Malware

Malicious software

- Malicious code can do anything any other program can such as
  - Writing message on screen
  - Stopping a running program
  - Generating a sound
- It can lie dormant , undetected until some event triggers it.
- Malicious code runs under user’s authority so it can do/access everything the user can

Virus

- A program that attaches itself to some other program in order to propagate
- Passive propagation
- Whenever host program is executed, virus replicates itself and pass on malicious code to other non-malicious programs by modifying them

Types of viruses

- Transient virus:
  - Its life depends on life of its host
  - It runs when its attached program executes and terminates when its attached program ends
  - During its execution it spreads infection to other programs
- Resident virus:
  - Locates itself in memory
  - Then it can remain active or can be activated as a stand-alone program even if attached program ends

Where do Viruses Live?

- Just about anywhere…
- Boot sector
  - Take control before anything else
- Memory resident
  - Stays in memory
- Applications, macros, data, etc.
- Library routines
- Compilers, debuggers, virus checker, etc.
  - These are particularly nasty!

Viruses

- Independent of operating system and hardware
- a typical virus goes through phases of:
  - dormant
  - propagation
  - triggering
  - execution

Phases of virus

- Dormant Phase:
  - The virus is idle.
  - 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.

Phases of virus

- 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.

Phases of virus

- 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.

Phases of virus

- 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.

Brain

- First appeared in 1986
- More annoying than harmful
- A prototype for later viruses
- Not much reaction by users
- What it did
  - Placed itself in boot sector (and other places)
  - Screened disk calls to avoid detection
  - Each disk read, checked boot sector to see if boot sector infected; if not, infect it
- Brain did nothing malicious

Worm

- A worm is a program which spreads usually over network connections.
- Unlike a virus which attach itself to a host program, worms always need a host program to spread.
- In practice, worms are not normally associated with one person computer systems.
- They are mostly found in multi-user systems such as Unix environments.

Worm

- To replicate itself, a worm uses some means to access remote systems.
  - Electronic mail or instant messenger facility
  - File sharing
  - Remote execution capability
  - Remote file access or transfer capability
  - Remote login capability

Worms

- Morris worm (1988)
- Code Red (2001)
- SQL Slammer (2004)

Morris Worm

- First appeared in 1988
- What it tried to do
  - Determine where it could spread
  - Spread its infection
  - Remain undiscovered
- Morris claimed it was a test gone bad
- “Flaw” in worm code
  - it tried to re-infect infected systems
  - Led to resource exhaustion
  - Adverse effect was like a so-called rabbit

Morris Worm

- How to spread its infection?
- Tried to obtain access to machine by
  - User account password guessing
  - Exploited buffer overflow
  - Exploited trapdoor in sendmail
- Flaws in sendmail was well-known at the time, but not widely patched

Code Red Worm

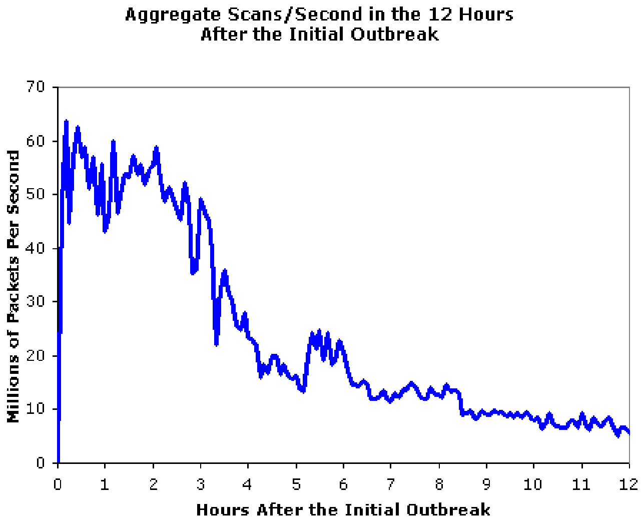
- Appeared in July 2001
- Infected more than **250,000 systems in about 15 hours**
- In total, infected 750,000 out of about 6,000,000 susceptible systems
- Exploited buffer overflow in Microsoft IIS server software
- Then monitored traffic on port 80 for other susceptible servers

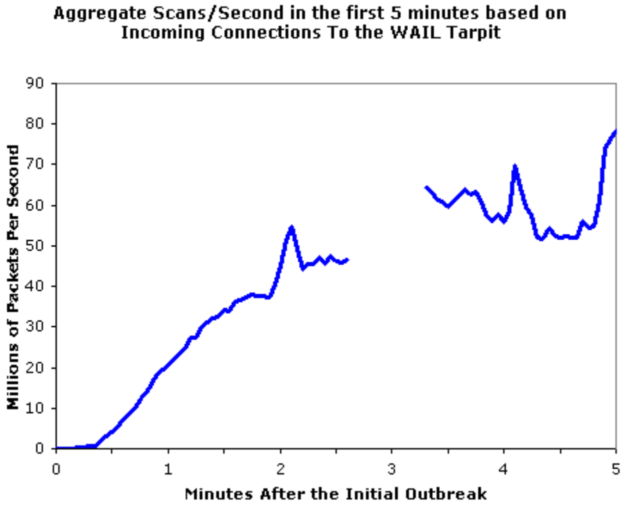
Code Red Worm

- What it did
  - Day 1 to 19 of month: tried to spread infection
  - Day 20 to 27: distributed denial of service attack on www.whitehouse.gov
- Later versions (several variants)
  - Included trapdoor for remote access

