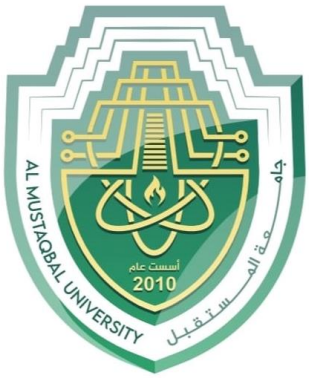

جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

قسم الامن السيبراني

Department of Cyber Security

Subject:

Malicious codes

Class:

THIRD

Lecturer:

Dr. Suha Alhussieny

Lecture: (4)

Viruses Classification , Virus Kits , Macro Viruses

Viruses Classification

There has been a continuous arms race between virus writers and writers of antivirus software since viruses first appeared. As effective countermeasures are developed for existing types of viruses.

Viruses are classified into **two orthogonal** axes:

1. the type of Target the virus tries to infect .

2. by Concealment strategy which is a method the virus uses to conceal itself from detection by users and antivirus software.

1- A virus classification by **Target** includes the following categories:

1. **Boot sector infector**: Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.

2. **File infector**: Infects files that the operating system or shell consider to be executable.

3. **Macro virus**: Infects files with macro code that is interpreted by an application.

2- A virus classification by **Concealment strategy** includes the following categories:

1. **No Concealment**: Not hiding at all is one concealment strategy which is remarkably easy to implement in a computer virus. It goes without saying, however,

that it's not very effective - once the presence of a virus is known, it's trivial to detect and analyze.

2. **Encryption**: A typical approach is as follows. A portion of the virus creates a rando encryption key and encrypts the remainder of the virus. The key is stored with the virus. When an infected program is invoked, the virus uses the stored random key to decrypt the virus. When the virus replicates, a different random key is selected. Because the bulk of the virus is encrypted with a different key for each instance, there is no constant bit pattern to observe.

3. **Stealth virus**: A form of virus explicitly designed to hide itself from detection by antivirus software. Thus, the entire virus, not just a payload is hidden. One example of a stealth virus was discussed earlier: a virus that uses compression so that the infected program is exactly the same length as an uninfected version. Far more sophisticated techniques are possible. For example, a virus can place intercept logic in disk I/O routines, so that when there is an attempt to read suspected portions of the disk using these routines, the virus will present back the original, uninfected program.Thus, *stealth* is not a term that applies to a virus as such but, rather, refers to a technique used by a virus to evade detection.

4. **Oligomorphism:** Assuming an encrypted virus' key is randomly changed with each new infection, the only unchanging part of the virus is the code in the decryptor loop. Anti-virus software will exploit this fact for detection, so the next logical development is to change the decryptor loop's code with each infection.

An *oligomorphic* virus, or *semi-polymorphic* virus, is an encrypted virus which has a small, finite number of different decryptor loops at its disposal. The virus selects a

new decryptor loop from this pool for each new infection. For example, Whale had 30 different decryptor variants, and Memorial had 96 decryptors. In terms of detection, oligomorphism only makes a virus marginally harder to spot. Instead of looking for one decryptor loop for the virus, anti-virus software can simply have all of the virus' possible decryptor loops enumerated, and look for them all.

5. **Polymorphic virus**: A virus that mutates with every infection, making detection by the "signature" of the virus impossible and harder. A polymorphic virus creates copies during replication that are functionally

equivalent but have distinctly different bit patterns. As with a stealth virus, the purpose is to defeat programs that scan for viruses. In this case, the "signature" of the virus will vary with each copy. To achieve this variation, the virus may randomly insert superfluous instructions or interchange the order of independent instructions. A more effective approach is to use encryption.The strategy of the encryption virus is followed. The portion of the virus that is responsible for generating keys and performing encryption/decryption is referred to as the *mutation engine*. The mutation engine itself is altered with each use.

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

7. **Strong Encryption**: The encryption methods discussed so far result in viruses that, once captured, are susceptible to analysis. The major problem is not the

encryption method, because that can always be strengthened; the major problem is that viruses carry their decryption keys with them.

