS – ZOMBIE, BOTS

- The next category of payload is where the malware subverts the computational and network resources of the infected system for use by the attacker.

- *Such a system is known as a bot (robot), zombie or drone, and secretly takes over another Internet-attached computer then uses that computer to launch or manage attacks that are difficult to trace to the bot's creator.*

- The bot is typically planted on hundreds or thousands of computers belonging to unsuspecting third parties.

- The compromised systems are not just personal computers, but include servers, and recently embedded devices such as routers or surveillance cameras.

- *The collection of bots often is capable of acting in a coordinated manner; such a collection is referred to as a botnet. This type of payload attacks the integrity and availability of the infected system*.

PAYLOAD – ATTACK AGENTS – ZOMBIE, 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

PAYLOAD – ATTACK AGENTS – ZOMBIE, BOTS

Uses of Bots [HONE05] lists the following uses of bots

Distributed denial-of-service (DDoS) attacks: A DDoS attack is an attack on a computer system or network that causes a loss of service to users

Spamming: With the help of a botnet and thousands of bots, an attacker is able to send massive amounts of bulk e-mail (spam).

Sniffing traffic: Bots can also use a packet sniffer to watch for interesting cleartext data passing by a compromised machine. The sniffers are mostly used to retrieve sensitive information like usernames and passwords.

Keylogging: If the compromised machine uses encrypted communication channels (e.g., HTTPS or POP3S), then just sniffing the network packets on the victim’s computer is useless because the appropriate key to decrypt the packets is missing. But by using a keylogger, which captures keystrokes on the infected machine, an attacker can retrieve sensitive information.

Spreading new malware: Botnets are used to spread new bots. This is very easy since all bots implement mechanisms to download and execute a file via HTTP or FTP. A botnet with 10,000 hosts that acts as the start base for a worm or mail virus allows very fast spreading and thus causes more harm.

Installing advertisement add-ons and browser helper objects (BHOs): Botnets can also be used to gain financial advantages. This works by setting up a fake website with some advertisements: The operator of this website negotiates a deal with some hosting companies that pay for clicks on ads. With the help of a

PAYLOAD – ATTACK AGENTS – ZOMBIE, BOTS

Uses of Bots [HONE05] lists the following uses of bots

Installing advertisement add-ons and browser helper objects (BHOs): Botnets can also be used to gain financial advantages. This works by setting up a fake website with some advertisements: The operator of this website negotiates a deal with some hosting companies that pay for clicks on ads. With the help of a botnet, these clicks can be “automated” so instantly a few thousand bots click on the pop-ups. This process can be further enhanced if the bot hijacks the start-page of a compromised machine so the “clicks” are executed each time the victim uses the browser.

Attacking IRC chat networks: Botnets are also used for attacks against Internet Relay Chat (IRC) networks. Popular among attackers is especially the so-called clone attack: In this kind of attack, the controller orders each bot to connect a large number of clones to the victim IRC network. The victim is flooded by service requests from thousands of bots or thousands of channel-joins by these cloned bots. In this way, the victim IRC network is brought down, similar to a DDoS attack.

Manipulating online polls/games: Online polls/games are getting more and more attention and it is rather easy to manipulate them with botnets. Since every bot has a distinct IP address, every vote will have the same credibility as a vote cast by a real person. Online games can be manipulated in a similar way.

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

- ***Now consider payloads where the malware gathers data stored on the infected system for use by the attacker.***

- A common target is the user’s login and password credentials to banking, gaming, and related sites, which the attacker then uses to impersonate the user to access these sites for gain.

- Less commonly, the payload may target documents or system configuration details for the purpose of reconnaissance (investigation) or espionage (intelligence or spying).

- ***These attacks target the confidentiality of this information.***

PAYLOAD – INFORMATION THEFT – KEYLOGGERS AND SPYWARE

Credential 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

Phishing and Identity 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

PAYLOAD – STEALTHING – BACKDOOR

- The final category of payload we discuss concerns techniques used by malware to hide its presence on the infected system, and to provide covert access to that system. ***This type of payload also attacks the integrity of the infected system.***

- ***A backdoor, also known as a trapdoor, is a secret entry point into a program that allows someone who is aware of the backdoor to gain access without going through the usual security access procedures.***

- Programmers have used backdoors legitimately for many years to debug and test programs; ***such a backdoor is called a maintenance hook.***

- This usually is done when the programmer is developing an application that has an authentication procedure, or a long setup, requiring the user to enter many different values to run the application.

- To debug the program, the developer may wish to gain special privileges or to avoid all the necessary setup and authentication.

- The programmer may also want to ensure that there is a method of activating the program should something be wrong with the authentication procedure that is being built into the application.