SQL Slammer

- ❑Infected **250,000 systems in 10 minutes!**
- ❑Code Red took 15 hours to do what Slammer did in 10 minutes
- ❑At its peak, Slammer infections doubled every 8.5 seconds
- ❑Slammer spread too fast
- ❑“Burned out” available bandwidth





SQL Slammer

- Why was Slammer so successful?
  - Worm fit in **one 376 byte UDP packet**
  - Firewalls often let small packet thru, assuming it could do no harm by itself
    - Then firewall monitors the connection

Trojan Horse

History of Trojan Horse

- In Greek mythology, the **Trojan Horse** was a wooden horse that was said to have been used by the Greeks during the Trojan war to enter the city of Troy and win the war.
- After a fruitless 10-year siege, the Greeks constructed a huge wooden horse at the behest of Odysseus, and hid a select force of men inside, including Odysseus himself.
- The Greeks pretended to sail away, and the Trojans pulled the horse into their city as a victory trophy.
- That night, the Greek force crept out of the horse and opened the gates for the rest of the Greek army, which had sailed back under the cover of darkness.
- The Greeks entered and destroyed the city, ending the war.

Trojan Horse Definition

- A Trojan describes the class of malware that appears to perform a desirable function but in fact performs undisclosed malicious functions that allow unauthorized access to the victim computer

Trojan Horse : Introduction

- A Trojan Horse program is a unique form of computer attack that allows a remote user a means of gaining access to a victim's machine without their knowledge.

- Trojan Horse initially appears to be harmless, but later proves to be extremely destructive.

- Trojan Horse is not a Virus.

Objectives of Trojan Horse Programs

Trojan horses can exploit your system in various and creative ways including:

- **Creating a "backdoor" that allows remote access to control your machine**
- **Recording keystrokes to steal credit card or password information**
- **Commandeering your system to distribute malware or spam to other computers**
- **Spying on your activities by sending screenshots of your monitor to a remote location**
- **Uploading or downloading files**
- **Erasing or overwriting data**

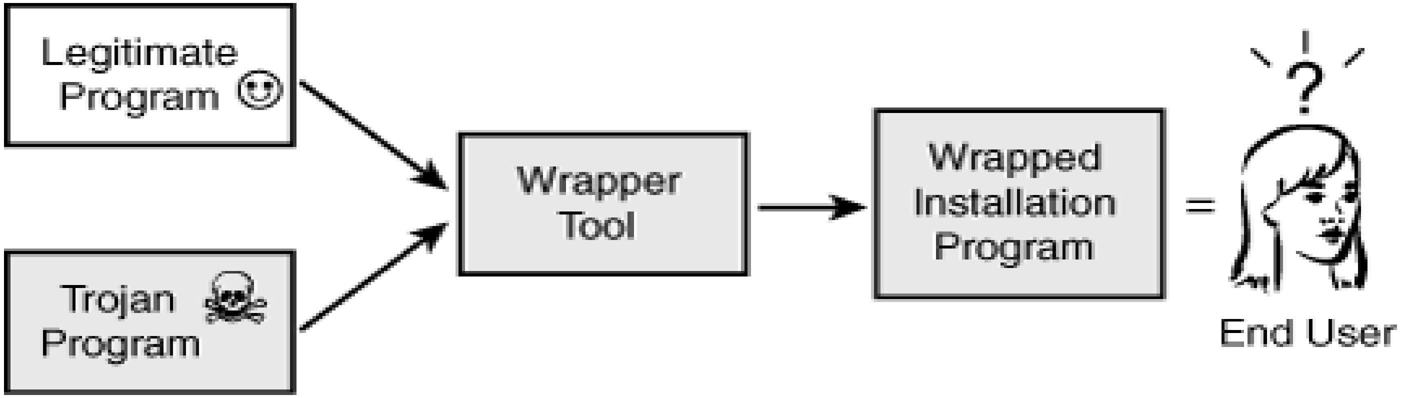
Types of Trojan Horses

The EC Council groups Trojan horses into seven main types

- Remote Access Trojans
  - Subseven
- Data Sending Trojans
  - Eblaster
- Destructive Trojans
  - Hard Disk Killer
- Proxy Trojans
  - Troj/Proxy-GG
- FTP Trojans
  - Trojan.Win32.FTP Attack
- security software disabler Trojans
  - Trojan.Win32.Disabler.b
- denial-of-service attack (DoS) Trojans
  - PC Cyborg Trojan