This might seem a necessary weakness, because if a virus doesn't have its key, it can't decrypt and run its code. There are, however, **two other possibilities**.

1. The key comes from outside an infected system:

• A virus can retrieve the key from a web site, but that would mean that the virus would then have to carry the web site's address with it, which could be blocked as a countermeasure. To avoid knowing a specific web site's name, a virus could use a web search engine to get the key instead.

• A binary virus is one where the virus is in two parts, and doesn't become virulent until both pieces are present on a system. There have only been a few binary viruses, such as Dichotomy and RMNS.

One manifestation of binary viruses would be where virus V1 has strongly encrypted code, and virus V2 has its key. But this scheme is unlikely to work well in practice. If V1 and V2 travel together, then both will bear the same risk of capture and analysis, defeating the purpose of separating the encryption key. If V1 and V2 spread separately (e.g., V2 is released a month after V1, and uses a different infection vector) then their spread would be independent.

2. The key comes from inside an infected system. Using environmental key generation, the decryption key is constructed of elements already present in the target's environment, like:

➢the machine's domain name

➢the time or date

➢some data in the system (e.g., file contents)

➢the current user name

➢the interface's language setting (e.g., Chinese, Hebrew).

This makes it very easy to target viruses to particular individuals or groups. A target doesn't even know that they possess the key.

Combined with strong encryption, environmental key generation would render a virus unanalyzable even if captured. To fully analyze an encrypted virus, it has to be decrypted, and while the elements comprising the key may be discovered, the exact value of the key will not. In this case, the only real hope of decryption lies in a poor choice of key. A poorly-chosen key with a relatively small range of possible values (e.g., the language setting) would be susceptible to a brute-force attack. method is to catch exceptions that invalid code may cause, then try to run the decrypted "code" and see if it works.

Virus Kits

Another weapon in the virus writers' armory is the virus-creation toolkit. Such a toolkit enables a relative novice to quickly create a number of different viruses. Although viruses created with toolkits tend to be less sophisticated than viruses

designed from scratch, the sheer number of new viruses that can be generated using a toolkit creates a problem for antivirus schemes.

Macro Viruses

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

Macro viruses are particularly threatening for **a number of reasons**:

1. A macro virus is platform independent. Many macro viruses infect Microsoft Word documents or other Microsoft Office documents. Any hardware platform and operating system that supports these applications can be infected.

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

3. Macro viruses are easily spread.A very common method is by electronic mail.

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

Macro viruses take advantage of a feature found in Word and other office applications such as Microsoft Excel, namely the macro. In essence, a macro is an executable program embedded in a word processing document or other type of file. Typically, users employ macros to automate repetitive tasks and thereby save keystrokes. The macro language is usually some form of the Basic programming language.A user might define a sequence of keystrokes in a macro and set it up so

that the macro is invoked when a function key or special short combination of keys is input.

Successive releases of MS Office products provide increased protection against macro viruses. For example, Microsoft offers an optional Macro Virus Protection tool that detects suspicious Word files and alerts the customer to the potential risk of opening a file with macros.Various antivirus product vendors have also developed tools to detect and correct macro viruses. As in other types o viruses, the arms race continues in the field of macro viruses, but they no longer are the predominant virus threat.

H.W/

1. Which of the following infects a master boot record or boot record?
2. A virus that infects executable files is known as:
3. Which virus infects files that contain macro code?
4. What is a concealment strategy used by a virus?
5. Which virus type does NOT hide itself?
6. A virus that encrypts itself using a random key for each infection is a:
7. Which virus modifies disk I/O routines to hide its presence?
8. Oligomorphic viruses differ from polymorphic ones because they:
9. A polymorphic virus avoids detection by:
10. Which virus rewrites its own code completely with every infection?
11. The mutation engine in a virus is responsible for:
12. In strong encryption viruses, where can the decryption key come from?
13. Environmental key generation uses elements such as:
14. Binary viruses consist of:
15. A virus-creation toolkit allows:
16. Viruses created using toolkits are usually:
17. Macro viruses are dangerous because they are:
18. Macro viruses spread mostly through:
19. Macro viruses infect:
20. Modern MS Office provides protection against: