

زبان تخصصی مهندسی کامپیوتر

درس سوم:

Fighting with Digital Virus

Part I- Writing Development: Supporting topic sentence

- در درس قبل، به دو روش از روشهای توسعه جمله اول پاراگراف اشاره شده است.
- در این درس، دو روش دیگر بنامهای Facts و Statistics برای توسعه جمله اول پاراگراف معرفی میشود.
-

- **Facts** ذکر حقایقی در مورد موضوع مورد بحث

Something, which is objectively proven, is called fact.

For example, industrial universities train engineers for a country.

- **Statistics** ارائه آمار در مورد برخی از جنبه های موضوع مورد بحث

Statistics are numerical facts showing some important information about a stated subject.

For example, One thousand international students are graduated from Iran each year.

Part II-Vocabulary

Erroneous (adj)

اشتباه، غلط

- Wrong; incorrect: *employers sometimes make erroneous assumptions.*

Malicious (adj)

بدخواه، بدجنس

- Characterized by malice; intending or intended to do harm: *Virus is a malicious software.*

Surreptitious (adj)

پنهانی، مخفی، مخفیانه

- Kept secret; they carried on a surreptitious affair.

Potential (adj)

بالقوه، امکان

- Having or showing the capacity to become or develop into something in the future: The potential uses of nuclear energy

Vulnerable (adj)

آسیب پذیر

- Susceptible to physical or emotional attack or harm: *we were in a vulnerable position.*

Legitimate (adj)

مشروع ، قانونی

- Conforming to the law or to rules: *his claims to legitimate authority.*

Replication (n)

کپی

- The action of copying or reproducing something: *A twentieth-century building would be cheaper than a replication of what was there before.*

Encipher (v)

کد کردن، رمزی کردن

- convert (a message or piece of text) into a coded form; encrypt.

Part III– Reading

DIGITAL VIRUS

Section 1: Pre-reading Questions

- What is a digital virus?
- Have you ever had a digital virus in your computer? What strategies did you use to clean your computer?
- What needs to be done in order not to face digital viruses in the computer?

Section 2: Reading Passage

- A digital virus is a computer program that can replicate itself and disseminate from one computer to another. The term "virus" is also commonly, but erroneously, employed to refer to other types of malware, including but not confined to adware and spyware programs that do not have a reproductive ability. Malwares such as Trojan horses and worms are sometimes confused with viruses, which are technically different. A worm can utilize security vulnerabilities to spread itself automatically to other computers through networks, while a Trojan horse is a program that shows harmless but performs malicious functions. Worms and Trojan horses, like viruses, may harm a computer system's data or performance. Some viruses and other malwares have symptoms noticeable to the computer user, but many are surreptitious or simply do nothing to call attention to themselves. Some viruses do nothing apart from reproducing themselves.



منتشر کردن، پراکندن - بدافزار - محدود شدن - ادوات تبلیغاتی - ادوات جاسوسی - تولید مثل - نشان، اثر

1. The vulnerability of operating systems to viruses

Just as a genetic **variety** in a population decreases the chance of a single disease **destroys** a population, the variety of software systems on a network similarly confines the destructive **potential** of viruses and malware. This became a particular **concern** in the 1990s, when Microsoft gained market **dominance** in desktop operating systems, web browsers, and Office **suites**. Writers of viruses and malware, due to Microsoft's desktop dominance, target Microsoft software. Although Windows is **by far** the most popular target operating system for virus writers, viruses also exist on other platforms. Any operating system that allows **third-party** programs to run can theoretically be infected by viruses.

