BVM Engineering College, VV Nagar

Gujarat Technological University

CYBER SECURITY

SEM 5
PRESENTATION

ANTIVIRUS

Electronics & Communication Dept.

Presented By :

1. Dharati Bhimani (140080111011)
2. Abhishek Budhbhatti (140080111012)
3. Chaitanya Tejaswi (140080111013)
4. Hemi Chaudhary (140080111015)
5. Darshi Contractor (140080111016)
6. Sarju Dadhaniya (140080111017)
7. Yash Dave(140080111018)
8. Devanshu Nandha (140080111020)
9. Drupad Pandya (140080111021)

Guided By:
Dr. Bhargav C Goradiya

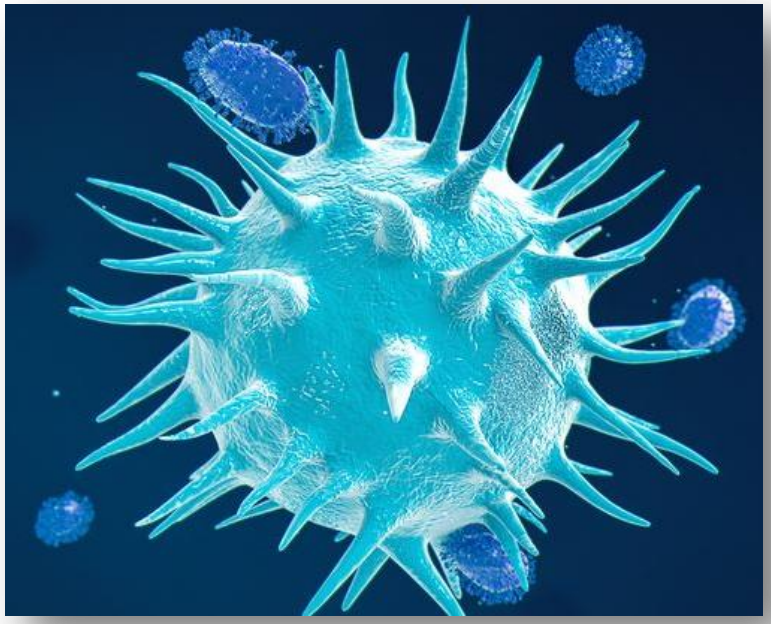
Content From:

1. https://en.wikipedia.org/wiki/Antivirus_software
2. https://cs.stanford.edu/people/eroberts/cs201/projects/viruses/anti-virus.html

Virus

Biological viruses copy themselves as a part of other organisms.

Similarly,
*"A **computer virus** is a program that is able to copy itself when it is run. Very often, computer viruses are run as a part of other programs."*



Operations & Functions of a Virus

Virus Parts

A viable computer virus must contain a search routine, which locates new files or new disks which are worthwhile targets for infection. Secondly, every computer virus must contain a routine to copy itself into the program which the search routine locates. The three main virus parts are:

1. Infection mechanism

Infection mechanism is how the virus spreads or propagates, a virus has a search routine, which locates new files or new disks for infection.

2. Trigger

Trigger is the compiled version that could be activated any time an executable with the virus is run that determines the event or condition for the payload to be activated or delivered such as a particular date, a particular time, particular presence of another program, capacity of the disk exceeding some limit, or a double-click that opens a particular file.

3. Payload

The payload is the actual body or data that perform the actual purpose of the virus. Payload activity might be noticeable, as most of the time it is the harmful activity, or some times non-destructive but distributive, which is called Virus hoax.

Operations & Functions of a Virus

Virus Phases

Virus phases is the life cycle of the computer virus, it can be divided into 4 phases:

1. Dormant Phase

The virus is idle. The virus will eventually be activated by the trigger which states which event will execute the virus, 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.

2. Triggering Phase

A dormant virus moves into this phase when it gets activated, it will now perform the function for which it was intended. 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.

