Module 3

:

Tools and Methods Used in Cybercrime

Syllabus:

Module 3: Tools and Methods used in Cybercrime: Introduction, Proxy servers and anonymizers, Phishing, Password cracking, Key loggers and spywares, Trojan horses and backdoors, Steganography.

SLT: Virus and Worms

Introduction:

- **The basic stages of an attack are**:

1. Initial Uncovering
2. Network Probe
3. Crossing the line toward electronic crime(E-Crime)
4. Capturing the network
5. Grab the data
6. Covering Tracks

1. **Initial Uncovering:**

- Reconnaissance
- Uncovers the information

2. **Network Probe:**

- Uses invasive techniques to scan the information.
- Ping sweep
- Port scanning tool

3. **Crossing the line towards electronic crime (E-Crime):**

- Make use of all possible holes on the target system.
- They use common gateway interface (CGI).
- Easiest way to gain an entry is by checking for default login accounts or empty passwords.

4. **Capturing the network:**

- At this stage, the attacker attempts to “own” the network.
- The attacker gains the foothold in the internal network quickly and easily of target system.
- The next step is to remove any evidence of the attack. There are number of hacking tools, that the attacker will install to clean up log files and remove any trace of an intrusion.

5. **Grab the data:**

- Attacker has “captured the network”.
- Steal the confidential data, customer credit card information etc.
- Launch attacks at other sites from victim’s network.

6. **Covering Tracks:**

- This refers to the activities undertaken by the attacker to extend misuse of the system without being detected.
- The attacker remain undetected for long periods.

- During this entire 6 stages, the attacker takes optimum care to hide his/her identity from the first step itself.

Table 4.2 | Tools used to cover tracks

Sr. No.	*Website*	*Brief Description*
1	http://www.ibt.ku.dk/jesper/ELSave/	**ELSave:** It is a tool to save and/or clear an NT event log. ELSave is written by Jesper Lauritsen. The executable is available on the weblink, but source code is not available.
2	http://ntsecurity.nu/toolbox/winzapper/	**WinZapper:** This tool enables to erase event records selectively from the security log in Windows NT 4.0 and Windows 2000. This program corrupts the event logs, therefore, they must be cleared completely.
3	http://www.evidence-eliminator.com/	**Evidence eliminator:** It is simple and one of the top-quality professional PC cleaning program that is capable of defeating all known investigative Forensic Software. Evidence eliminator permanently wipes out evidence so that forensic analysis becomes impossible.
4	http://www.traceless.com/computer-forensics/	**Traceless:** It is a privacy cleaner for Internet explorer (IE) that can delete common Internet tracks, including history, cache, typed URLs, cookies, etc.

Sr. No.	*Website*	*Brief Description*
5	http://www.acesoft.net/	**Tracks Eraser Pro:** It deletes following history data: • Delete address bar history of IE, Netscape, AOL, Opera. • Delete cookies of IE, Netscape, AOL, Opera. • Delete Internet cache (temporary Internet files). • Delete Internet history files. • Delete Internet search history. • Delete history of autocomplete. • Delete IE plugins (selectable). • Delete index.dat file. • Delete history of start menu run box. • Delete history of start menu search box. • Delete windows temp files. • Delete history of open/save dialog box. • Empty recycle bin.

Proxy Servers and Anonymizers:

- ***Proxy server*** is a computer on the network which acts as an intermediary for connections with other computers on that network.
- The attacker first connect to a proxy server and establish the connection with the target system.
- This enables an attacker to surf on the web anonymously and hide the attack.

➢**Example:** A client connects to the proxy server and requests some services available from a different server.

➢The proxy server evaluates the request and provides the resource by establishing the connection to the respective server and requests the required service on behalf of the client.

- A proxy server can allow an attacker to hide ID.

- A **proxy server** has following **purposes**:

1. Keep the systems behind the curtain.
2. Speed up access to a resource (through “caching”). It is usually used to cache the webpages from a web server.
3. Specialized proxy servers are used to filter unwanted content such as advertisements.
4. Proxy server can be used as IP address multiplexer to enable to connect number of computers on the internet, whenever one has only one IP address.

- **Advantage of proxy server**: its cache memory can serve all users.

- An ***anonymizer*** or an ***anonymous proxy*** is a tool that attempts to make activity on the internet untraceable.
- It accesses the internet on the user's behalf, protecting personal information by hiding the source computer's identifying information.
- In 1997, the first anonymizer software tool was created by Lance Cottrell, developed by Anonymizer.com
- The anonymizer hides/remove all the identifying information from a user's computer while the user surfs on the Internet, which ensures the privacy of the user.

Phishing:

- ***Phishing*** is a process of stealing personal and financial data and can also infect systems with viruses and a method of online ID theft in various cases.

➢**Example**: While checking E-Mail one day a user finds a message from the bank threatening him/her to close the bank account if he/she does not reply immediately.

➢Although the message seems to be suspicious from the contents of the message, it is difficult to conclude that it is a false/ fake E-Mail.

- Most people associate Phishing with E-Mail messages that spoof or mimic banks, credit card companies or other business such as Amazon.
- These messages look authentic and attempt to get users to reveal their personal information.

- **How Phishing works?**

1. Planning
2. Setup
3. Attack
4. Collection
5. Identity theft and Fraud

Password Cracking:

- Password is like a key to get an entry into computerized system like a lock.
- **Password cracking** is a process of recovering passwords from data that have been stored in or transmitted by a computer system.
- Usually, an attacker follows a common approach- repeatedly making guesses for the password.
- The **purpose of password cracking** is as follows:

1. To recover a forgotten password.
2. As a preventive measure by system administrators to check for easily crackable passwords.
3. To gain unauthorized access to a system.

- **Manual password cracking** is to attempt to logon with different passwords.
- The **attacker follows the following steps**:

1. Find a valid user account such as an Administrator or Guest;
2. Create a list of possible passwords;
3. Rank the passwords from high to low probability;
4. Key-in each password;
5. Try again until a successful password is found.

- Passwords can be guessed sometimes with knowledge of the user's personal information.

➢**Example**: User's DOB, Vehicle number, Mobile number etc.

- An attacker can also create a script file (e.g.: Automated programs) which will be executed to try each password in a list.
- Passwords are stored in a database and password verification process is established into the system when a user attempts to login or access a restricted resource.
- To ensure confidentiality of passwords, the password verification data is usually not stored in a clear text format.

➢**Example:** One-way Function (either encryption function or cryptographic hash) is applied to the password.