PAYLOAD – STEALTHING – ROOTKIT

- ***A rootkit is a set of programs installed on a system to maintain covert access to that system with administrator (or root) privileges, while hiding evidence of its presence to the greatest extent possible***
  - This provides access to all the functions and services of the operating system
  - The rootkit alters the host's standard functionality in a malicious and stealthy way.

- ***With root access, an attacker has complete control of the system and can add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand***
  - A rootkit can make many changes to a system to hide its existence, making it difficult for the user to determine that the rootkit is present and to identify what changes have been made.
  - In essence, a rootkit hides by subverting the mechanisms that monitor and report on the processes, files, and registries on a computer.

ROOTKIT CLASSIFICATION CHARACTERISTICS

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

PAYLOAD – STEALTHING – ROOTKIT

A rootkit can be classified using the following characteristics:

- **Persistent:** Activates each time the system boots. The rootkit must store code in a persistent store, such as the registry or file system, and configure a method by which the code executes without user intervention. This means it is easier to detect, as the copy in persistent storage can potentially be scanned.

- **Memory based:** Has no persistent code and therefore cannot survive a reboot. However, because it is only in memory, it can be harder to detect.

- **User mode:** Intercepts calls to APIs (application program interfaces) and modifies returned results.
  - For example, when an application performs a directory listing, the return results do not include entries identifying the files associated with the rootkit.

- **Kernel mode:** Can intercept calls to native APIs in kernel mode. The rootkit can also hide the presence of a malware process by removing it from the kernel’s list of active processes.

- **Virtual machine based:** This type of rootkit installs a lightweight virtual machine monitor, then runs the operating system in a virtual machine above it. The rootkit can then transparently intercept and modify states and events occurring in the virtualized system.

- **External mode:** The malware is located outside the normal operation mode of the targeted system, in BIOS or system management mode, where it can directly access hardware.