Trojan Horse Techniques

- Combine malicious code with a legitimate program



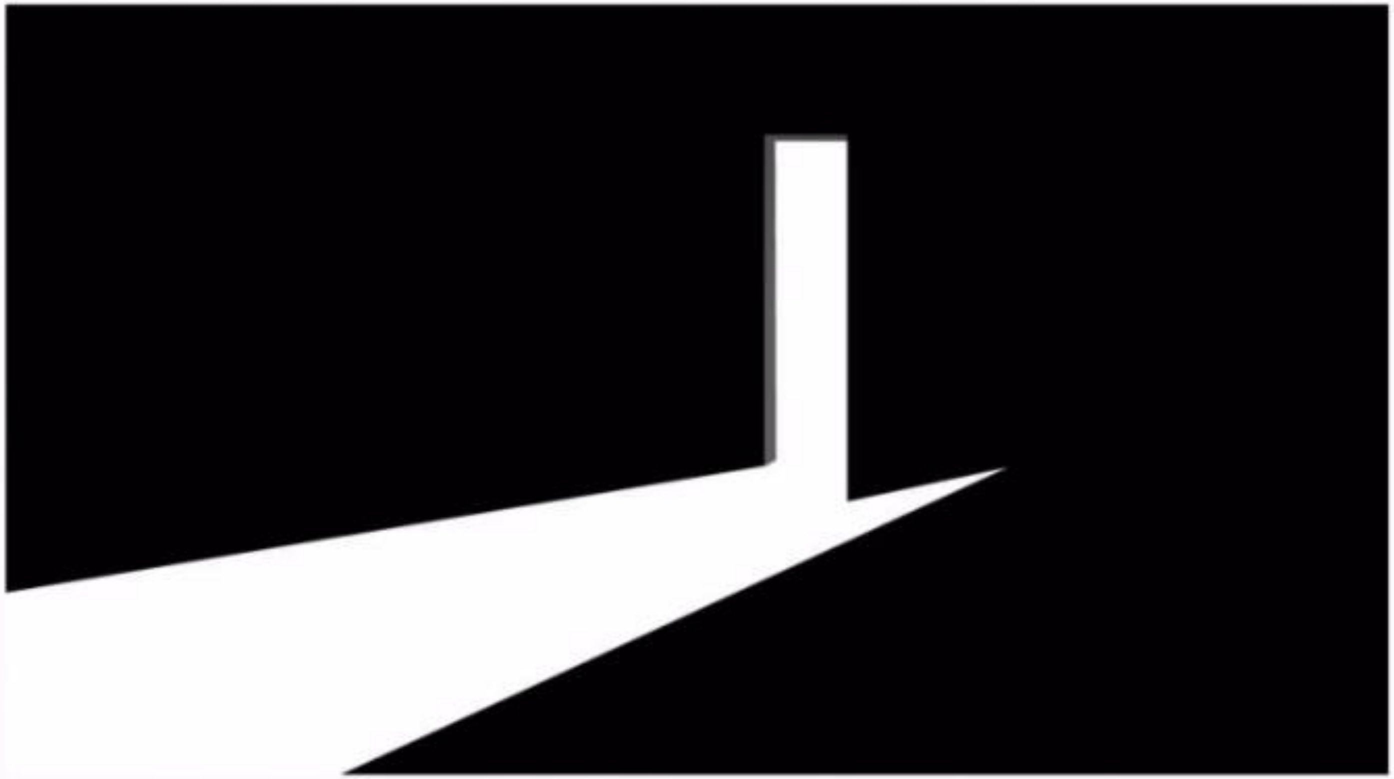
Prevention of Trojan Horse Programs

- Install latest security patches for the operating system.
- Install Anti-Trojan software.
  - Trojan Hunter
  - A- Squared
- Install anti-virus software and update it regularly
- Install a secure firewall
- Do not give strangers access (remote as well as physical) to your computer.
- Do not run any unknown or suspicious executable program just to "check it out".
- Scan all email attachments with an antivirus program before opening it.

Prevention of Trojan Horse Programs

- Do regular backup of your system.
- Do not use the features in programs that can automatically get or preview files.
- Do not type commands that others tell you to type, or go to web addresses mentioned by strangers.
- Never open instant message (IM) attachments from unknown people.
- Do not use peer-to-peer or P2P sharing networks, such as Kazaa, Limewire, Gnutella, etc. as they do not filter out malicious programs hidden in shared files.
- Educate your coworkers, employees, and family members about the effects of Trojan Horse.
- Finally, protection from Trojans involves simple common sense

BACKDOORS



Backdoor Attack

- It is a vulnerability that gives an attacker unauthorized access to a system by bypassing normal security mechanisms. This threat works in the background, hiding itself from the user, and it’s tough to detect and remove.

- Cybercriminals commonly use backdoors to install malware, giving them remote administrative access to a system. Once an attacker has access to a system through a backdoor, they can potentially modify files, steal personal information, install unwanted software, and even take control of the entire computer.

Backdoor Attack

- These kinds of attacks represent a serious risk to users of both computers and mobile devices since an attacker can potentially gain access to your personal files, as well as sensitive financial and identity information

- If an attacker uses a backdoor to install keylogging software on your computer, allowing them to see everything that you type, including passwords and once this information is in the hands of the cybercriminals, your accounts could be compromised, opening the door to identity theft.

Tips to protect you from back door threats

- Use comprehensive security software on your computers and mobile devices to protect you from malware.

- Never click on an email attachment or a link sent from people you don’t know and watch what you download from the web.

- Be careful about which sites you visit, since less secure sites can install malware on your computer simply by visiting a compromised web page. You can check the safety of a website before you visit it by using any web vulnerability assessment tool, which tells you if a site is safe or not right in your search window.

- Only install programs that you need, minimizing your exposure to potential vulnerabilities.