➢The most commonly used hash functions can be computed rapidly, and the attacker can text these hashes with the help of password cracking tools to get the plain text password.

Password Cracking Tools:

Website	*Brief Description*
www.defaultpassword.com	**Default password(s):** Network devices such as switches, hubs and routers are equipped with "default passwords" and usually these passwords are not changed after commissioning these devices into the network (i.e., into LAN). The intruders can gain the access using these default passwords by visiting the said website.
http://www.oxid.it/cain.html	**Cain & Abel:** This password recovery tool is typically used for Microsoft Operating Systems (OSs). It allows to crack the passwords by sniffing the network, cracking encrypted passwords using dictionary, brute force attacks, decoding scrambled passwords and recovering wireless network keys.
http://www.openwall.com/john	**John the Ripper:** This is a free and open-source software – fast password cracker, compatible with many OSs like different flavors of Unix, Windows, DOS, BeOS and OpenVMS. Its primary purpose is to detect weak Unix passwords.
http://freeworld.thc.org/thc-hydra	**THC-Hydra:** It is a very fast network logon cracker which supports many different services.
http://www.aircrack-ng.org	**Aircrack-ng:** It is a set of tools used for wireless networks. This tool is used for 802.11a/b/g wired equivalent privacy (WEP) and *Wi*-Fi *P*rotected *A*ccess (WPA) cracking. It can recover a 40 through 512-bit WEP key once enough encrypted packets have been gathered. It can also attack WPA 1 or 2 networks using advanced cryptographic methods or by brute force.

Website	*Brief Description*
http://www.solarwinds.com	**SolarWinds:** It is a plethora of network discovery/monitoring/attack tools and has created dozens of special-purpose tools targeted at systems administrators. Security-related tools include many network discovery scanners, a Simple Network Management Protocol (SNMP) brute force cracker, router password decryption and more.
http://www.foofus.net/fizzgig/pwdump	**Pwdump:** It is a Window password recovery tool. Pwdump is able to extract NTLM and LanMan hashes from a Windows target, regardless of whether Syskey is enabled. It is also capable of displaying password histories if they are available.
http://project-rainbowcrack.com	**RainbowCrack:** It is a hash cracker that makes use of a large-scale time-memory trade-off. A traditional brute force cracker tries all possible plain texts one by one, which can be time-consuming for complex passwords. RainbowCrack uses a time-memory trade-off to do all the cracking-time computation in advance and store the results in so-called "rainbow tables." It does take a long time to precompute the tables but RainbowCrack can be hundreds of times faster than a brute force cracker once the precomputation is finished.
http://www.hoobie.net/brutus	**Brutus:** It is one of the fastest, most flexible remote password crackers available for free. It is available for Windows 9x, NT and 2000. It supports HTTP, POP3, FTP, SMB, TELNET, IMAP, NTP and more.

Website	*Brief Description*
http://www.l0phtcrack.com	**L0phtCrack:** It is used to crack Windows passwords from hashes which it can obtain from stand-alone Windows workstations, networked servers, primary domain controllers or Active Directory. It also has numerous methods of generating password guesses (dictionary, brute force, etc.).
http://airsnort.shmoo.com	**AirSnort:** It is a wireless LAN (WLAN) tool which recovers encryption keys. It operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered. It requires approximately 5–10 million encrypted packets to be gathered. Once enough packets have been gathered, AirSnort can guess the encryption password in under a second. It runs under Windows or Linux.

- **Password cracking attacks can be classified under three categories as follows**:

1. Online attacks
2. Offline attacks
3. Non-electronic attacks

1. **Online Attacks**:

- An attacker can create a script file that will be executed to try each password in a list and when matches, an attacker can gain the access to the system.
- The most popular online attack is "**man-in-the middle (MITM) attack**", also termed as '**bucket-brigade attack**' or sometimes '**Janus attack**'.
- MITM attack is a form of active eavesdropping in which the attacker establishes a connection between a victim and the server to which a victim is connected.
- When a victim client connects to the fraudulent server the MITM server intercepts the call, hashes the password and passes the connection to the victim server.
- This type of attack is used to obtain the password for E-Mail accounts on public websites such as Yahoo, Hotmail, and Gmail and can also used to get the passwords for financial websites that would like to gain the access to banking websites.

2. **Offline Attacks**:

- ***Offline attacks*** are performed from a location other than the target where these passwords reside or are used.
- Offline attacks usually require physical access to the computer and copying the password file from the system onto removable media.
- **Different types of offline password attacks**:

Type of Attack	Description	Example of a Password
1. Dictionary Attack	Attempts to match all the words from the dictionary to get the password.	Administrator
2. Hybrid Attack	Substitutes numbers and symbols to get the password	AdmInIstrator
3. Brute force Attack	Attempts all possible permutation-combinations of letters, numbers, and special characters	Adm!n@09

3. **Strong, Weak, and Random Passwords:**

- A ***weak password*** is one, which could be easily guessed, short, common, and a system default password that could be easily found by executing a brute force attack and by using a subset of all possible passwords.
- Passwords that can be easily guessed by acquaintances of the netizens (such as DOB, pet's name) are considered to be very short.

➢**Examples of weak passwords are**:

1. Susan: Common personal name;
2. aaaa: Repeated letters, can be guessed;
3. Abc123: can be easily guessed;
4. Admin: can be easily guessed;
5. 12/3/75: date, possibly of personal importance;
6. December12

- A ***strong password*** is long enough, random or otherwise difficult to guess-producible only by the user who choose it.
- The length of time deemed to be too long will vary with the attacker, the attacker's resource, the ease wit which a password can be tried and the value of the password to the attacker.
- A password controlling access to large bank's electronic money transfer system might be worth many weeks of computer time for trying to crack it.

➢**Examples of strong passwords:**

1. Convert_$100 to Euros!
2. 382456390H
3. 4pRtelai@3
4. MoOoOfln245679
5. t3wahSetyeT4

4. **Random Passwords:**

- Password is stronger if it includes a mix of upper- and lower-case letters, numbers and other symbols, when allowed, for the same number of characters.
- The difficulty in remembering such a password increases the chance that the user will write down the password, which makes it more vulnerable to a different attack.
- A password can, at first sight, be random, but if we really examine it, it is just a pattern. One of these types of passwords is 26845. Although short, it is not easily guessed.
- Forcing the users to use system-created random passwords ensures that the password will have no connection with that user and should not be found in any dictionary.
- Almost all OS's include password aging;

The general guidelines applicable to the password policies, which can be implemented organization-wide are as follows:

1. Passwords and user logon identities (IDs) should be unique to each authorized user.
2. Passwords should consist of a minimum of eight alphanumeric characters (no common names or phrases).
3. There should be computer-controlled lists of prescribed password rules and periodic testing (e.g., letter and number sequences, character repetition, initials, common words and standard names) to identify any password weaknesses.
4. Passwords should be kept private, that is, not shared with friends, colleagues, etc. They shall not be coded into programs or noted down anywhere.
5. Passwords shall be changed every 30/45 days or less. Most operating systems (OSs) can enforce a password with an automatic expiration and prevent repeated or reused passwords.
6. User accounts should be frozen after five failed logon attempts. All erroneous password entries should be recorded in an audit log for later inspection and action, as necessary.
7. Sessions should be suspended after 15 minutes (or other specified period) of inactivity and require the passwords to be re-entered.
8. Successful logons should display the date and time of the last logon and logoff.
9. Logon IDs and passwords should be suspended after a specified period of non-use.
10. For high-risk systems, after excessive violations, the system should generate an alarm and be able to simulate a continuing session (with dummy data) for the failed user (to keep this user connected while personnel attempt to investigate the incoming connection).

Netizens should practice password guidelines to avoid being victim of getting their personal E-Mail accounts hacked/ attacked by the attackers.

1. Passwords used for business E-Mail accounts, personal E-Mail accounts (Yahoo/Hotmail/Gmail) and banking/financial user accounts (e.g., online banking/securities trading accounts) should be kept separate.
2. Passwords should be of minimum eight alphanumeric characters (common names or phrases should be phrased).
3. Passwords should be changed every 30/45 days.
4. Passwords should not be shared with relatives and/or friends.
5. Password used previously should not be used while renewing the password.
6. Passwords of personal E-Mail accounts (Yahoo/Hotmail/Gmail) and banking/financial user accounts (e.g., online banking/securities trading accounts) should be changed from a secured system, within couple of days, if these E-Mail accounts has been accessed from public Internet facilities such as cybercafes/hotels/libraries.
7. Passwords should not be stored under mobile phones/PDAs, as these devices are also prone to cyber-attacks (explained in Section 3.8, Chapter 3).
8. In the case of receipt of an E-Mail from banking/financial institutions, instructing to change the passwords, before clicking the weblinks displayed in the E-Mail, legitimacy of the E-Mail should be ensured to avoid being a victim of Phishing attacks (we will explain Phishing attack in detail in Chapter 5).
9. Similarly, in case of receipt of SMS from banking/financial institutions, instructing to change the passwords, legitimacy of the E-Mail should be ensured to avoid being a victim of Smishing attacks (explained in detail in Chapter 3).
10. In case E-Mail accounts/user accounts have been hacked, respective agencies/institutes should be contacted immediately.

Keyloggers and Spywares:

- Keystroke logging, from called keylogging, is the practice of noting (or logging) the keys struck on a keyboard, typically in a convert manner so that the person using the keyboard is unaware that such actions are being monitored.
- Keystroke logger or keylogger is quicker and easier way of capturing the passwords and monitoring the victims IT savvy behavior.
- It can be classified as **software keylogger** and **hardware keylogger**.

1. **Software Keyloggers:**

- These are software programs installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded.
- Software keyloggers are installed on a computer system by Trojans or viruses without the knowledge of the user.
- Cybercriminals always install such tools on the insecure computer systems available in public places and can obtain the required information about the victim very easily.
- A keylogger usually consists of two files that get installed in the same directory: a dynamic link library (DLL) file and an EXEcutable (EXE) file that installs the DLL file and triggers it to work. DDL does all the recording of keystrokes.

Table 4.5 | Software keyloggers

Website	*Brief Description*
http://www.soft-central.net	**SC-KeyLog PRO:** It allows to secretly record computer user activities such as E-Mails, chat conversations, visited websites, clipboard usage, etc. in a protected logfile. SC-KeyLog PRO also captures Windows user logon passwords. The captured information is completely hidden from the user and allows to remotely install the monitoring system through an E-Mail attachment without the user recognizing the installation at all.
http://www.spytech-web.com	**Spytech SpyAgent Stealth:** It provides a large variety of essential computer monitoring features as well as website and application filtering, chat blocking and remote delivery of logs via E-Mail or FTP.
http://www.relytec.com	**All In One Keylogger:** It is an invisible keystrokes recorder and a spy software tool that registers every activity on the PC to encrypted logs. This keylogger allows secretly tracking of all activities from all computer users and automatically receiving logs to a desired E-Mail/FTP accounting. With this keylogger, one can read chat conversations, look at the E-Mails as well as watch the sites that have been surfed.
http://www.stealthkeylogger.org	**Stealth Keylogger:** It is a computer monitoring software that enables activity log report where the entire PC keyboard activities are registered either at specific time or hourly on daily basis. The entire log reports are generated either in text or HTML file format as defined by the user. The keylogger facilitates mailing of log report at the specified E-Mail address.
http://www.blazingtools.com	**Perfect Keylogger:** It has its advanced keyword detection and notification. User can create a list of "on alert" words or phrases and keylogger will continually monitor keyboard typing, URLs and webpages for these words or phrases – for example, "bomb," "sex," "visiting places around Mumbai" and "Windows vulnerabilities." When a keyword is detected, perfect keylogger makes screenshot and sends E-Mail notification to the user.

makes screenshot and

http://kgb-spy-software.en.softonic.com

KGB Spy: It is a multifunctional keyboard tracking software, widely used by both regular users and IT security specialists. This program does not just record keystrokes but is also capable of recording language-specific characters. It records all typed data/all keyboard activity. It can be used to monitor children's activity at home or to ensure employees do not use company's computers inappropriately. Visit www.refog.com to find more on this product.

http://www.spy-guide.net/spybuddy-spy-software.htm

Spy Buddy: This, along with keylogger, has following features:

- Internet conversation logging;
- disk activity logging;
- Window activity logging;
- application activity logging;
- clipboard activity logging;
- AOL/Internet explorer history;
- printed documents logging;
- keylogger keystroke monitoring;
- websites activity logging;
- screenshot capturing;
- WebWatch keyword alerting

Website	*Brief Description*
http://www.elite-keylogger.com	**Elite Keylogger:** It captures every keystroke typed, all passwords (including Windows logon passwords), chats, instant messages, E-Mails, websites visited, all program launched, usernames and time they worked on the computer, desktop activity, clipboard, etc.
http://www.cyberspysoftware.com	**CyberSpy:** It provides an array of features and easy-to-use graphical interface along with computer monitoring capabilities such as keep tabs on the employees and keeps track of what children are viewing on the Internet. CyberSpy can be used as complete PC monitoring solution for any home or office. CyberSpy records all websites visited, instant message conversations, passwords, E-Mails and all keystrokes pressed. It also has the ability to provide screenshots at set intervals.
http://www.mykeylogger.com	**Powered Keylogger:** Powered keylogger can be used for the following: • *Surveillance:* It is for anyone to control what happens on the computer when the computer's owner is away. • *Network administration:* It is for network administrators to control outgoing traffic and sites visited. • *Shared PC activity tracking:* It is to analyze the usage of shared PC. • *Parental control:* It helps parents to monitor their children's computer and Internet activity. • *Employee productivity monitoring:* It helps managers to check and increase productivity of their stuff or just to prevent the leak of important information.

2. Hardware Keyloggers:

- To install these keyloggers, physical access to the computer system is required.
- Hardware keyloggers are small hardware devices.
- These are connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device.
- Cybercriminals install such devices on ATM machines to capture ATM cards PINs.
- Each keypress on the keyboard of the ATM gets registered by these keyloggers.
- These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence.

➢ **Antikeylogger**:

- Antikeylogger is a tool that can detect the keylogger installed on the computer system and also can remove the tool.
- **Advantages of using antikeylogger are as follows**:

1. Firewalls cannot detect the installations of keyloggers on the systems; hence, antikeyloggers can detect installations of keyloggers.
2. This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs; if not updated, it does not serve the purpose, which makes the users at risk.
3. Prevents Internet banking frauds. Passwords can be easily gained with the help of installing keyloggers.
4. It prevents ID theft.
5. It secured E-Mail and instant messaging/chatting.

➢ **Spywares**:

- Spyware is a type of malware that is installed on computers which collects information about users without their knowledge.
- The presence of Spyware is typically hidden from the user; it is secretly installed on the user's personal computer.
- Sometimes, Spyware such as keyloggers are installed by the owner of a shared, corporate or public computer on purpose to secretly monitor other users.
- The features and functions of such Spywares are beyond simple monitoring.
- Spyware programs collect personal information about the victim such as the Internet surfing habits/patterns and websites visited.
- Spyware can also redirect Internet surfing activities by installing another stealth utility on the user's computer system.

- Spyware may also have an ability to change computer settings, which may result in slowing of the Internet connection speeds and slowing of response time that may result into user complaining about the Internet speed connection with Internet Service Provider (ISP).
- To overcome the emergence of Spyware that proved to be troublesome for the normal user, anti-Spyware softwares are available in the market.
- Installation of anti-Spyware software has become a common element now-a-days from computer security practices perspective.

Table 4.6 | Spywares

Website	*Brief Description*
http://www.e-spy-software.com	**007 Spy:** It has following key features: • Capability of overriding "antispy" programs like "Ad-aware"; • record all websites URL visited in Internet; • powerful keylogger engine to capture all passwords; • view logs remotely from anywhere at anytime; • export log report in HTML format to view it in the browser; • automatically clean-up on outdated logs; • password protection.
http://www.spectorsoft.com	**Spector Pro:** It has following key features: • Captures and reviews all chats and instant messages; • captures E-Mails (read, sent and received); • captures websites visited; • captures activities performed on social networking sites such as MySpace and Facebook; • enables to block any particular website and/or chatting with anyone; • acts as a keylogger to capture every single keystroke (including usernames and passwords).
http://www.spectorsoft.com	**eBlaster:** Besides keylogger and website watcher, it also records E-Mails sent and received, files uploaded/downloaded, logging users' activities, record online searches, recording MySpace and Facebook activities and any other program activity.
http://www.remotespy.com	**Remotespy:** Besides remote computer monitoring, silently and invisibly, it also monitors and records users' PC without any need for physical access. Moreover, it records keystrokes (keylogger), screenshots, E-Mail, passwords, chats, instant messenger conversations and websites visited.

Website	*Brief Description*
http://www.topofbestsoft.com	**Stealth Recorder Pro:** It is a new type of utility that enables to record a variety of sounds and transfer them automatically through Internet without being notified by original location or source. It has following features: • Real-time MP3 recording via microphone, CD, line-in and stereo mixer as MP3, WMA or WAV formatted files; • transferring via E-Mail or FTP, the recorded files to a user-defined E-Mail address or FTP automatically; • controlling from a remote location; • voice mail, records and sends the voice messages.
http://www.amplusnet.com	**Stealth Website Logger:** It records all accessed websites and a detailed report can be available on a specified E-Mail address. It has following key features: • Monitor visited websites; • reports sent to an E-Mail address; • daily log; • global log for a specified period; • log deletion after a specified period; • hotkey and password protection; • not visible in add/remove programs or task manager.
http://www.flexispy.com	**Flexispy:** It is a tool that can be installed on a cell/mobile phone. After installation, Flexispy secretly records coversation that happens on the phone and sends this information to a specified E-Mail address.
http://www.wiretappro.com	**Wiretap Professional:** It is an application for monitoring and capturing all activities on the system. It can capture the entire Internet activity. This spy software can monitor and record E-Mail, chat messages and websites visited. In addition, it helps in monitoring and recording of keystrokes, passwords entered and all documents, pictures and folders viewed.

Trojan Horses and Backdoors:

- Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm, for example, ruining the file allocation table on the hard disk.
- A Trojan Horse may get widely redistributed as part of a computer virus.
- Like Spyware and Adware, Trojans can get into the system in a number of ways, including from a web browser, via E-Mail or in a handle with other software downloaded from the Internet.
- It is also possible to inadvertently transfer malware through a USB flash drive or other portable media.

- It is possible that one could be forced to reformat USB flash drive or other portable device to eliminate infection and avoid transferring it to other machines.
- Unlike virus and worms, Trojans do not replicate themselves, but they can be equally destructive.
- For example, waterfalls.scr is a waterfall screen saver as originally claimed by the author; however, it can be associated with malware and become a Trojan to upload hidden programs and allow unauthorized access to the user’s PC.

- **<u>Some typically examples of threats by Trojans are as follows</u>**:

1. They erase, overwrite or corrupt data on a computer.
2. They help to spread other malware such as viruses.
3. They deactivate or interfere with antivirus and firewall programs.
4. They allow remote access to the computer.
5. They upload and download files without user's knowledge.
6. They gather E-Mail addresses and use them for Spam.
7. They copy fake links to fake websites, display porno sites, play sounds/ videos and display images.
8. They slow down, restart or shutdown the system.
9. They reinstall themselves after being disabled.
10. They disable the task manager/ control panel.