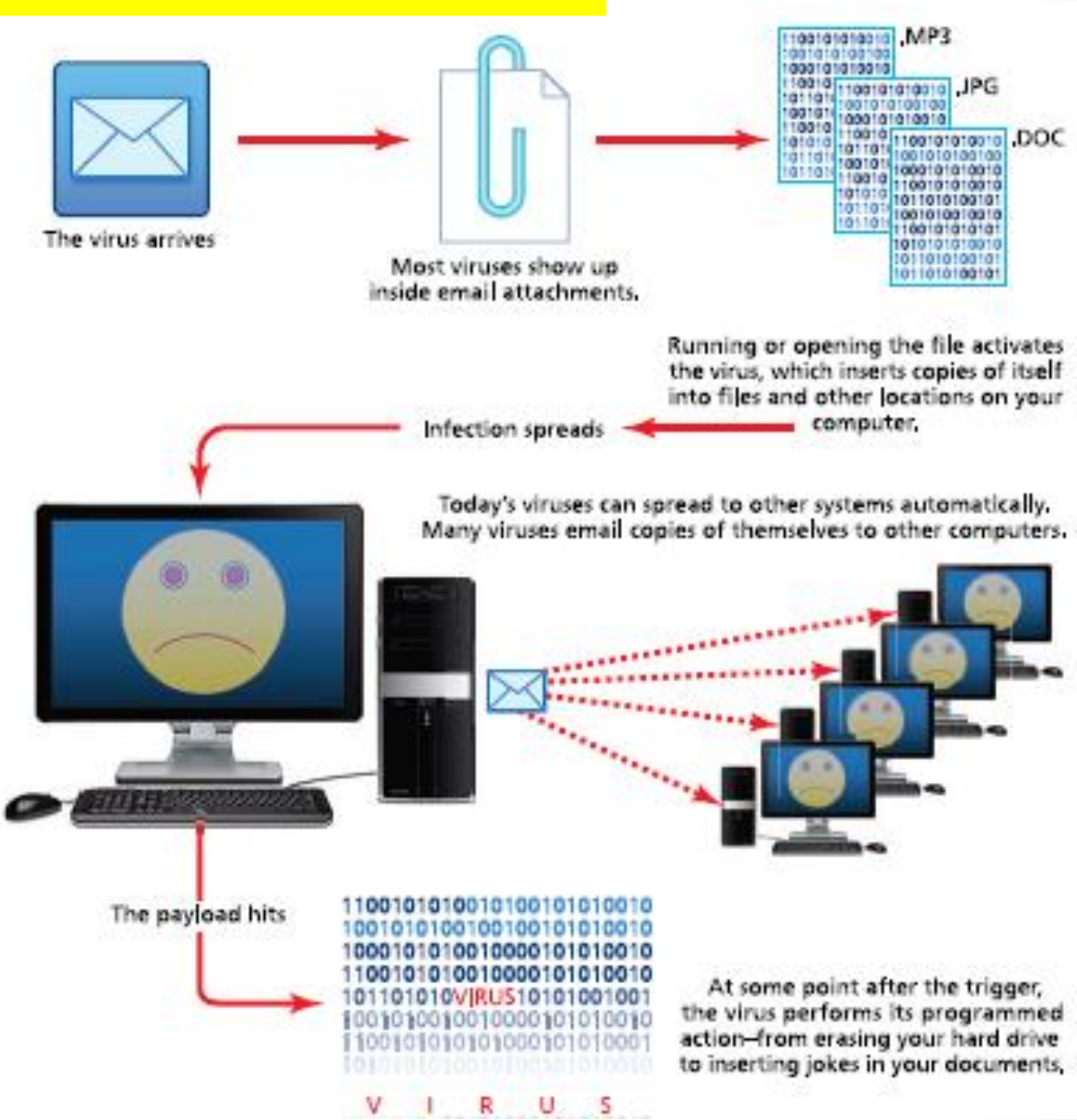
3. Propagation Phase

The virus starts propagating, that is multiplying itself. 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.

4. Execution Phase

This is the actual work of the virus, where the payload will be released. It can be destructive such as deleting files on disk or harmless such as popping messages on screen.

