



HOW ANTIVIRUS WORKS?

**Lecture 9
2021-2022
CS- CCMS- TU**

Dr. Mocheb Lazam Shuwandy

ANTIVIRUS

- Antivirus software typically uses two different techniques to accomplish his mission:
 - Examining (scanning) files to look for known viruses matching definitions in a virus dictionary
 - Identifying suspicious behavior from any computer program which might indicate infection. Such analysis may include data captures, port monitoring and other methods.

ANTIVIRUS MODES

- Anti-virus programs have two basic modes:
 - “static” file scanning: useful for when you have to scan a file or a volume to check to see if any of the files are currently infected with malware
 - real-time “dynamic” scanning: is really what is needed to prevent the computer from getting infected in the first place. In this mode, all files that the operating system opens or uses are scanned first before they are fully opened.

APPROACHES

- **Dictionary**

- A signature is a characteristic byte-pattern that is part of a certain virus or family of viruses
- In the virus dictionary approach, when the antivirus software examines a file, it refers to a dictionary of known viruses that the authors of the antivirus software have identified. If a piece of code in the file matches any virus identified in the dictionary, then the antivirus software can take one of the following actions:
 1. attempt to repair the file by removing the virus itself from the file
 2. quarantine the file (such that the file remains inaccessible to other programs and its virus can no longer spread)
 3. delete the infected file

APPROACHES

- **Dictionary**

- the virus dictionary approach requires periodic (generally online) downloads of updated virus dictionary entries.
- users identify new viruses "in the wild", they can send their infected files to the authors of antivirus software, who then include information about the new viruses in their dictionaries.
- Dictionary-based antivirus software typically examines files when the computer's operating system creates, opens, closes or e-mails them. In this way it can detect a known virus immediately upon receipt

