**Некоммерческое акционерное общество**

**АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ**

Кафедра
Иностранные
языки

# ПРОФЕССИОНАЛЬНО-ОРИЕНТИРОВАННЫЙ

# АНГЛИЙСКИЙ ЯЗЫК

Методические указания по чтению и переводу текстов
для студентов специальности 5В100200 - Системы информационной безопасности

Алматы, 2014

СОСТАВИТЕЛЬ: Л.Д. Сергеева. Профессионально-ориентированный Английский язык. Методические указания для студентов специальности 5В100200 - Системы информационной безопасности. – Алматы: АУЭС, 2013. – 48 с.

Данные методические указания предназначены для студентов специальности 5В100200 – Системы информационной безопасности. Изучение профессионально-ориентированного английского языка (LSP) формирует профессиональную компетенцию будущих специалистов.

Рецензент: канд.филолог.наук, доцент АУЭС Козлов В.С.

Печатается по плану издания некоммерческого акционерного общества «Алматинский университет энергетики и связи» на 2013 г.

**Unit 1**
**Malware**
**Text 1**

## Internet Security
## Malware: viruses, worms, Trojans and spyware

malware ['mælweə] – вредоносные программы

to alter ['ɒltə]– изменять

to attach [ə'tætʃ] – прикрепляться

to exploit security flaws [flɔː] – использовать недостатки программы

self-contained [ˌselfkən'teind ]- автономный

disguised [dis'gaizd]– замаскированный

legitimate [lə'dʒitimət] software – легальное программное обеспечение

ominous ['ɒminəs] – зловещий

undocumented means - секретное средство

troubleshoot ['trʌbˌlʃuːt] - устранение неполадок

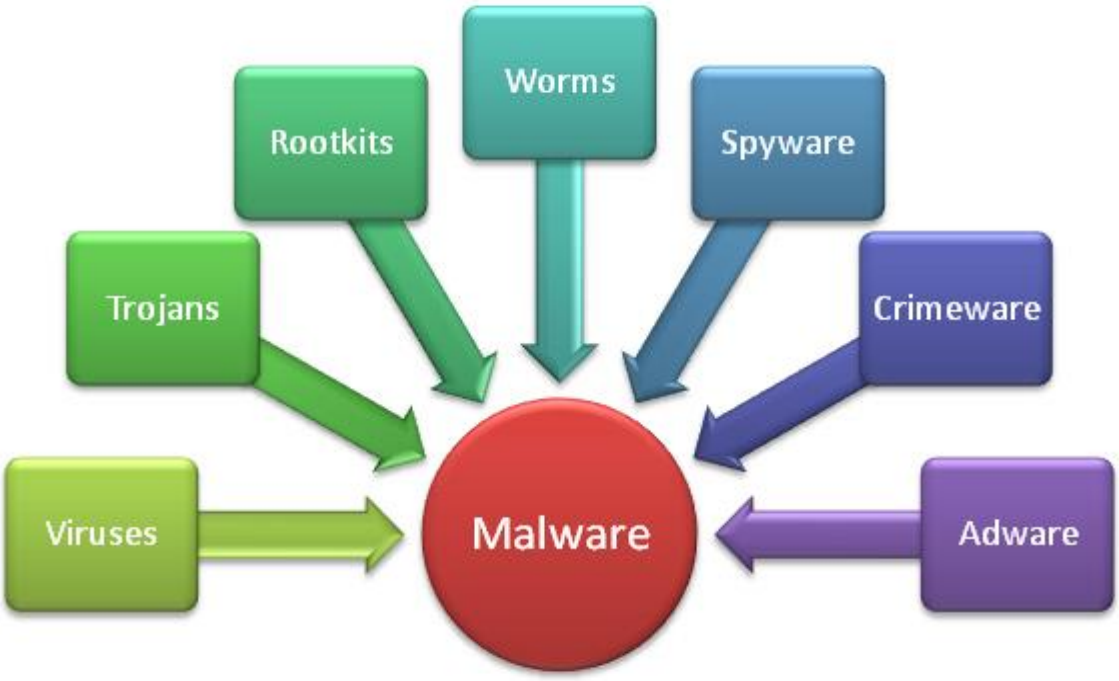
to boot up [buːt] – загружаться

targeted computer ['tɑː.git] – компьютер жертвы

payload ['peiləud] – полезная нагрузка

(un)authorized access to information – (не)санкционированный доступ к информации

access mediation rules - правила разграничения доступа



*Malware* **(**malicious [məˈlɪʃəs] software) is software created to damage or alter the computer data or operations. There are the main types:

*Viruses* are programs that spread by attaching themselves to executable files or documents. When the infected program is run, the virus propagates to other files or programs on the computer. Some viruses are designed to work at a particular time or on a specific date, e.g. on Friday 13th. An email virus spread by sending a copy of itself to everyone in an email address book.

*Worms* are self-copying program that have the capacity to move from one computer to another without human help, by exploiting security flaws in computer networks. Worms are self-contained and don't need to be attached to a documents or program the way viruses do.

*Trojan horses* are malicious program disguised as innocent-looking files or embedded within legitimate software. Once they are activated, they may affect the computer in a variety of ways: some are just annoying; others are more ominous, creating a *backdoor* to the computer which can be used to collect stored data. They don't copy themselves or reproduce by infecting other files. *A backdoor* is a secret or undocumented means of getting into a computer system. Many programs have backdoors placed by the programmer to allow them to gain access to troubleshoot or change the program. Some backdoors are placed by hackers once they gain access to allow themselves an easier way in next time or in case their original entrance is discovered.