How a virus works



Kinds of Viruses

1. Macro-virus or script virus

These viruses infect the files created using some applications or programs that contain macros such as doc, pps, xls and mdb. They automatically infect the files with macros and also templates and documents that are contained in the file. They hide in documents shared through e-mail and networks.

Example: Relax, bablas, Melissa.A, 097M/Y2K

2. Memory Resident virus

They usually fix themselves inside the computer memory. They get activated every time the OS runs and end up infecting other opened files. They hide in RAM.

Example: CMJ, meve, randex, mrklunky

3. Boot sector virus

They specifically target the Boot sector/Master Boot Record (MBR) of the host's hard drive or removable storage media (flash drives, floppy disks, etc.)

Example: brain virus

4. Directory virus

They infect the computer's directory by changing the path indicating file location. They are usually located in the disk but affect the entire directory.

Example: dir-2 virus

5. Overwrite virus

They delete any information in a file they infect, leaving them partially or completely useless once they are infected. Once in the computer, they replaces all the file content but the file size doesn't change.

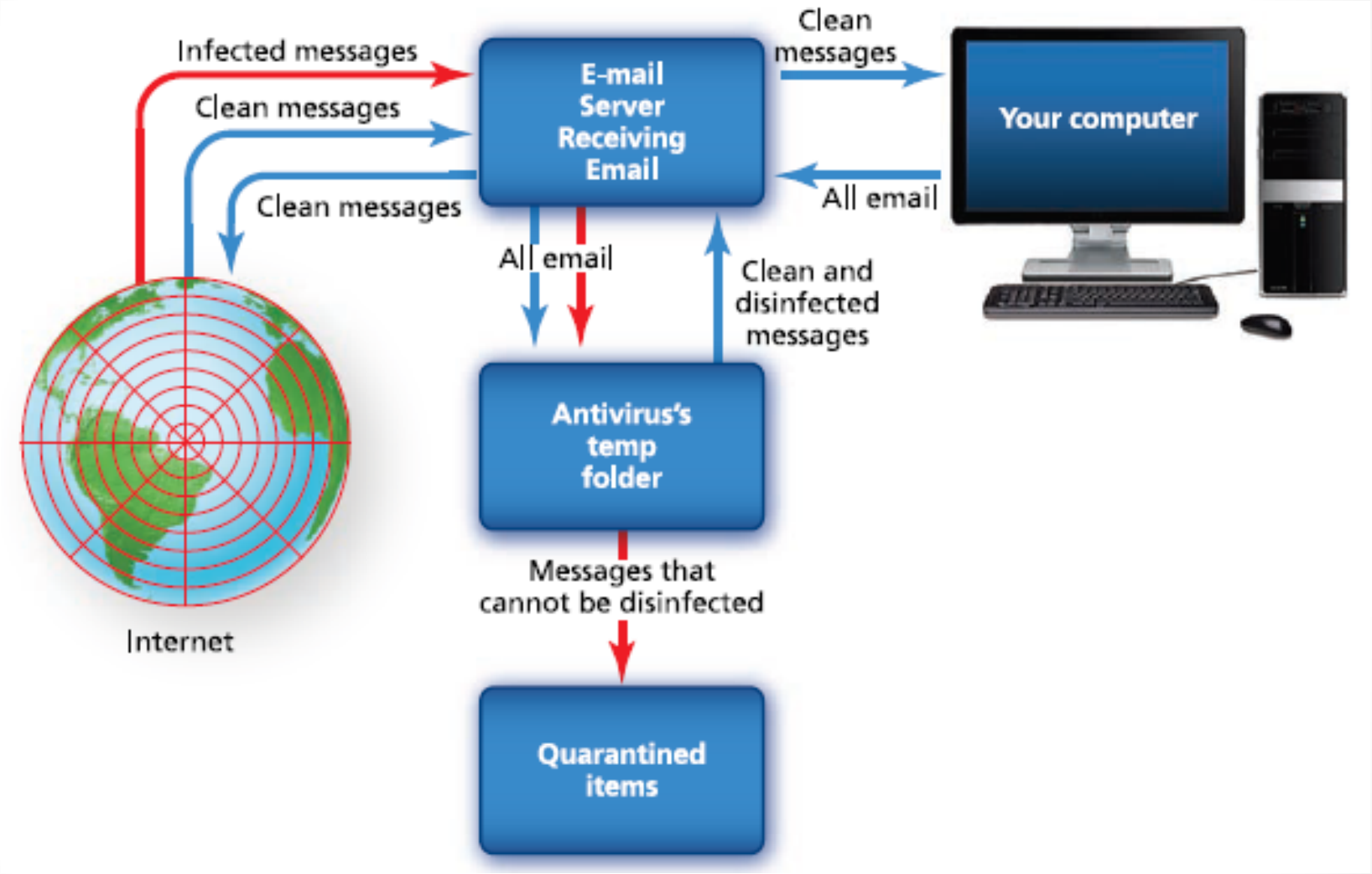
Example: Trj.Reboot, way, trivial.88.D

6. Web Scripting virus

Most web pages include some complex codes in order to create an interactive and interesting content. Such a code is often exploited to cause certain undesirable actions. They mostly originate from the infected web pages or browsers.

Example: JS.Fortnight – a virus that spreads via malicious emails.

Stopping a virus



Antivirus Software

Virus Detection Methods

There are four major methods of virus detection in use today:

Scanning

Integrity checking

Interception

Heuristic detection

Of these, scanning and interception are very common, with the other two only common in less widely-used anti-virus packages. Unfortunately, while scanning is very effective against known viruses, it is completely incapable of dealing with new viruses, forcing anti-virus analysis centers into a reactive stance.

Scanning

Definition: A scanner will search all files in memory, in the boot sector (the sector on disk that specifies where boot information is,) and on disk for code snippets that will uniquely identify a file as a virus.