APPROACHES

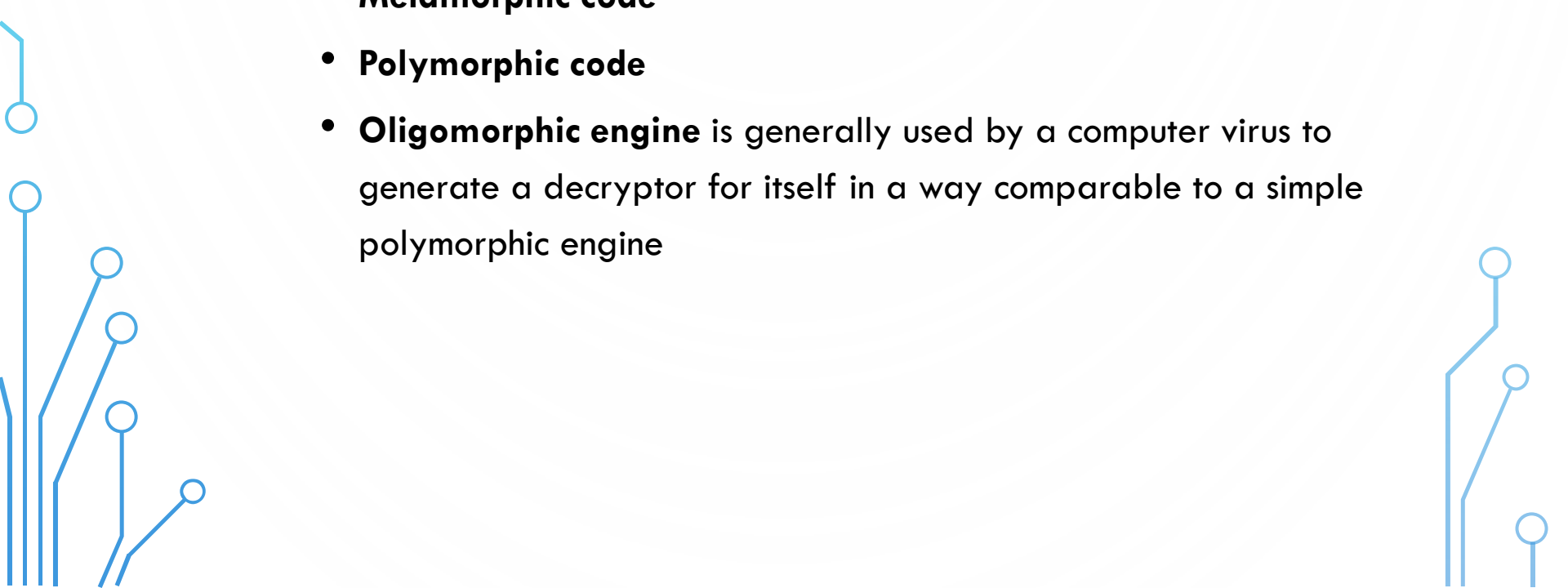
- **Dictionary**

- System Administrator can typically schedule the antivirus software to examine (scan) all files on the user's hard disk on a regular basis.
- Although the dictionary approach can effectively contain virus outbreaks in the right circumstances.



APPROACHES

- **Dictionary**

- Virus's Technology to avoid the Dictionary Approach is:
 - **Metamorphic code**
 - **Polymorphic code**
 - **Oligomorphic engine** is generally used by a computer virus to generate a decryptor for itself in a way comparable to a simple polymorphic engine
- 

APPROACHES

- **Dictionary**

- Previous technology weakness are:

- Polymorphism:

- A small portion of it is left unencrypted and used to jumpstart the encrypted software. Anti-virus software targets this small unencrypted portion of code.
 - Anti-virus software can detect it by decrypting the viruses using an emulator, or by statistical pattern analysis of the encrypted virus body.

- most oligomorphic viruses aren't able to generate more than a few hundred different decryptors, so detecting them with simple signatures is still possible



APPROACHES

- Suspicious behavior:
 - The suspicious behavior approach doesn't attempt to identify known viruses, but instead monitors the behavior of all programs.
 - If one program tries to write data to an executable program, for example, the antivirus software can flag this suspicious behavior, alert a user and ask what to do.

APPROACHES

- Suspicious behavior
 - the suspicious behavior approach provides protection against brand-new viruses that do not yet exist in any virus dictionaries.
 - However, it can also sound a large number of false positives, and users probably become desensitized to all the warnings.
 - If the user clicks "Accept" on every such warning, then the antivirus software obviously gives no benefit to that user

APPROACHES

- Suspicious behavior weakness
 - The fact that many legal S/W behave like malicious S/W make the job of antivirus harder
 - Ex: There are commercial software that have many features as dynamic code encryption/decryption, code replace, metamorphic engine, API export, anti debug/dump/trace and more. They are used to protect software programs from illegal use (cracking and reverse engineering)



APPROACHES

- **Heuristic analysis:**

- try to emulate the beginning of the code of each new executable that the system invokes before transferring control to that executable.
- If the program seems to use self-modifying code or otherwise appears as a virus (if it immediately tries to find other executables, for example), one could assume that a virus has infected the executable.
- Heuristic scanners have a higher rate of false positives than do signature scanners but they have the significant advantage of being able to detect unknown viruses.