Spam

- **Spamming** is the use of messaging systems to send multiple unsolicited messages (**spam**) to large numbers of recipients for commercial advertising, non-commercial use, phishing or simply repeatedly sending the same message to the same user.

- The most widely recognized form of spam is email spam

- This term is applied to similar abuses in other media like instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, online classified ads spam, mobile phone messaging spam, Internet forum spam, spam on mobile apps, television advertising and file sharing spam.

Spam

- It is named after SPAM, luncheon meat, a restaurant that has Spam in almost every dish.
- Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, servers, infrastructures, IP ranges, and domain names
- There are several spamming tools available to send bulk mail by hiding the spammer’s identity.

Trap Door

- A trap door is kind of a secret entry point into a program that allows anyone to gain access to any system without going through the usual security access procedures.
- Another definition of a trap door is it is a method of bypassing normal authentication methods. Therefore it is also known as a back door.
- Trap Doors are quite difficult to detect and also in order to find them the programmers or the developers have to go through the components of the system.
- Programmers use Trap door legally to debug and test programs. Trap doors turn to threats when any dishonest programmers gain illegal access.
- Program development and software update activities should be the first focus of security measures. The operating system that controls the trap doors is difficult to implement.

Security Implications

The presence of trapdoors poses a significant security risks, as they can be abused by attackers to compromise systems, steal data, or conduct malicious activities without detection. Therefore, it's essential to identify and secure or remove any unintended or unauthorized trapdoors from computer systems and software.

Trapdoors and Backdoors

- Trapdoor
  - Hard-coded access built into the program
  - Ensures access should normal access methods fail
  - Creates vulnerability in systems using the software
- Backdoor
  - Ensures continued unrestricted access in the future
  - Attackers implant them in compromised systems
  - Can be installed inadvertently with a Trojan horse

What is a Denial-of-Service Attack?

- A Denial-of-Service (DoS) attack is an attack on a computer network that limits, restricts, or stops authorized users from accessing system resources.
  - DoS attacks work by flooding the target with traffic or sending it data that causes it to crash. It deprives genuine users of the service or resources they expect to receive.
  - DoS assaults frequently target high-profile corporations such as banks, commerce, media companies, and government and trade organizations' web servers.
  - Even though DoS assaults seldom result in the theft or loss of critical information or other assets, they can take a lot of time and money to cope with.

Types of DoS Attacks

- In a **Smurf Attack**, the attacker sends Internet Control Message Protocol broadcast packets to a number of hosts with a spoofed source Internet Protocol (IP) address that belongs to the target machine. The recipients of these spoofed packets will then respond, and the targeted host will be flooded with those responses.

- A **SYN flood** occurs when an attacker sends a request to connect to the target server but does not complete the connection through what is known as a three-way handshake—a method used in a Transmission Control Protocol (TCP)/IP network to create a connection between a local host/client and server. The incomplete handshake leaves the connected port in an occupied status and unavailable for further requests. An attacker will continue to send requests, saturating all open ports, so that legitimate users cannot connect.

Types of DoS Attacks

- **Teardrop attack:** A teardrop attack exploits a vulnerability in the TCP/IP Internet protocol suite that prevents the server from reassembling fragmented data packets. The server is flooded with fragmented packets, which overlap each other and make it difficult for the server to recompile the original data. This causes the server to crash.

- **ICMP flood attack:** The ICMP protocol is used to communicate diagnostic information between the client and the server. By sending an excessive number of ICMP pings, the target server fails to respond to all requests with the available resources. This ultimately causes the server to be unresponsive, resulting in a denial-of-service condition.

Types of DoS Attacks

- **Buffer overflow attack:** The buffer overflow attack exploits a vulnerability in the sequential data buffers that hold data temporarily.
  - The attack attempts to store more data than the allocated memory buffer, which overwrites the adjacent memory buffer locations. This causes the memory stack to store corrupted and overwritten error data, which leads the server to crash or fail to prevent the execution of malicious code. Repeated attempts to corrupt these buffers cause a Denial of Service condition on the server.

Types of DoS Attacks

- **Ping of Death Attack**: The ping of death is a form of denial-of-service (DoS) attack that occurs when an attacker crashes, destabilizes, or freezes computers or services by targeting them with oversized data packets. A correct Internet Protocol version 4 (IPv4) packet is formed of a maximum of 65,535 bytes, and most legacy computers cannot handle larger packets. Sending a ping larger than this violates the IP rules, so attackers send packets in fragments which, when the targeted system attempts to reassemble, results in an oversized payload that can cause the system to crash, freeze, or reboot.
- **Unintended DoS Attack**: Not all DoS attacks emerge as malicious activity. A web service that cannot adequately handle a temporary surge in organic web traffic, like on Black Friday in the U.S., can also crash and run into a state similar to the Denial of Service.

System Corruption:

Definition: System corruption refers to the unintended or unauthorized alteration of data, software, or hardware components of a computer system, leading to its malfunctioning or loss of integrity.

- Causes: Corruption can occur due to various reasons, including software bugs, hardware failures, malware infections, and improper shutdowns.

- Effects: System corruption can result in data loss, application crashes, system instability, and overall degradation of system performance.

Attack agents

Definition: Attack agents are entities or components responsible for carrying out malicious activities in a cyber attack. These can be individuals, groups, or automated scripts used to exploit vulnerabilities in systems or networks.