Obviously, this requires a list of unique signatures that will be found in viruses and not in benign programs. To prevent false alarms, most scanners also will check the code of a suspected file against either the virus code itself or a checksum of it. (A checksum is a method frequently used to determine if data has been changed, and involves summing all of the bits in a file.) This is the most common method of virus detection available, and is implemented in all major anti-virus software packages.

Types:

1. On-access scans files when they are loaded into memory prior to execution.
2. On-demand scans all of main memory, the boot sector, and disk memory as well, and is started by a user when he/she wishes.

Advantages: Scanners **can find viruses that haven't executed yet** - this is critical for e-mail worms, which can spread themselves rapidly if not stopped. Also, false alarms have become extremely rare with the software available today. Finally, scanners are also very good at detecting viruses that they have the signatures for.

Disadvantages:

1. If the **software is using a signature string to detect the virus**, all a virus writer would have to do is modify the signature string to develop a new virus. This is seen in polymorphic viruses.
2. A **scanner can only scan for something it has the signature of**. The Maltese Amoeba virus was a very destructive virus that activated on November 11, 1991, and was able to spread rapidly before its activation without being detected. According to the 1991 Virus Bulletin: "Prior to November 2nd, 1991, no commercial or shareware scanner (of which VB has copies) detected the Maltese Amoeba virus. Tests showed that not ONE of the major commercial scanners in use ... detected this virus." Although virus updates occur more frequently today because of the Internet, viruses still cannot be detected until one has executed.

Integrity Checking

Definition: An integrity checker records integrity information about important files on disk, usually by check-summing. Should a file change due to virus activity or corruption, the file will no longer match the recorded integrity information. The user is prompted, and can usually be given an option to restore the file to its pre-corrupted/infected state. This is an extensive process, and few virus checkers today utilize it.

Advantages: Integrity checking is the only way to determine whether a virus has damaged a file, and it's fairly foolproof. Most integrity checkers today also have the benefit of detecting other damage to data, such as corruption, and can restore that as well.