APPROACHES

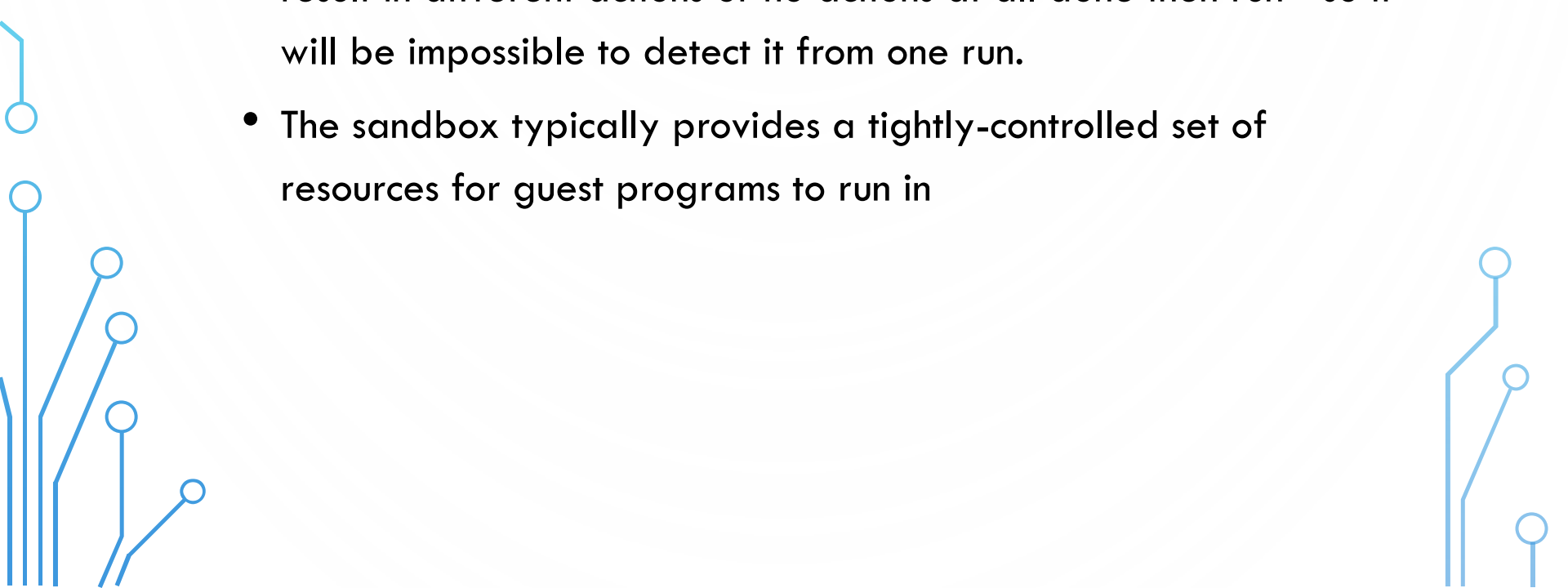
- **Sandbox:**

- **sandbox** is a security mechanism for safely running programs. It is often used to execute untested code, or programs from unverified third-parties, suppliers and untrusted users.
- emulates the operating system and runs the executable in this simulation. After the program has terminated, software analyzes the sandbox for any changes which might indicate a virus.
- Because of performance issues, this type of detection normally only takes place during on-demand scans



APPROACHES

- **Sandbox:**

- Also this method may fail as virus can be nondeterministic and result in different actions or no actions at all done then run - so it will be impossible to detect it from one run.
 - The sandbox typically provides a tightly-controlled set of resources for guest programs to run in
- 

WEAKNESSES OF ANTIVIRUS S/W

- Many security professionals agree that the current approach to defend against malicious software with antivirus is not good enough, but it is best solution that we have right now.
- The main shortcomings in the antivirus software:

WEAKNESSES OF ANTIVIRUS S/W

1. Reactive approach: Your antivirus as good as your definition files. If you did not update them, the antivirus program will not be able to detect a new malware. The most critical problems for the antivirus software to detect malicious code are:
 - new or modified malicious code
 - rootkit programs
 - Software Misuse
2. Inability to protect themselves: With sufficient system permissions, malware can change antivirus settings and configuration.

WEAKNESSES OF ANTIVIRUS S/W

3. Inability to revert the results of malware infection process.

- Too often, “installation process” of malware includes copying files, changing registry and system configuration files, changing other software configuration. Some of these changes still present in the infected system, even after an antivirus program delete or disinfect malware files.
- Almost for every severe virus/worm, antivirus vendors issues “Removal Tool”.
- this is means that the antivirus vendors saying to their customers: “our antivirus isn’t good enough to clean your system – please use this tool”

RETRO VIRUSES

- retro viruses are the viruses that attack security programs
- “Attack is the best defense strategy”
- The malware instead of hiding from detection by security S/W it target these S/W as its (part of) malicious action

THE BLACK ANTIVIRUS

- a(white) antivirus used for the good purposes while Black Antivirus is the same antivirus, but used for the “bad” purposes.
- An unexpected problem:
 - “virus definition database” has the definitions for security tools used today in the computer security world to defend and protect computer systems.
 - Malware could includes antivirus engine and signature definition files for security tools.
- To protect our tools, need to evade the Antivirus detection! Therefore, security tools need to be a polymorphic or even metamorphic.