تنوع - ویران کردن - نگرانی - تسلط، غلبه - ملتزمین، همراهان - به مراتب، بسیار - شخص ثالث

2. Types of Digital Virus

In order to replicate itself, a virus must be **permitted** to execute code and write to the memory. For this reason, many viruses **attach** themselves to executable files that may be part of **legitimate** programs. If a user attempts to **launch** an infected program, the virus code may be executed simultaneously. Viruses can be divided into two types based on their behavior when they are executed. **Nonresident** viruses immediately search for other **infectable** hosts, infect those targets, and finally transfer control to the application program they infected. Resident viruses do not search for hosts when they are launched. Instead, a resident virus loads itself into memory on execution and transfers control to the host program. The virus stays active on the background and infects new hosts when other programs or the operating system itself accesses those files.

اجازه دادن - چسباندن - بارگذاری کردن - غیر مقیم - قابل آلوده شدن

2. 1. Nonresident viruses

Nonresident viruses can be thought of as consisting of a *finder module* and a *replication module*. The finder module is responsible for finding new files to infect. For each new executable file the finder module **encounters**, it calls the replication module to infect that file.

2. 2. Resident viruses

Resident viruses contain a replication module that is similar to the one employed by nonresident viruses. A finder module, however, does not call this module. The virus loads the replication module into memory when it is executed and **ensures** that this module is executed each time the operating system is called to perform a certain operation. The replication module can be called; for example, each time the operating system executes a file. In this case, the virus infects every suitable program that is executed on the computer.

3. Tricks of Digital Viruses

3.1. Stealth Strategies

Some viruses employ different kinds of **deception** to avoid user detection. Some old viruses, especially on the MS-DOS platform, keep unchanged the "*last modified*" date of a host file when the virus infects the file. This approach does not deceive antivirus software, especially those, which maintain cyclic redundancy checks on file changes. Some viruses can infect files without increasing their sizes or damaging the files. They **fulfill** this by overwriting unused areas of executable files. These are called **cavity viruses**. For example, the CIH virus, or Chernobyl Virus, infects Portable Executable files. Because those files have many empty gaps, the small length virus does not add to the size of the file. Some viruses try to avoid detection by destroying the tasks associated with antivirus software before it can detect them.

As computers and operating systems improve, old hiding techniques need to be updated or replaced. **Protecting** a computer against viruses may require **migrating** a file system towards detailed and **explicit** permission for every kind of file access.

حقه، اغفال - انجام دادن - حفره - محافظت کردن - مهاجرت کردن - صریح، آشکار

3. 2. Read request intercepts

While some antivirus software employ various techniques to counter **stealth** mechanisms, the infection occurs and any **recourse** to clean the system is unreliable. In Microsoft Windows operating systems, the NTFS file system is **proprietary**. Direct access to files without using the Windows OS is **undocumented**. This leaves antivirus software little **alternative** but sends a read request to Windows OS files that handle such requests. Some viruses trick antivirus software by **intercepting** its requests to the OS. A virus can hide itself by intercepting the request to read the infected file, handling the request itself, and returning an uninfected version of the file to the antivirus software. The interception can occur through code injection of the actual operating system files that would handle the read request. Thus, an antivirus software attempting to detect the virus will either not be given permission to read the infected file, or the read request will be served with the uninfected version of the same file.

The only reliable method to avoid stealth is to boot from a medium that is known to be clean. Security software can then be used to check the **dormant** operating system files. Most security software relies on virus signatures, or they employ heuristics.

Security software may also use a database of file **hashes** for Windows OS files, so the security software can identify altered files, and request Windows installation media to replace them with authentic versions. In older versions of Windows, file hashes of Windows OS files stored in Windows—to allow file **integrity**/authenticity to be checked—could be overwritten so that the System File Checker would report that altered system files are authentic, so using file hashes to scan for altered files would not always guarantee finding an infection.