*Spyware* is software designed to collect information from computers for commercial or criminal purposes, is another example of malicious software. It usually comes hidden in fake freeware or shareware applications downloadable from the Internet.

*Rootkit* is a type of software designed to hide the fact that an operating system has been compromised, sometimes by replacing vital executables. Rootkits allow viruses and malware to "hide in plain sight" by disguising as necessary files that your antivirus software will overlook. Rootkits themselves are not harmful; they are simply used to hide malware, bots and worms. Rootkits get their name from the Unix term for the primary administrator account called "root" and "kits," which refer to the software pieces that implement the tool. To install a rootkit, an attacker must first gain access to the root account by using an exploit or obtaining the password by cracking it or social engineering. Rootkits were originally used in the early 1990's and targeted UNIX operating systems. Today, rootkits are available for many other operating systems, including Windows. Because rootkits are activated before your operating system even boots up, they are very difficult to detect and therefore provide a powerful way for attackers to access and use the targeted computer without the owner's notice. Due to the way rootkits are used and installed, they are notoriously difficult to remove. Rootkits today usually are not used to gain elevated access, but instead are used to mask malware payloads more effectively.

*Adware* is a program that installs an additional component that feeds advertising, often by delivering pop-up ads or by installing a toolbar in your browser. Adware is considered a legitimate alternative offered to consumers who do not wish

to pay for software. There are many ad-supported programs, games or utilities that are distributed as adware (or freeware). Today we have a growing number of software developers who offer their goods as "sponsored" freeware (adware) until you pay to register. If you're using legitimate adware, when you stop running the software, the ads should disappear, and you always have the option of disabling the ads by purchasing a registration key.

*1 Find words or phrases in the article which are similar in meaning to these words and phrases:*

a) to change
b) to join a file such as a document, picture, or computer program, to an email
c) disadvantage
d) having an appearance that hides the true form
e) discovering why something does not work effectively and making suggestions about how to improve it

*2 Which malware:*

a) is embedded within legitimate software?
b) Is designed to collect information from computers for commercial or criminal purposes?
c) is self-copying program that have the capacity to move from one computer to another without human help?
d) installs an additional component that feeds advertising, often by delivering pop-up ads or by installing a toolbar in your browser?
e) spread by attaching themselves to executable files or documents?
f) is a type of software designed to hide the fact that an operating system has been compromised, sometimes by replacing vital executables?
g) are malicious program disguised as innocent-looking files or embedded within legitimate software?

*3 Decide if there statements TRUE or FALSE:*

a) Malware **(**malicious software) is software created to secure the computer data or operations.
b) Some worms are designed to work at a particular time or on a specific date, e.g. on Friday 13$^{th}$.
c) Viruses are self-contained and don’t need to be attached to a documents or program.
d) Once Rootkits are activated, they may affect the computer in a variety of ways: some are just annoying; others are more ominous, creating a *backdoor* to the computer which can be used to collect stored data.
e) Adware usually comes hidden in fake freeware or shareware applications downloadable from the Internet.
f) Worms today usually are not used to gain elevated access, but instead are used to mask malware payloads more effectively.

g) Spyware is considered a legitimate alternative offered to consumers who do not wish to pay for software.

*4 Translate collocations:*

malicious [mə'lɪʃəs] software; to damage or alter the computer data or operations; executable files or documents; self-copying program; by exploiting security flaws in computer networks; malicious program disguised as innocent-looking files; within legitimate software; others are more ominous; undocumented means; to gain access to troubleshoot or change the program; to hide malware, bots and worms; operating system even boots up; delivering pop-up ads; legitimate adware.

**Text 2**

**Computer viruses**

wipe out – уничтожать
tie up – мешать

replicate ['replɪkeɪt]– копировать

victim ['vɪktɪm] жертва

fuss [fʌs] – суматоха
consumer losses – потребительские потери
online threat [θret] – онлайн угроза

arguably ['a:gjuəbli] - пожалуй
how to throw a monkey wrench into the figurative gears – как вставлять палки в колеса, выражаясь в переносном смысле

prankster ['præŋkstər] – шутник
the name has stuck ever since - название осталось с тех пор
corrupted Web links – нарушить соединение с другими сайтами по ссылке

cripple ['krɪpl] – наносить вред

Computer viruses can be a nightmare. Some can wipe out the information on a hard drive, tie up traffic on a computer network for hours, turn an innocent machine into a zombie and replicate and send themselves to other computers. If you've never had a machine fall victim to a computer virus, you may wonder what the fuss is about. But the concern is understandable -- according to Consumer Reports, computer viruses helped contribute to $8.5 billion in consumer losses in. Computer viruses are just one kind of online threat, but they're arguably the best known of the bunch.

Computer viruses have been around for many years. In fact, in 1949, a scientist named John von Neumann theorized that a self-replicated program was possible. The computer industry wasn't even a decade old, and already someone had figured out how to throw a monkey wrench into the figurative gears. But it took a few decades before programmers known as *hackers* began to build computer viruses.

While some pranksters created virus-like programs for large computer systems, it was really the introduction of the personal computer that brought computer viruses to the public's attention. A doctoral student named Fred Cohen was the first to describe self-replicating programs designed to modify computers as viruses. The name has stuck ever since.

In the good old days (i.e., the early 1980s), viruses depended on humans to do the hard work of spreading the virus to other computers. A hacker would save the virus to disks and then distribute the disks to other people. It wasn't until modems became common that virus transmission became a real problem. Today when we think of a computer virus, we usually imagine something that transmits itself via the Internet. It might infect computers through e-mail messages or corrupted Web links. Programs like these can spread much faster than the earliest computer viruses.

*1 Find words or phrases in the article which are similar in meaning to these words and phrases:*

a) a computer program or part of a computer program that can make copies of itself and is intended to prevent the computer from working normally

b) to connect computers together so that they can share information

c) someone who hacks into other people's computer systems

d) propagation

e) a flat circular device, usually inside a square container, which has a magnetic covering and is used for storing computer information

*2 Answer the questions:*

1 Why are computer viruses so dangerous?

2 What did a scientist named John von Neumann theorize in 1949?

3 When did programmers known as *hackers* begin to build computer viruses?

4 Who was the first to describe self-replicating programs designed to modify computers as viruses?

5 How would a hacker distribute computer virus in the early 1980s?

6 Why did virus transmission become a real problem?

7 How does a computer virus transmit itself today?

We're going to take a look at 10 of the worst computer viruses to cripple a computer system. Let's start with the Melissa virus.