➢ Backdoor:

- A backdoor is a means of access to a computer program that bypasses security mechanisms.
- A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes.
- Attackers often use backdoors that they detect or install themselves as part of an exploit.
- A backdoor works in background and hides from the user. Similar to virus, therefore difficult to detect and completely disable.
- A backdoor is one of the most dangerous parasite, as it allows a malicious person to perform any possible action on a compromised system.
- Most backdoors are autonomic malicious programs that must be somehow installed to a computer.

➢ What a Backdoor Does?

- Following are some functions of backdoor:

1. It allows the attacker to create, delete, rename, copy or edit any files, execute various commands; changes any system settings; alter the Windows registry; run, control and terminate applications; install arbitrary software and parasites.
2. It allows an attacker to control computer hardware devices, modify related settings, shutdown or restart a computer without asking for user permission.
3. It steals sensitive personal information, valuable documents, passwords, login names, ID details; logs user activity and tracks web browsing habits.
4. It records keystrokes that a user types on a computer's keyboard and captures screenshots.

5. It sends all gathered data to a predefined E-Mail address, upload it to a predetermined FTP server or transfers it through a background Internet connection to a remote host.
6. It infects files, corrupts installed applications and damages the entire system.
7. It distributes infected files to remote computers with certain security vulnerabilities and performs attacks against hacker-defined remote hosts.
8. It installs hidden FTP server that can be used by malicious persons for various illegal purposes.
9. It degrades Internet connection speed and overall system performance, decreases system security and causes software instability.
10. It provides no uninstall feature, and hides processes, files and other objects to complicate its removal as much as possible.

- **<u>Few examples of backdoor Trojans</u>**:

1. Back Orifice
2. Bifrost
3. SAP backdoors
4. Onapsis Bizploit

How to Protect from Trojan Horses and Backdoors:

- **Follow the following steps to protect the system from Trojan Horses and backdoors:**

1. Stay away from suspect websites/weblinks
2. Surf on the Web cautiously
3. Install antivirus/Trojan remover software

Steganography:

- Steganography is a Greek word that means “**sheltered writing**”.
- It is a method that attempts to hide the existence of a message or a communication.
- The word steganography comes from the 2 Greek words: **steganos** means “**covered**” and **graphein** means “**to write**” that means “**concealed writing**”.
- Given the sheer volume of data stored and transmitted electronically in the world today, it is no surprise that countless methods of protecting such data have evolved.
- One lesser known but rapidly growing method is steganography, the art and science of adding information so that it does not even appear to exist!
- The different names for steganography are **data hiding, information hiding** and **digital watermarking**.

- The term “cover” or “cover medium” is used to describe the original, innocent message, data, audio, still video and so on.
- It is the medium that hides the secret message.
- It must have a parts that can be altered or used without damaging or noticeably changing the cover media.
- If the cover media are digital, these alterable parts are called as redundant bits.
- These bits or a subset can be replaced with the message that is intended to be hidden.
- Steganography in digital media is very similar to “digital watermarking”. In other words, when steganography is used to place a hidden “trademark” in image, music and software, the result is a technique referred to as “watermarking”.

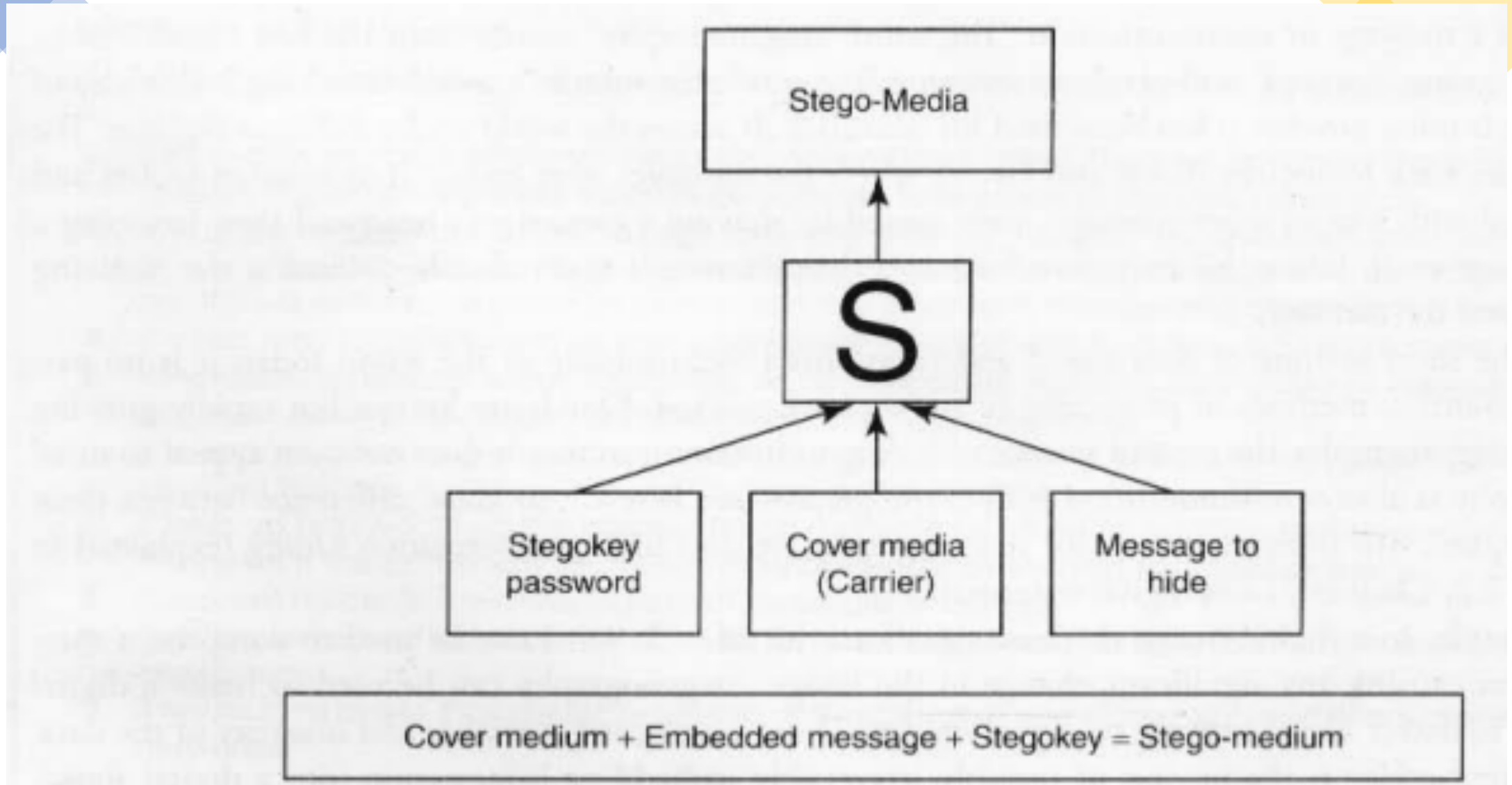

Figure 4.4 | How steganography works.