PAYLOAD – STEALTHING – ROOTKIT

Virtual Machine and Other External Rootkits

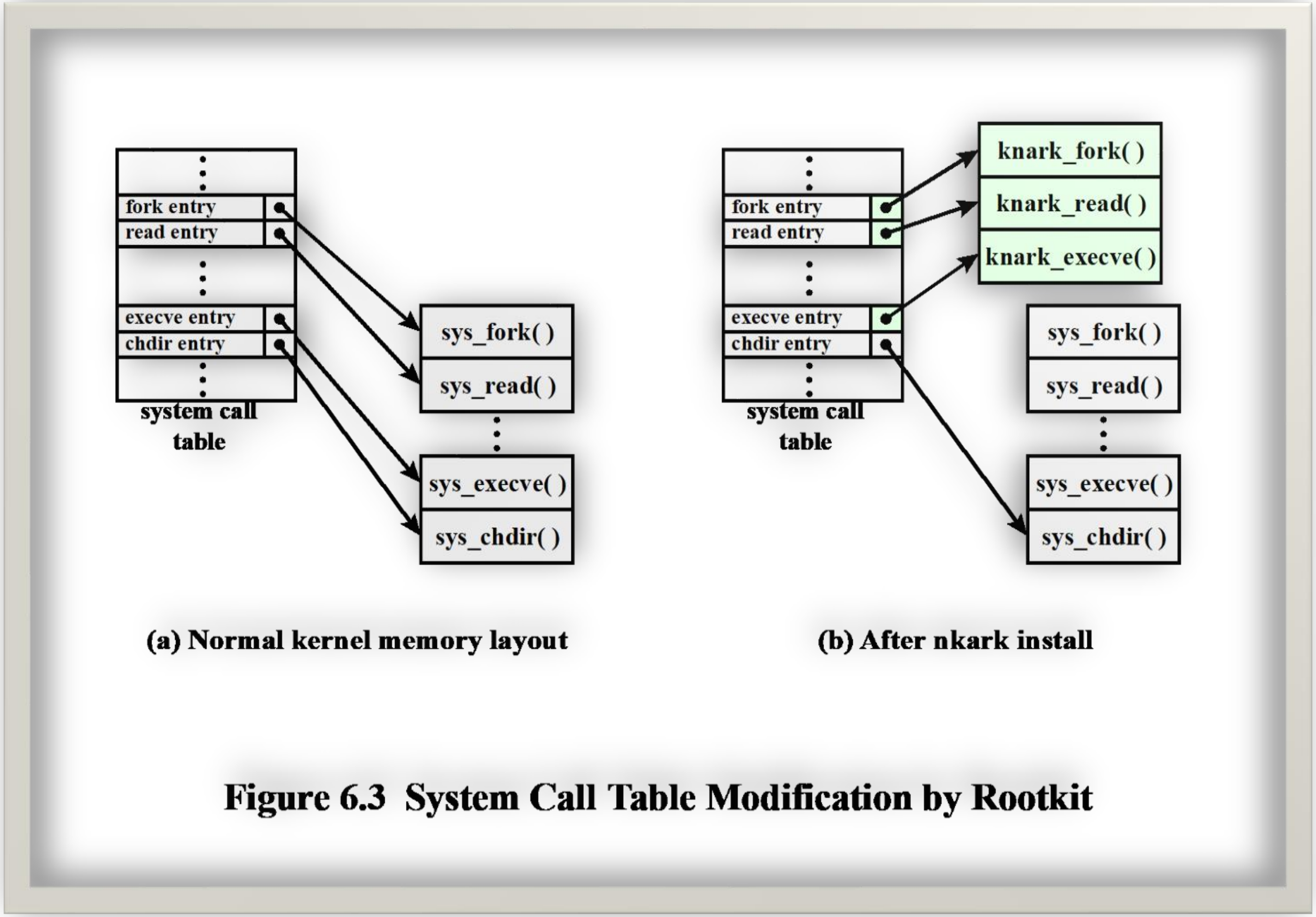


Figure 6.3 System Call Table Modification by Rootkit

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

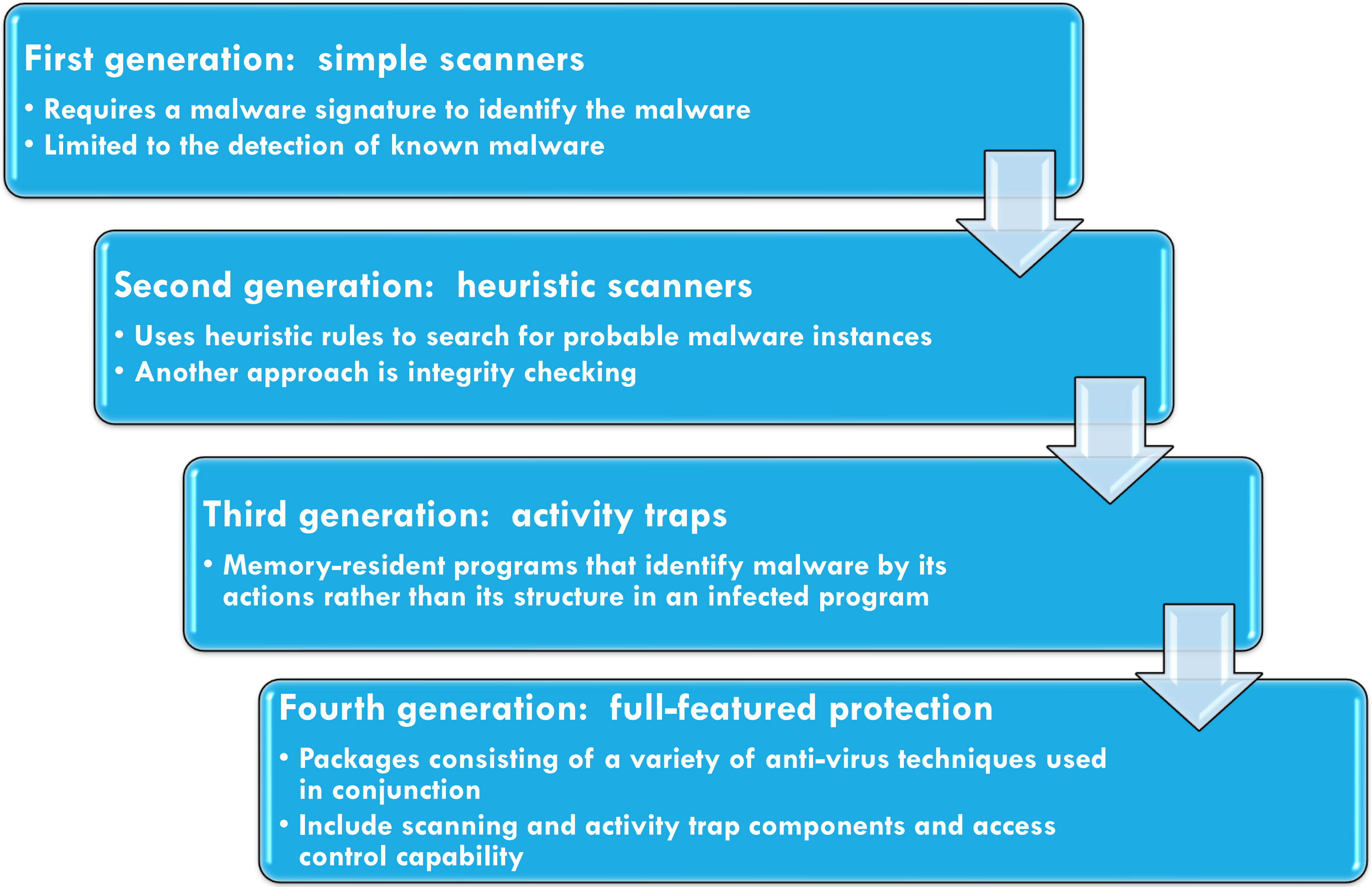
MALWARE COUNTERMEASURE APPROACHES

Requirements for effective malware counter measures:

- **Generality:** The approach taken should be able to handle a wide variety of attacks.
- **Timeliness:** The approach should respond quickly so as to limit the number of infected programs or systems and the consequent activity.
- **Resiliency:** The approach should be resistant to evasion techniques employed by attackers to hide the presence of their malware.
- **Minimal denial-of-service costs:** The approach should result in minimal reduction in capacity or service due to the actions of the countermeasure software, and should not significantly disrupt normal operation.
- **Transparency:** The countermeasure software and devices should not require modification to existing (legacy) OSs, application software, and hardware.
- **Global and local coverage:** The approach should be able to deal with attack sources both from outside and inside the enterprise network.

GENERATIONS OF ANTI-VIRUS SOFTWARE

Host-Based Scanners and Signature-Based Anti-Virus



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

SANDBOX ANALYSIS

Running potentially malicious code in an emulated sandbox or on a virtual machine

Allows the code to execute in a controlled environment where its behavior can be closely monitored without threatening the security of a real system

Running potentially malicious software in such environments enables the detection of complex encrypted, polymorphic, or metamorphic malware

The most difficult design issue with sandbox analysis 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

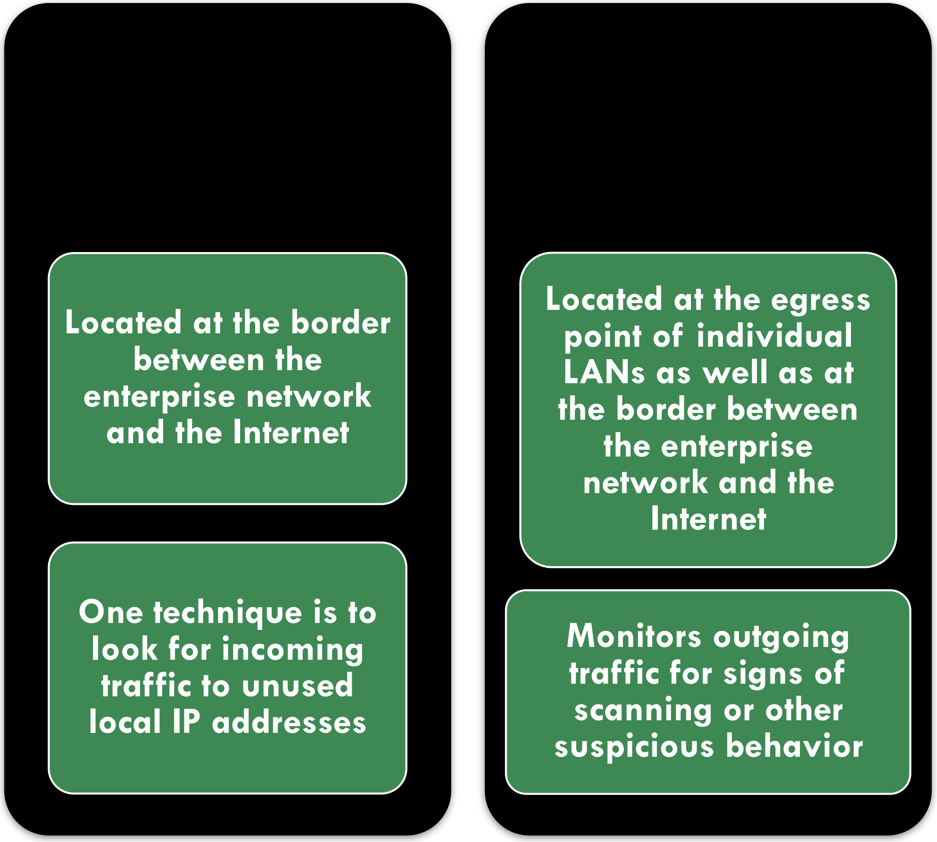
PERIMETER SCANNING APPROACHES

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



Located at the border between the enterprise network and the Internet

One technique is to look for incoming traffic to unused local IP addresses

Located at the egress point of individual LANs as well as at the border between the enterprise network and the Internet

Monitors outgoing traffic for signs of scanning or other suspicious behavior

Two types of monitoring software