- Types: Attack agents include hackers, malware, botnets, insiders, and other malicious actors who attempt to gain unauthorized access, steal data, disrupt services or cause damage to computer systems and networks.

- Examples: Attack agents may deploy various attack techniques such as phishing, ransomware, DDoS (Distributed Denial of Service), SQL injection, and social engineering to achieve their objectives.

Information theft

Definition: Information theft, also known as data theft, involves the unauthorized acquisition of sensitive or confidential information from individuals, organizations, or systems.

- Targets: Attackers may target personal information (e.g., credit card details, passwords), intellectual property, financial data, trade secrets, or any other valuable data that can be exploited for financial gain or competitive advantage.

- Methods: Information theft can occur through various means, including hacking, malware infections, phishing, social engineering, insider threats, and physical theft of devices or storage media.

- Consequences: Information theft can lead to financial losses, reputational damage, legal consequences (e.g., regulatory fines), identity theft, fraud, and loss of trust among customers or stakeholders.

Zombie

Definition: In the context of cybersecurity, a zombie refers to a compromised computer or device that has been infected with malware and is under the control of a remote attacker.

- Functionality: Zombies, also known as bots or botnets, can be used to carry out various malicious activities, such as sending spam emails, launching DDoS attacks, distributing malware, or stealing sensitive information.

- Propagation: Zombies are typically recruited into botnets through malware infections, exploiting vulnerabilities in operating systems, applications, or network services.

- Mitigation: Detecting and mitigating zombie infections requires deploying antivirus software, intrusion detection systems, firewalls, and other security measures to identify and quarantine compromised devices before they can be used for malicious purposes.

Rootkits

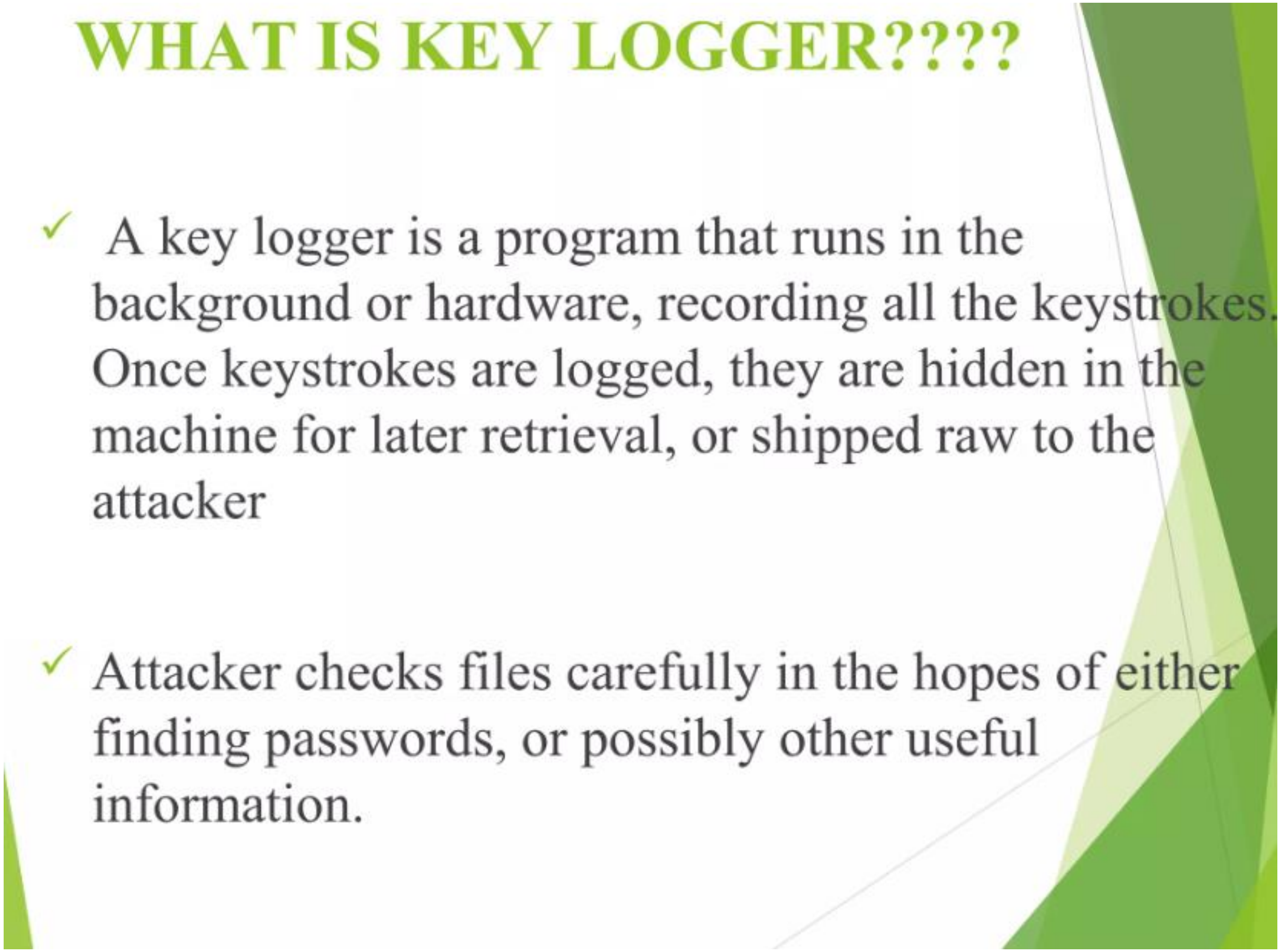
Definition: Rootkits are stealthy types of malware designed to conceal the presence of malicious software or unauthorized access on a compromised system.