نهانکاری - توسل - انحصاری بودن - غیر معتبر - چاره، جایگزین - میان گرفتن - غیرفعال - درهم و برهم - درستی، صداقت

3.3. Self-modification

Most modern antivirus programs try to find virus-patterns inside ordinary programs by scanning them for **so-called** virus signatures. Unfortunately, the term is **misleading**, in that viruses do not **possess** unique signatures in the way that human beings do. Such a virus signature is merely a sequence of bytes that an antivirus program looks for because it is known to be part of the virus. A better term would be "search strings". Different antivirus programs will employ different search strings, and indeed different search methods, when identifying viruses. If a virus scanner finds such a pattern in a file, it will double check to make sure that it has found the virus. This is because it may merely be a **coincidental** sequence in an **innocent** file. Then the user can delete, or (in some cases) "clean" or "heal" the infected file. Some viruses employ techniques that make detection difficult by means of signatures but probably not impossible. These viruses modify their code on each infection. That is, each infected file contains a different variant of the virus.

به اصطلاح - غلط انداز - دارا (مالک) بودن - اتفاقی - پاک، بیگناه

3.4. Encryption with a variable key

A more advanced method is the use of simple **encryption** to **encipher** the virus. In this case, the virus consists of a small **decrypting** module and an encrypted copy of the virus code. If the virus is encrypted with a different key for each infected file, the only part of the virus that remains constant is the decrypting module, which would (for example) be **appended** to the end. In this case, a virus scanner cannot directly detect the virus using signatures, but it can still detect the decrypting module, which still makes indirect detection of the virus possible. Since these signatures would be **symmetric** keys, stored on the infected host, they can decrypt the final virus, but are probably not required. This is because the self-modifying code rarely flags the file as suspicious.

An old, but **compact**, encryption involves XORing each byte in a virus with a constant, so that the exclusive-OR operation had to be only repeated for decryption. It is suspicious for a code to modify itself, so the code to do the encryption/decryption may be part of the signature in many virus definitions.

کدگذاری - کد گشا - اضافه (ضمیمه) کردن - متقارن - فشرده

4. Antivirus software

Many users install antivirus software that can detect and **eliminate** known viruses when the computer attempts to download or run the executable files (which may be distributed as an email attachment, or on USB flash drives, for examples). Some antivirus software **block** known malicious web sites that attempt to install malware. Antivirus software does not change the **underlying** capability of hosts to transmit viruses. Users must update their software **regularly** to **patch** security vulnerabilities (holes). Antivirus software also needs to be regularly updated in order to recognize the latest **threats**.

حذف کردن - مسدود کردن - پایه، اصلی - به طور منظم - وصله کردن - تهدید

4.1. How Antivirus software works

There are two common methods that an antivirus software application uses to detect viruses. The first most common method of virus detection uses a list of virus signature definitions. This works by examining the content of the computer memory (its RAM, and boot sectors) and the files stored on fixed or removable drives (hard drives, floppy drives, or USB flash drives), and comparing those files against a database of known virus "signatures". As mentioned before, Virus signatures are just strings of code that are used to identify individual viruses; for each virus, the anti-virus designer tries to choose a unique signature string that will not be found in a **legitimate** program. Different anti-virus programs use different "signatures" to identify viruses. The disadvantage of this detection method is that users are only protected from viruses that are detected by signatures in their most recent virus definition update, and not protected from new viruses. A second method to find viruses is to use a **heuristic** algorithm based on common virus behaviors. This method has the ability to detect new viruses for which anti-virus security **firms** have yet to define a "signature", but it also **gives rise** to more false positives than using signatures. False positives can be **disruptive**, especially in a commercial environment.

مکاشفه ای - شرکت، موسسه - موجب شدن - مزاحم

Part IV- Reading comprehension

Mark each statement as T (True), F (False), or NG (Not Given) to the information in the reading comprehension passage.

1. Virus refers to malware, adware and spyware programs having a productive ability.
2. Like desktop computers, laptops can be vulnerable to get viruses but have no symptoms.
3. Microsoft company has been famous and found its markets for many years.
4. There are different kinds of viruses depending on their behavior.
5. A finding and replication module is part of resident viruses.
6. Some viruses use different kind of tricks to run away from detection.
7. Computers cannot defend themselves against various viruses.
8. There is no security software to keep a computer as safe as possible.