Table 4.10 | Steganography tools

Website	*Brief Description*
http://www.securityfocus.com	**DiSi-Steganograph:** It is a very small, DOS-based steganographic program that embeds data in PCX images.
http://www.brothersoft.com/invisible-folders-54597.html	**Invisible Folders:** It has the ability to make any file or folder invisible to anyone using your PC even on a network.
http://www.invisiblesecrets.com	**Invisible Secrets:** It not only encrypts the data and files for safe-keeping or for secure transfer across the Net but also hides them in places such as picture or sound files or webpages. These types of files are a perfect disguise for sensitive information.
http://www.programurl.com/stealth-files.htm	**Stealth Files:** It hides any type of file in almost any other type of file. Using steganography technique, Stealth Files compresses, encrypts and then hides any type of file inside various types of files (including EXE, DLL, OCX, COM, JPG, GIF, ART, MP3, AVI, WAV, DOC, BMP) and other types of video, image and executable files.
http://www.programurl.com/hermetic-stego.htm	**Hermetic Stego:** It is a steganography program that allows to encrypt and hide contents of any data file in another file so that the addition of the data to the container file will not noticeably change the appearance of that file. This program allows hiding a file of any size in one or more BMP image files with or without the use of a user-specified stego/encryption key so that (a) the presence of the hidden file is undetectable (even by forensic software using statistical methods) and (b) if a user-specified stego key is used then the hidden file can be extracted only by someone, using this software, who knows that stego key.
http://www.securstar.com/products_drivecryptpp.php	**DriveCrypt Plus (DCPP):** It has following features: • It allows secure hiding of an entire OS inside the free space of another OS. • Full-disk encryption (encrypts parts or 100% of your hard disk including the OS). • Preboot authentication (before the machines boots, a password is requested to decrypt the disk and start your machine).

➢ **Steganalysis**:

- Steganalysis is the art and science of getting messages that are hidden in images audio/video files using steganography.
- The goal of steganalysis is to identify suspected packages and to determine whether or not they have payload encoded into them, and if possible, recover it.
- Automated tools are used to detect such steganographed data/ information hidden in the image and audio and/or video files.

Virus and Worms:

- ***Computer* virus** is a program that can “infect” legitimate programs by modifying them to include a possibly “evolved” copy of itself.
- Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines.
- A computer virus passes from computer to computer.
- Viruses may also contain malicious instructions that may cause damage or annoyance.
- Viruses can often spread without any readily visible symptoms.
- A virus can start on event-driven effects, time driven effects, or can occur at random.

- **<u>Viruses can take some typical actions</u>**:

1. Display a message to prompt an action which may set of the virus;
2. Delete files inside the system into which viruses enter;
3. Scramble data on a hard disk;
4. Cause erratic screen behavior;
5. Halt the system (PC);
6. Just replicate themselves to propagate further harm.

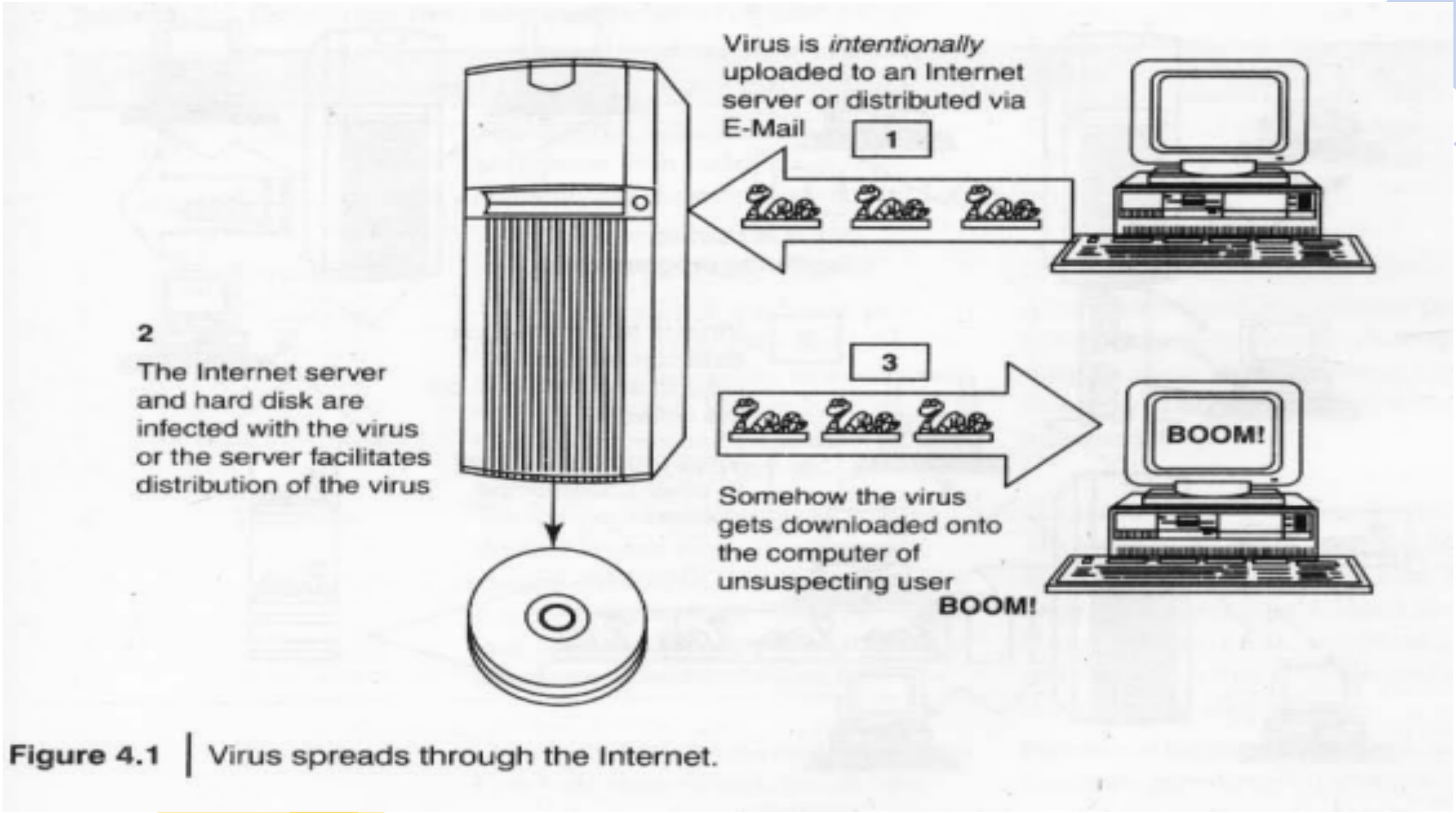

Figure 4.1 | Virus spreads through the Internet.

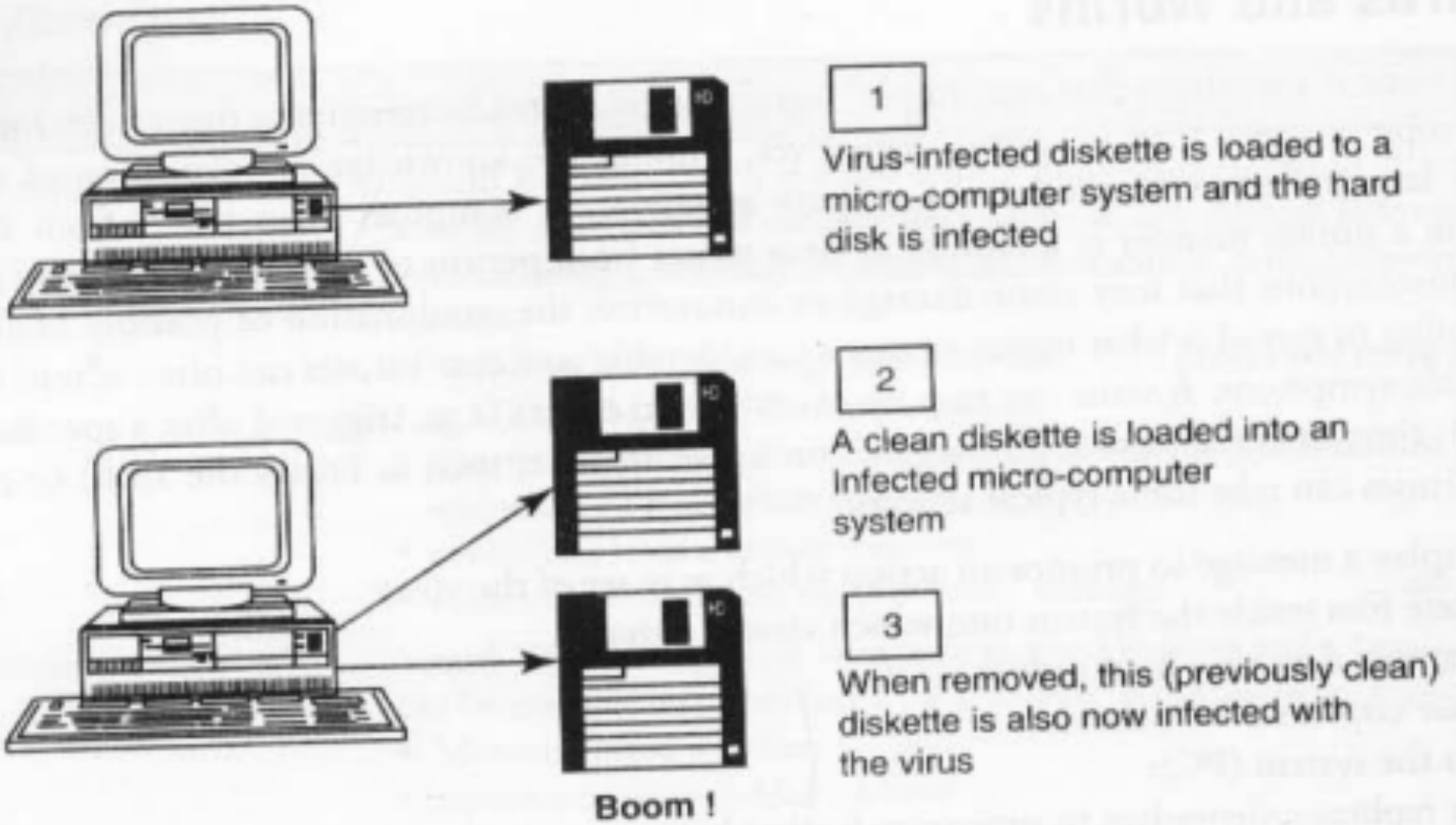

Figure 4.2 | Virus spreads through stand-alone system.

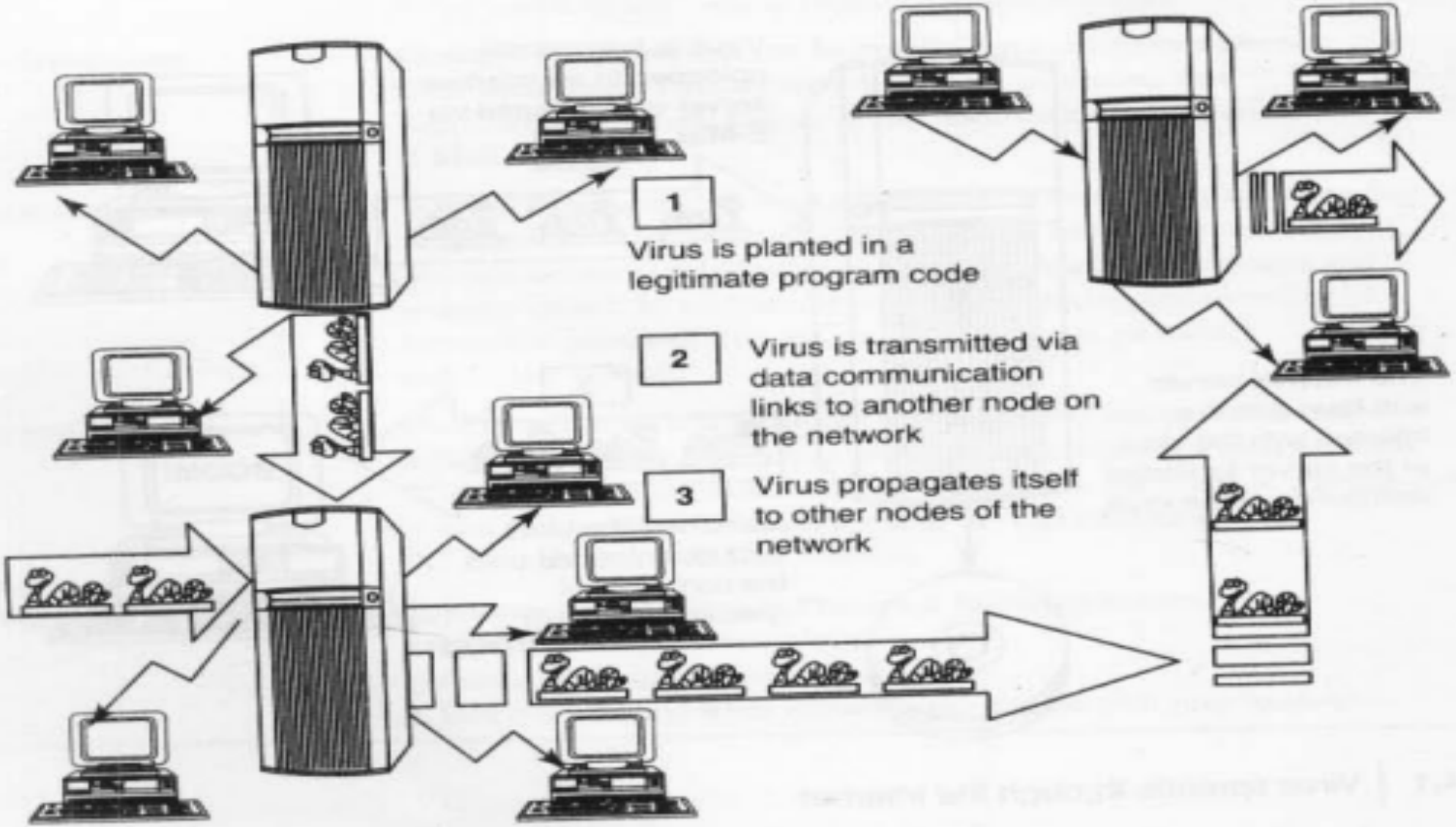

Figure 4.3 | Virus spreads through local networks.

- **Difference between Computer virus and worm:**

Sr. No.	Facet	Virus	Worm
1	Different types	Stealth virus, self-modified virus, encryption with variable key virus, polymorphic code virus, metamorphic code virus	E-Mail worms, instant messaging worms, Internet worms, IRC worms, file-sharing networks worms
2	Spread mode	Needs a host program to spread	Self, without user intervention
3	What is it?	A computer virus is a software program that can copy itself and infect the data or information, without the users' knowledge. However, to spread to another computer, it needs a host program that carries the virus	A computer worm is a software program, self-replicating in nature, which spreads through a network. It can send copies through the network with or without user intervention
4	Inception	The creeper virus was considered as the first known virus. It was spread through ARPANET in the early 1970s. It spreads through the TENEX OS and uses connected modem to dial out to a remote computer and infect it.	The name worm originated from The Shockwave Rider, a science fiction novel published in 1975 by John Brunner. Later researchers John F Shock and Jon A Hupp at Xerox PARC published a paper in 1982, *The Worm Programs* and after that the name was adopted
5	Prevalence	Over 100,000 known computer viruses have been there though not all have attacked computers (till 2005)	Prevalence for virus is very high as against moderate prevalence for a worm.

Types of Viruses:

1. Boot Sector viruses
2. Program viruses
3. Multipartite viruses
4. Stealth viruses
5. Polymorphic viruses
6. Macro viruses
7. Active X and Java Control

1. **Boot Sector Viruses:**

- It infects the storage media on which operating system is stored (e.g.: floppy diskettes and hard drives) and which is used to start the computer system.
- Entire data or programs are stored on the floppy disk and hard drives in smaller sections called sectors.
- The first sector is called the BOOT and it carries the master boot record(MBR).
- MBR's function is to read and load OS, that is, it enables the computer system to start through OS.
- Hence, if virus attacks an MBR or infects the boot record of the disk, such floppy disk infects victim's hard drive when he or she reboots the system while the infected disk is in the drive.
- Once the victim's hard drive is infected all the floppy diskette that are being used in the system will be infected.

2. **Program Viruses:**

- These viruses became active when the program file is executed.
- Once these program files (usually with extensions .bin, .com, .exe) gets infected, the virus make copies of itself and infects the other programs on the computer system.

3. **Multipartite Viruses:**

- It is a hybrid of a boot sector and program viruses.
- It infects program files along with the boot record when the infected program is active.
- When the victim starts the computer system next time, it will infect the local drive and other programs on the victim's computer system.

4. **Stealth Viruses:**

- It camouflages and/or masks itself and so detecting this type of virus is very difficult.
- It can disguise itself such a way that antivirus software also cannot detect it thereby preventing spreading into the computer system.
- It alters its file size and conceals itself in the computer memory to remain in the system undetected.
- The first computer virus, named as BRAIN, was a stealth virus.
- A good antivirus detects a stealth virus lurking on the victim's system by checking the areas the virus must have infected by leaving evidence in memory.

5. **Polymorphic Viruses:**

- It acts like a ‘Chameleon’ that changes its virus signature every time it spreads through the system.
- Hence, it is always difficult to detect polymorphic virus with the help of an antivirus program.
- Polymorphic generators are the routines(i.e., small programs) that can be linked with the existing viruses.
- The first all-purpose polymorphic generator was the mutation engine(MTE) published in 1991.

6. **Macroviruses:**

- Many applications such as Microsoft Word and Microsoft Excel, support MACRO's.
- These macros are programmed as a macro embedded in a document.
- Once a macrovirus gets onto a victim's computer then every document, he/she produce will be infected.
- This type of virus is relatively new and may get slipped by the antivirus software if the user does not have the most recent version installed on his/her system.

7. **Active X and Java Control:**

- All the web browsers have settings about active X and Java controls.
- Little awareness is needed about managing and controlling these settings of the web browser to prohibit and allow certain functions to work- such as enabling or disabling the pop ups, downloading the files and sound- which invites the threats for the computer system being targeted by unwanted software(s) floating in cyber space.