- Functionality: Rootkits modify the operating system's kernel or system firmware to hide their presence from antivirus software, system utilities, and security mechanisms.

- Capabilities: Rootkits can provide attackers with persistent access to compromised systems, allowing them to execute malicious commands, steal sensitive information, or maintain control over the system without detection.

- Removal: Removing rootkits can be difficult, as they often require specialized tools and techniques to detect and eradicate from infected systems.

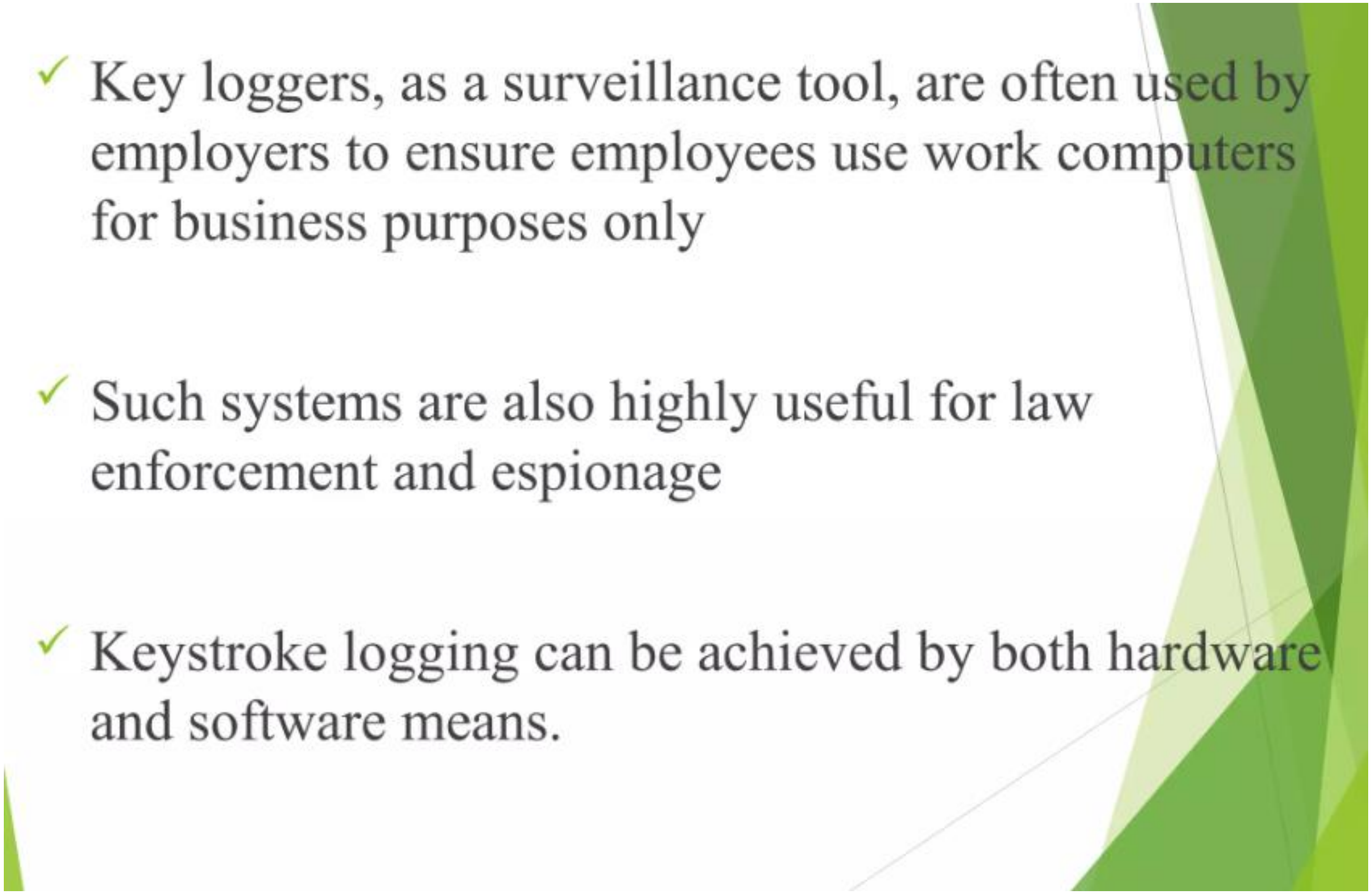
Keyloggers



WHAT IS KEY LOGGER????

- ✓ A key logger is a program that runs in the background or hardware, recording all the keystrokes. Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped raw to the attacker

- ✓ Attacker checks files carefully in the hopes of either finding passwords, or possibly other useful information.



- ✓ Key loggers, as a surveillance tool, are often used by employers to ensure employees use work computers for business purposes only

- ✓ Such systems are also highly useful for law enforcement and espionage

- ✓ Keystroke logging can be achieved by both hardware and software means.

✓ There are two types of keyloggers :

1. Hardware Keylogger
2. Software Keylogger

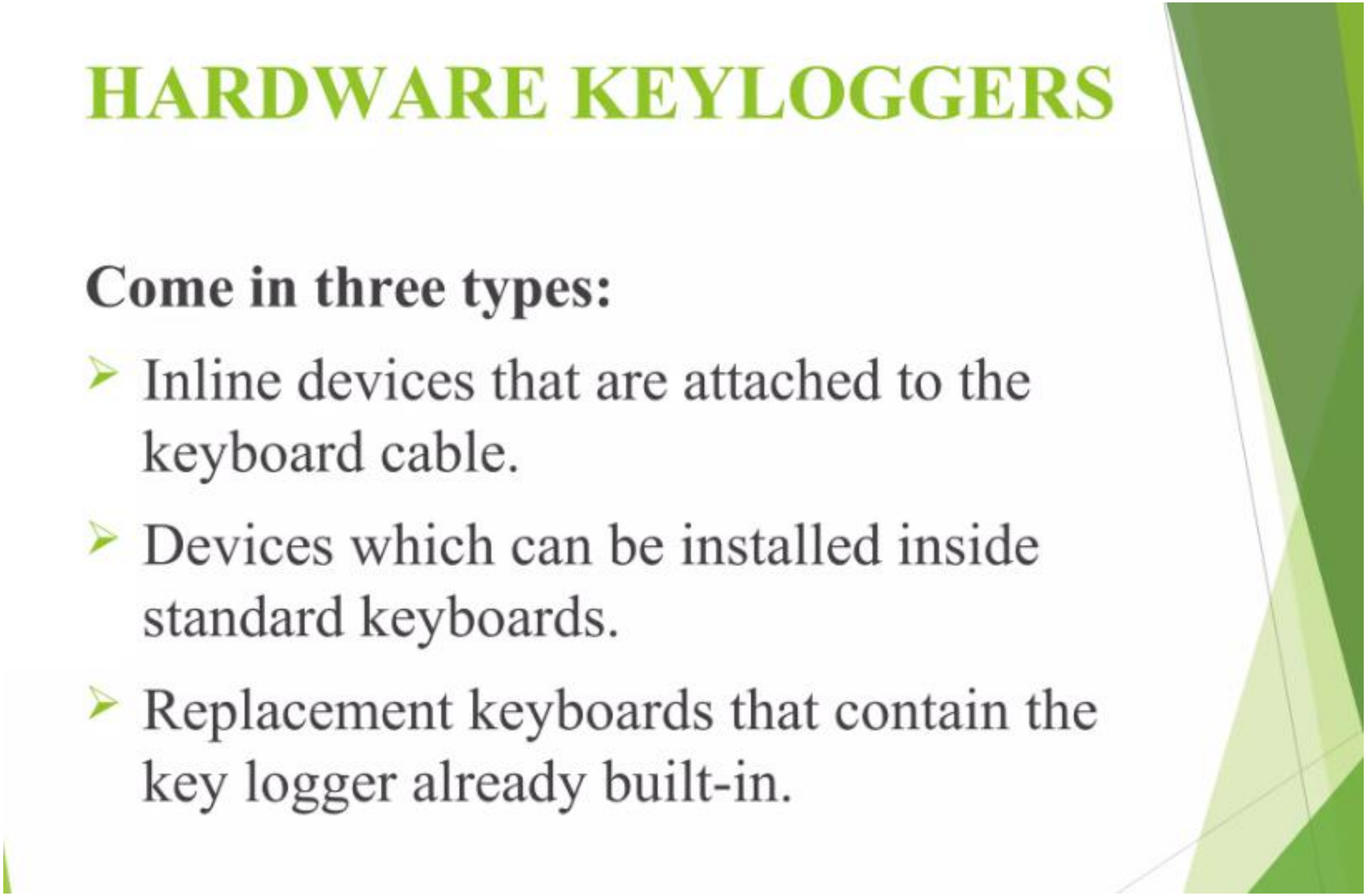
Hardware-based Keylogger

HARDWARE KEYLOGGER

✓ Hardware keyloggers are used for keystroke logging, a method of capturing and recording computer users' keystrokes, including sensitive passwords.

✓ Generally, recorded data is retrieved by typing a special password into a computer text editor.

✓ The hardware keyloggers plugged in between the keyboard and computer detects that the password has been typed and then presents the computer with "typed" data to produce a menu.



HARDWARE KEYLOGGERS

Come in three types:

- Inline devices that are attached to the keyboard cable.
- Devices which can be installed inside standard keyboards.
- Replacement keyboards that contain the key logger already built-in.

SOME HARDWARE KEYLOGGERS

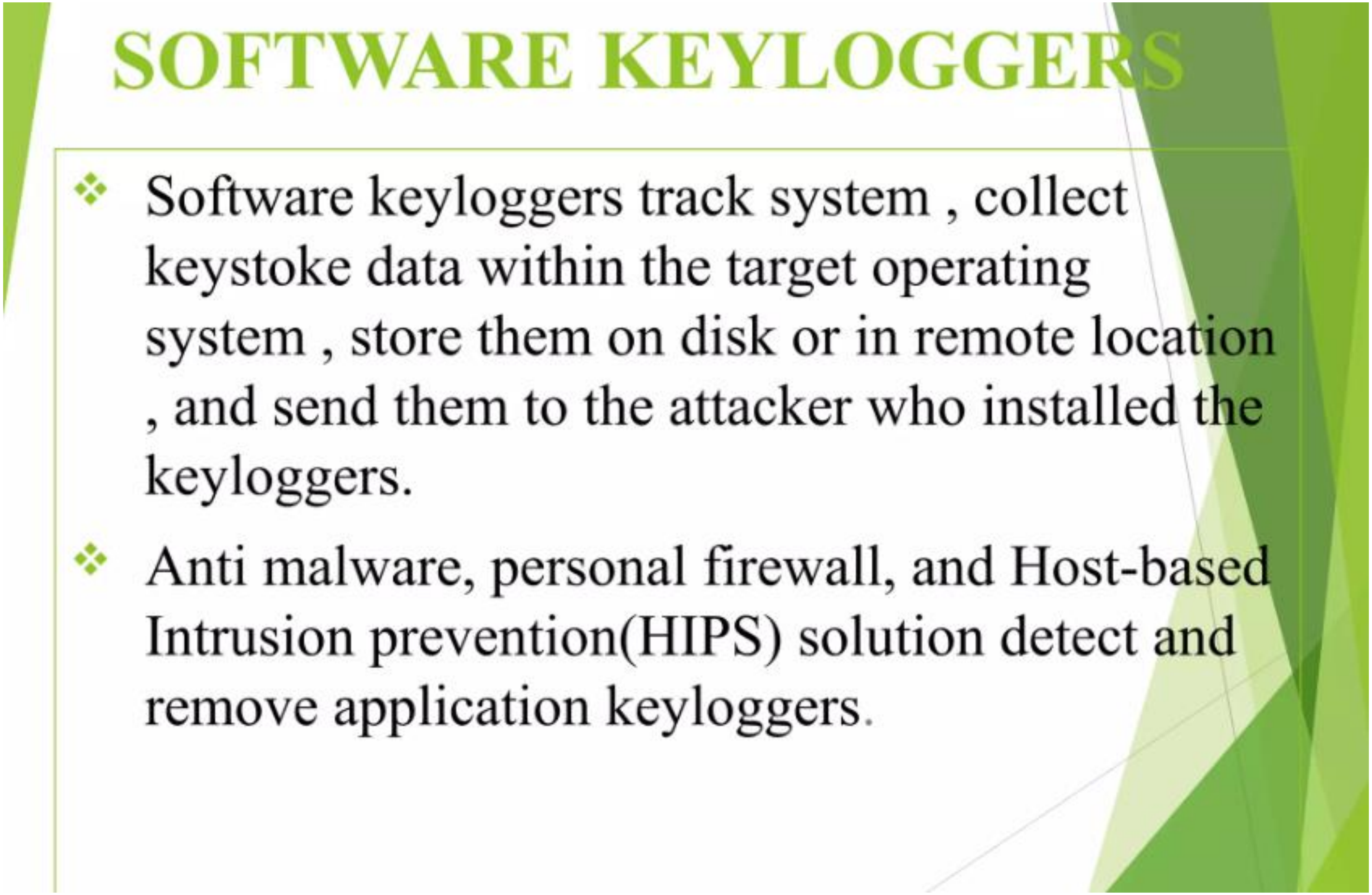
- Hardware KeyLogger Stand-alone Edition
  a tiny hardware device that can be attached in between a keyboard and a computer.
- Hardware KeyLogger Keyboard Edition
  looks and behaves exactly like a normal keyboard, but it keeps a record of all keystrokes typed on it.
- KeyGhost Hardware Keylogger
  a tiny hardware device that can be attached in between a keyboard and a computer.
- KeyKatcher Keystroke Logger
  a tiny hardware device that can be attached in between a keyboard and a computer.

✓ **Advantages :**

1. Antivirus techniques cannot catch these.
2. Work on all computing platforms.

✓ **Disadvantages :**

1. It can be spotted by a suspicious user.



SOFTWARE KEYLOGGERS

- Software keyloggers track system , collect keystoke data within the target operating system , store them on disk or in remote location , and send them to the attacker who installed the keyloggers.
- Anti malware, personal firewall, and Host-based Intrusion prevention(HIPS) solution detect and remove application keyloggers.

Software keylogger detection methods include:

- Scan local drive for log.txt or other log file names associate with known keyloggers.
- Implement solution that detect unauthorized file transfer via FTP or other protocols;
- Scan content sent via email or other authorized means looking for sensitive information;
- Detect encrypted files transmitted to questionable destinations.

Advantages :

1. Are hard to detect
2. Can be deployed remotely via a software vulnerability attack
3. Are fairly easy to write

Disadvantage :

1. A good antivirus scheme could sniff these out.
2. Far fewer cons with the software, so these are much more common than hardware-type keyloggers.

EXAMPLE OF WINDOWS KEYLOGGERS

- Badtrans : a keylogger worm that exploited vulnerability in outlook express and internet explorer. It collect keystrokes and them to various e mail address.
- Magic lantern: FBI’s own software to wire tap|log email passing through ISPs.