Disadvantages:

1. The major problem with integrity checking is that **not enough companies offer comprehensive integrity checking software.**
2. Most anti-virus suites that do offer it **don't protect enough files**, and those that they do may not be damaged at all with newer viruses.
3. Simpler integrity checkers **won't be able to differentiate between damage done via corruption and damage done via a virus**, thus giving the user unclear information as to what's going on.
4. Finally, this **process is simply rather cumbersome** - in today's computers, many important files are changed by as little as booting up and shutting down, so integrity checkers need to be coupled with scanners for maximum efficacy in detecting viruses.

Heuristic Virus Checking

Definition: This is a generic method of virus detection. Anti-virus software makers develop a set of rules to distinguish viruses from non-viruses. Should a program or code segment follow these rules, then it is marked a virus and dealt with accordingly. This allows detection of any virus, and theoretically, should be sufficient to deal with any new virus attacks.

Advantages: Generic virus protection would make all other virus scanners obsolete and would be sufficient to stop any virus. The user doesn't need to download weekly virus updates anymore, because the software can detect all viruses.

Disadvantages:

1. Although these are huge benefits to heuristic virus checking, the **technology today is not sufficient**.
2. Virus writers can **easily write viruses that don't obey the rules**, making the current set of virus detection rules obsolete.
3. **Changes to these rules must be downloaded**, and thus these virus checkers must be updated and won't stop many new viruses, which gives them similar characteristics to scanners.
4. In addition, the **potential for false alarms and not detecting a known virus is greater** with heuristic checkers than with scanners.

Interception

Definition: Interception software detects virus-like behavior and warns the user about it.
How to detect virus-like behavior? Use heuristics again. Many viruses will perform some suspicious action, like relocating themselves in memory and installing themselves as resident programs. Many software packages have this as an option, although most people usually disable it.

Advantages: Interception is a good generic method to stop logic bombs and Trojan horses. Logic bombs will trigger a (usually destructive) sequence given an event, such as the date being set to a certain date. When not detected by scanners, interception software will usually detect the destructive and unusual sequences of events caused by logic bombs and Trojan horses.

Disadvantages:

1. Interceptors also **have all the drawbacks of heuristic systems** - difficulty differentiating virus from non-virus, and easy to program around.
2. Most **interceptors are very easy to disable**, and so many viruses frequently disable them before launching. Due to the nature of an interceptor, this software is unable to detect viruses before they launch, and a lot of damage could already have been done.
3. Lastly, interceptors are a nuisance **and frequently prompt the user to allow/disallow activity during software installations and system upgrades**, making the above very tedious. Combined with their limited usefulness, most software packages disable or strongly limit interception by default.

Problems with anti-virus software

Anti-virus software suffers from more problems than not being able to detect cutting edge viruses.

1. Many copies of anti-virus software are unable to detect even old viruses, because end users frequently forget or simply don't update their virus scanner's virus databases until it's too late.
2. On-demand scans are rarely performed because they're slow and hog resources while running, so dormant viruses tend to have a rather long life.
3. On-access scanners aren't free of troubles, either - some consume too many resources, so many users are tempted to disable them if they're on a slower machine.
4. Finally, while anti-virus software may become extremely good at sensing virus activity, there are always new security holes to exploit in operating system and networking software that would give viruses another entry point that bypasses the anti-virus software. Finding a security hole and getting reported on one of these sites is considered to be an honor among the virus writing community. An example of one of these sites is SANS, which has bulletins about hacker and virus attacks.

The bottom line? Anti-virus software in use today is fairly effective - but only if it's kept updated and the user takes precautions (such as not opening unfamiliar documents or programs.) Despite all this, anti-virus software cannot protect against brand new viruses, and few users take the necessary precautions.

A survey was done of corporate computer users, finding that many users still get infected even if they are required to take all the necessary precautions. (Source: ICSA Labs Computer Virus Prevalence Survey 2000.) With the Internet daily growing larger, it is unlikely that anti-virus software will be able to protect all of the users connected; however, with proper care and attention, people should be able to deal with all but the most unusual viruses.

THANK YOU !