THE BLACK INTRUSION DETECTION SYSTEM:

- Malware can use IDS system to “shut down” security systems at the network level.
- Such malware will primary target internal corporate LAN and could carry itself an IDS engine or change the existing one with new rules (if possible).
- malware carry engine itselfand use MAC and ARP poisoning to sniff in a switched network.
- Any communication that passes the wire were the malware was able to “see” it, is a subject for this attack.
- The solution for this problem may be the use of **covert channels**

VIRUS EXAMPLE

- **Win32/Simile:**

- is a metamorphic computer virus written in assembly language for Microsoft Windows (most recent version in early March 2002)
- It was written by the virus writer Mental Driller
- When the virus is first executed, it checks the current date. If the host file (the file that is infected with the virus) imports the file User32.dll, then on the 17th of March, June, September, or December, a message is displayed.
- Depending on the version of the virus the case of each letter in the text is altered randomly. On May 14, a message saying "Free Palestine!" will be displayed if the system locale is set to Hebrew.

VIRUS EXAMPLE

- The virus then rebuilds itself. This metamorphic process is very complex and accounts for around 90% of the virus' code
- After the rebuild, the virus searches for executable files in folders on all fixed and remote drives.
- The virus contains checks to avoid infecting "goat" or "bait" files
- The infection process uses the structure of the host, as well as random factors, to control the placement of the virus body and the decryptor.
- The virus contains no destructive payload

SQL SLAMMER WORM

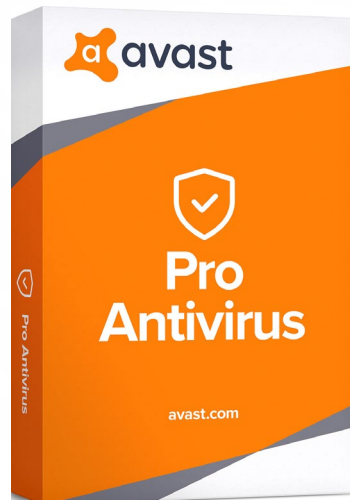
- The **SQL slammer worm** is a computer worm that caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic
- It spread rapidly, infecting most of its 75,000 victims within ten minutes.
- it exploited two buffer overflow bugs in Microsoft's flagship SQL Server and Desktop Engine database products
- The worm is a small (376 bytes) piece of code that does little other than generate random IP addresses and send itself out to those addresses.

SQL SLAMMER WORM

- If a selected address happens to belong to a host that is running an unpatched copy of Microsoft SQL Server Resolution MSDE Service, the host immediately becomes infected and begins spraying the Internet with more copies of the worm program.
- The worm is so small that it does not contain code to write itself to disk, so it only stays in memory, and it is easy to remove.

ANTIVIRUS EXAMPLE

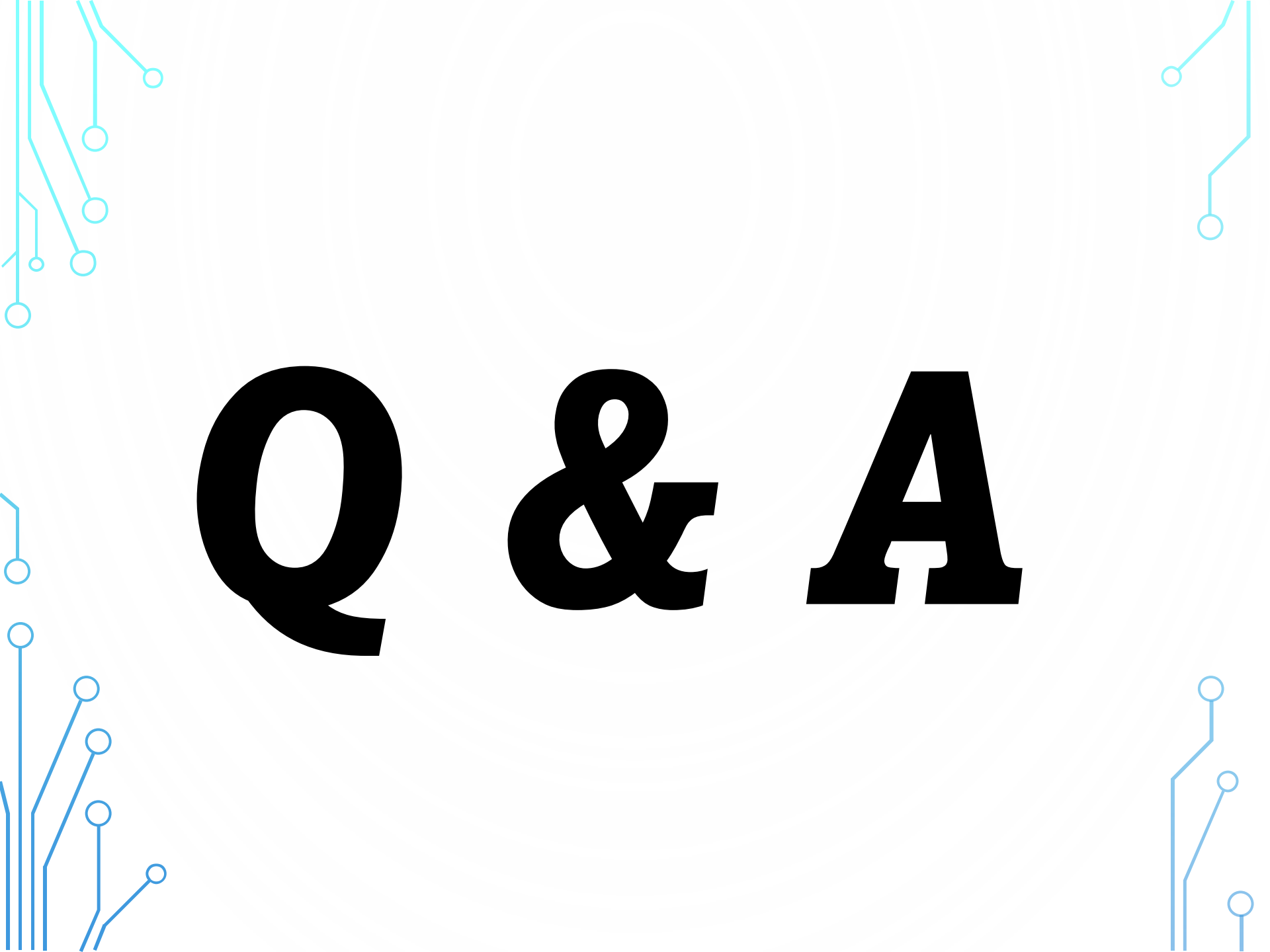
- one of the most popular full-featured freeware anti-virus applications for Microsoft Windows users.
- Official website: <http://www.avast.com/>



ANTIVIRUS EXAMPLE

- Features :

- Standard Shield — Real-time protection
- IM shield — Instant Messenger protection
- P2P shield — P2P protection
- Internet Mail — E-mail protection
- Outlook/Exchange — Microsoft Outlook/Exchange protection
- Web Shield — HTTP protection (local transparent proxy)
- Script blocker — script checker
- Network Shield — basic protection against well-known network worms. Acts as a lightweight Intrusion Detection System
- Audible alarms — vocal warnings such as "Caution, a virus has been detected!"
- boot-time scan — through the program interface, a user can schedule a boot-time scan to remove viruses that load during Windows startup and therefore difficult to remove.

The image features a white background with decorative light blue circuit-like lines in the corners. These lines consist of vertical and horizontal segments connected by small circles, resembling a stylized PCB or network diagram. The central focus is the text 'Q & A' in a large, bold, black serif font. The 'Q' has a thick, rounded body and a curved tail. The ampersand is a classic, ornate design. The 'A' is a tall, blocky letter with a wide base and a pointed top.

Q & A