**1 Melissa**

to tempt [tempt] - искушать

recipient [rɪˈsɪpiənt] – получатель

to unleash [ʌnˈliːʃ] – выпустить

wreaked havoc – посеяла хаос

trial process – судебный процесс

lost his case – проиграл свое дело

jail sentence – тюремный срок

ultimately - в конечном счете

In the spring of 1999, a man named David L. Smith created a computer virus based on a Microsoft Word macro. He built the virus so that it could spread through e-mail messages. Smith named the virus "Melissa," saying that he named it after an exotic dancer from Florida.

Rather than shaking its moneymaker, the Melissa computer virus tempts recipients into opening a document with an e-mail message like "Here is that document you asked for, don't show it to anybody else." Once activated, the virus replicates itself and sends itself out to the top 50 people in the recipient's e-mail address book.

The virus spread rapidly after Smith unleashed it on the world. The United States federal government became very interested in Smith's work -- according to statements made by FBI officials to Congress, the Melissa virus "wreaked havoc on government and private sector networks". The increase in e-mail traffic forced some companies to discontinue e-mail programs until the virus was contained.

After a lengthy trial process, Smith lost his case and received a 20-month jail sentence. The court also fined Smith $5,000 and forbade him from accessing computer networks without court authorization. Ultimately, the Melissa virus didn't cripple the Internet, but it was one of the first computer viruses to get the public's attention.

*Answer the questions:*

1 Who created Melissa?

2 How could Melissa spread?

3 Why did the United States federal government become very interested in Smith's work?

4 What was Smith’s punishment?

5 Did the Melissa virus cripple the Internet?

**2 I love you**

a digital menace ['menis] - цифровая угроза

to emerge [ɪ'mɜːdʒ] – возникать

threat [θret] - угроза

a standalone program – отдельная программа

It bore the name – она носила имя

a secret admirer – тайный поклонник

in several folders – в нескольких папках

Internet Relay Chat - ретранслируемый чат в Интернете

to fix bugs - исправить ошибки

citing a lack of evidence - ссылаясь на отсутствие доказательств

dropped the charges - сняли обвинения

A year after the Melissa virus hit the Internet; a digital menace emerged from the Philippines. Unlike the Melissa virus, this threat came in the form of a worm - it was a standalone program capable of replicating itself. It bore the name I love you.

The I love you virus initially traveled the Internet by e-mail, just like the Melissa virus. The subject of the e-mail said that the message was a love letter from a secret admirer. An attachment in the e-mail was what caused all the trouble. The original worm had the file name of love-letter-for you.txt.vbs. The vbs extension pointed to the language the hacker used to create the worm: *Visual Basic Scripting*.

According to anti-virus software producer McAfee, the I love you virus had a wide range of attacks:

- It copied itself several times and hid the copies in several folders on the victim's hard drive.
- It added new files to the victim's registry keys.
- It replaced several different kinds of files with copies of itself.
- It sent itself through Internet Relay Chat clients as well as e-mail.
- It downloaded a file called win-bugsfix.exe from the Internet and executed it. Rather than fix bugs, this program was a password-stealing application that e-mailed secret information to the hacker's e-mail address.

Who created the I love you virus? Some think it was Onel de Guzman of the Philippines. Filipino authorities investigated de Guzman on charges of theft - at the time the Philippines had no computer espionage or sabotage laws. Citing a lack of evidence, the Filipino authorities dropped the charges against de Guzman, who would neither confirm nor deny his responsibility for the virus. According to some estimates, the I love you virus caused $10 billion in damages.

Now that the love fest is over, let's take a look at one of the most widespread viruses to hit the Web.

*Decide if there statements TRUE or FALSE:*

1) Melissa virus is the same as I love you.

2) The original virus had the file name of love-letter-for-you.txt.vbs

3) I love you virus copied itself several times and hid the copies in one folder on the victim's hard drive.

4) I love you virus added new files to the victim's password.

5) I love you virus replaced several different kinds of files with copies of other files.

6) It sent itself through Internet Relay Chat clients only.

7) win-bugsfix.exe program fixed bugs.

8) Onel de Guzman created the I love you virus.

9) I love you virus caused $100 billion in damages.

10) At present I love you virus spread over The Internet successfully.

*Translate without dictionary:*

**Gotcha!**

Gotcha! ['gɒtʃə]- Попался!
virus hoaxes - вирусные мистификации
replicate themselves – копировать сам себя

As if viruses, worms and Trojan horses weren't enough, we also have to worry about *virus hoaxes*. These are fake viruses - they don't actually cause any harm or replicate themselves. Instead, the creators of these viruses hope that people and media companies treat the hoax as if it were the real deal. Even though these hoaxes aren't immediately dangerous, they are still a problem. Like the boy who cried wolf, hoax viruses can cause people to ignore warnings about real threats.

**3 The Klez Virus**

setting the bar [ba:] high – установив высокую планку
plague [pleɪg] - досаждать
render – сделать
pose as a virus-removal tool- представляться как инструмент удаления вирусов
spoofing – подмена

The Klez virus marked a new direction for computer viruses, setting the bar high for those that would follow. It debuted in late 2001, and variations of the virus plagued the Internet for several months. The basic Klez worm infected a victim's computer through an e-mail message, replicated itself and then sent itself to people in the victim's address book. Some variations of the Klez virus carried other harmful programs that could render a victim's computer inoperable. Depending on the version, the Klez virus could act like a normal computer virus, a worm or a Trojan horse. It could even disable virus-scanning software and pose as a virus-removal tool.

Shortly after it appeared on the Internet, hackers modified the Klez virus in a way that made it far more effective. Like other viruses, it could come through a victim's address book and send itself to contacts. But it could also take another name from the contact list and place that address in the "From" field in the e-mail client. It's called spoofing - the e-mail appears to come from one source when it's really coming from somewhere else.

Spoofing an e-mail address accomplishes a couple of goals. For one thing, it doesn't do the recipient of the e-mail any good to block the person in the "From" field, since the e-mails are really coming from someone else. A Klez worm programmed to spam people with multiple e-mails could clog an inbox in short order, because the recipients would be unable to tell what the real source of the problem was. Also, the e-mail's recipient might recognize the name in the "From" field and therefore be more receptive to opening it.

*Answer the questions:*

1When did Klez first appear?
2 How did the basic Klez worm infect a victim's computer?
3 Which form could the Klez virus act in?
4 How did Klez virus operate after modifying by hackers?
5 What goals does spoofing an e-mail address accomplish?

*Translate without dictionary:*

## Antivirus Software

It's important to have an antivirus program on your computer, and to keep it up to date. But you shouldn't use more than one suite, as multiple antivirus programs can interfere with one another. Here's a list of some antivirus software suites:

- Avast Antivirus
- AVG Anti-Virus
- Kaspersky Anti-Virus
- McAfee VirusScan
- Norton AntiVirus

Several major computer viruses debuted in 2001. In the next section, we'll take a look at Code Red.

### 4 Code Red and Code Red II

pop up - неожиданно возникнуть

vulnerability [ˈvʌlnərəbl̩] - уязвимость

a buffer overflow problem - проблема переполнения буфера

buffers can handle - буферы могут обрабатывать

to overwrite adjacent [əˈdʒeɪsənt] memory - переписывать на прилегающую память

a distributed denial of service (DDoS) attack - распределенный отказ в обслуживании атаки

woe [wəʊ] – горе, несчастье

The Code Red and Code Red II worms popped up in the summer of 2001. Both worms exploited an operating system vulnerability that was found in machines running Windows 2000 and Windows NT. The vulnerability was a *buffer overflow problem*, which means when a machine running on these operating systems receives more information than its buffers can handle; it starts to overwrite adjacent memory.

The original Code Red worm initiated a distributed denial of service (DDoS) attack on the White House. That means all the computers infected with Code Red tried to contact the Web servers at the White House at the same time, overloading the machines.

A Windows 2000 machine infected by the Code Red II worm no longer obeys the owner. That's because the worm creates a *backdoor* into the computer's operating system, allowing a remote user to access and control the machine. In computing terms, this is a *system-level compromise*, and it's bad news for the computer's owner. The person behind the virus can access information from the victim's computer or even use the infected computer to commit crimes. That means the victim not only has to deal with an infected computer, but also may fall under suspicion for crimes he or she didn't commit.

While Windows NT machines were vulnerable to the Code Red worms, the viruses' effect on these machines wasn't as extreme. Web servers running Windows

NT might crash more often than normal, but that was about as bad as it got. Compared to the woes experienced by Windows 2000 users, that's not so bad.

Microsoft released software patches that addressed the security vulnerability in Windows 2000 and Windows NT. Once patched, the original worms could no longer infect a Windows 2000 machine; however, the patch didn't remove viruses from infected computers -- victims had to do those themselves.

*Decide if there statements TRUE or FALSE:*

1 The Code Red and Code Red II exploited an operating system vulnerability that was found in machines running Windows 2007 and Windows XP.

2 A *buffer overflow problem* means when a machine running on these operating systems receives information than its buffers can handle.

3 A distributed denial of service (DDoS) attack on the White House. That means all the computers infected with Code Red tried to block the Web servers at the White House.

4 The worm creates a *backdoor* into the computer's documents, allowing a remote user to access and download them.

5 While Windows NT machines were vulnerable to the Code Red worms, the viruses' effect on these machines was as extreme.

6 Software patches removed viruses from infected computers.

*Translate without dictionary:*

**What do I do now?**

What should you do if you find out your computer has been hit with a computer virus? That depends on the virus. Many antivirus programs are able to remove viruses from an infected system. But if the virus has damaged some of your files or data, you'll need to restore from backups. It's very important to back up your information often. And with viruses like the Code Red worms, it's a good idea to completely reformat the hard drive and start fresh. Some worms allow other malicious software to load onto your machine, and a simple antivirus sweep might not catch them all.

**5 Nimda**

crawl [krɔ:l] - ползать
propagating - распространяющийся
limited privileges - ограниченный доступ
fodder for the worm – корм для червя

Another virus to hit the Internet in 2001 was the Nimda (which is admin spelled backwards) worm. Nimda spread through the Internet rapidly, becoming the fastest propagating computer virus at that time. In fact, according to TruSecure CTO Peter Tippett, it only took 22 minutes from the moment Nimda hit the Internet to reach the top of the list of reported attacks.

The Nimda worm's primary targets were Internet servers. While it could infect a home PC, its real purpose was to bring Internet traffic to crawl. It could travel

through the Internet using multiple methods, including e-mail. This helped spread the virus across multiple servers in record time.

The Nimda worm created a backdoor into the victim's operating system. It allowed the person behind the attack to access the same level of functions as whatever account was logged into the machine currently. In other words, if a user with limited privileges activated the worm on a computer, the attacker would also have limited access to the computer's functions. On the other hand, if the victim was the administrator for the machine, the attacker would have full control.

The spread of the Nimda virus caused some network systems to crash as more of the system's resources became fodder for the worm. In effect, the Nimda worm became a distributed denial of service (DDoS) attack.

*Answer the questions:*

1Why was the virus called Nimda?

2 How much does it take from the moment Nimda hit the Internet to reach the top of the list of reported attacks?

3 What was the real purpose of Nimda?

4 How could Nimda travel through the Internet?

5 Why did Nimda worm create a backdoor into the victim's operating system?

6 What did the spread of the Nimda virus cause?

*Translate without dictionary:*

**Phoning it in**

Not all computer viruses focus on computers. Some target other electronic devices. Here's just a small sample of some highly portable viruses:

- CommWarrior attacked smart phones running the Symbian operating system (OS).
- The Skulls Virus also attacked Symbian phones and displayed screens of skulls instead of a home page on the victims' phones.
- RavMonE.exe is a virus that could infect iPod MP3 devices made between Sept. 12, 2006, and Oct. 18, 2006.
- Fox News reported in March 2008 that some electronic gadgets leave the factory with viruses pre-installed -- these viruses attack your computer when you sync the device with your machine.

Next, we'll take a look at a virus that affected major networks, including airline computers and bank ATMs.

**6 SQL Slammer/Sapphire**

sapphire ['sæfaɪər] - сапфир

outage ['aʊtɪdʒ] - перебой в работе

culprit ['kʌlprɪt] – виновник

In late January 2003, a new Web server virus spread across the Internet. Many computer networks were unprepared for the attack, and as a result the virus brought down several important systems. The Bank of America's ATM service crashed, the city of Seattle suffered outages in 911 service and Continental Airlines had to cancel several flights due to electronic ticketing and check-in errors.

The culprit was the SQL Slammer virus, also known as Sapphire. By some estimates, the virus caused more than $1 billion in damages before patches and antivirus software caught up to the problem. The progress of Slammer's attack is well documented. Only a few minutes after infecting its first Internet server, the Slammer virus was doubling its number of victims every few seconds. Fifteen minutes after its first attack, the Slammer virus infected nearly half of the servers that act as the pillars of the Internet.

The Slammer virus taught a valuable lesson: It's not enough to make sure you have the latest patches and antivirus software. Hackers will always look for a way to exploit any weakness, particularly if the vulnerability isn't widely known. While it's still important to try and head off viruses before they hit you, it's also important to have a worst-case-scenario plan to fall back on should disaster strike.

*Answer the questions:*

1 When did a new Web server virus spread across the Internet?

2 What was the result of the attack of a new Web server virus?

3 How much did the virus cause in damages before patches and antivirus software caught up to the problem?

4 What tine did it take to Slammer virus to infect nearly half of the servers that act as the pillars of the Internet?

5 What lesson did The Slammer virus teach?

*Translate without dictionary:*

**A Matter of Timing**

to sit dormant – находиться в состоянии покоя
unleash an attack – начать атаку

Some hackers program viruses to sit dormant on a victim's computer only to unleash an attack on a specific date. Here's a quick sample of some famous viruses that had time triggers:

- The Jerusalem virus activated every Friday the 13th to destroy data on the victim computer's hard drive.
- The Michelangelo virus activated on March 6, 1992 -- Michelangelo was born on March 6, 1475.
- The Chernobyl virus activated on April 26, 1999 -- the 13th anniversary of the Chernobyl meltdown disaster.
- The Nyxem virus delivered its payload on the third of every month, wiping out files on the victim's computer.

Computer viruses can make a victim feel helpless, vulnerable and despondent.

*Next, we'll look at a virus with a name that evokes all three of those feelings.*

**7 MyDoom**

doom [du:m] – 1. рок, судьба 2. гибель, смерть

trigger ['trigə] - спусковой крючок

outbreak ['aʊtbreik] – вспышка
search engine - поисковая система
eventually - в конце концов
a search request - поисковый запрос
spoof [spu:f] – подменить
to track [træk] – отследить

The MyDoom (or Novarg) virus is another worm that can create a backdoor in the victim computer's operating system. The original MyDoom virus - there have been several variants - had two triggers. One trigger caused the virus to begin a denial of service (DoS) attack starting Feb. 1, 2004. The second trigger commanded the virus to stop distributing itself on Feb. 12, 2004. Even after the virus stopped spreading, the backdoors created during the initial infections remained active.

Later that year, a second outbreak of the MyDoom virus gave several search engine companies grief. Like other viruses, MyDoom searched victim computers for e-mail addresses as part of its replication process. But it would also send a search request to a search engine and use e-mail addresses found in the search results. Eventually, search engines like Google began to receive millions of search requests from corrupted computers. These attacks slowed down search engine services and even caused some to crash.

MyDoom spread through e-mail and peer-to-peer networks. According to the security firm Message Labs, one in every 12 e-mail messages carried the virus at one time. Like the Klez virus, MyDoom could spoof e-mails so that it became very difficult to track the source of the infection.

*Answer the questions:*

1) What can the MyDoom (or Novarg) virus create?

2) Which two triggers did the original MyDoom virus had?

3) Why did a second outbreak of the MyDoom virus give several search engine companies grief?

4) How did MyDoom spread?

5) Which similarities did the Klez virus and MyDoom have?

*Translate without dictionary:*

**Oddball Viruses**

to act in odd ways - действовать странным образом

Not all viruses cause severe damage to computers or destroy networks. Some just cause computers to act in odd ways. An early virus called Ping-Pong created a bouncing ball graphic, but didn't seriously damage the infected computer. There are

several joke programs that might make a computer owner think his or her computer is infected, but they're really harmless applications that don't self-replicate. When in doubt, it's best to let an antivirus program remove the application.

Next, we'll take a look at a pair of viruses created by the same hacker: the Sasser and Netsky viruses.

### 8 Sasser and Netsky

random ['rændəm] – случайный

to alter ['ɒltə] – изменять
to spoof [spu:f] – подделывать

probation [prə'beɪʃən] – испытательный срок

Sometimes computer virus programmers escape detection. But once in a while, authorities find a way to track a virus back to its origin. Such was the case with the Sasser and Netsky viruses. A 17-year-old German named Sven Jaschan created the two programs and unleashed them onto the Internet. While the two worms behaved in different ways, similarities in the code led security experts to believe they both were the work of the same person.

The Sasser worm attacked computers through a Microsoft Windows vulnerability. Unlike other worms, it didn't spread through e-mail. Instead, once the virus infected a computer, it looked for other vulnerable systems. It contacted those systems and instructed them to download the virus. The virus would scan random IP addresses to find potential victims. The virus also altered the victim's operating system in a way that made it difficult to shut down the computer without cutting off power to the system.

The Netsky virus moves through e-mails and Windows networks. It spoofs e-mail addresses and propagates through a 22,016-byte file attachment. As it spreads, it can cause a denial of service (DoS) attack as systems collapse while trying to handle all the Internet traffic. At one time, security experts at Sophos believed Netsky and its variants accounted for 25 percent of all computer viruses on the Internet.

Sven Jaschan spent no time in jail; he received a sentence of one year and nine months of probation. Because he was under 18 at the time of his arrest, he avoided being tried as an adult in German courts.

So far, most of the viruses we've looked at target PCs running Windows. But Macintosh computers aren't immune to computer virus attacks. In the next section, we'll take a look at the first virus to commit a Mac attack.

*Answer the questions:*

1) Who created the the Sasser and Netsky viruses and unleashed them onto the Internet?

2) Why did security experts believe they both were the work of the same person?

3) How did the Sasser worm attack computers?
4) How did the Sasser worm spread?
5) How did the Sasser worm alter the victim's operating system?
6) How did The Netsky virus move?
7) What happened after The Netsky virus spread?
8) What punishment did Sven Jaschan suffer?

*Translate without dictionary:*

**Black Hats**

Just as you'd find good and bad witches in Oz, you can find good and bad hackers in our world. One common term for a hacker who sets out to create computer viruses or compromise system security is a *black hat*. Some hackers attend conventions like the Black Hat conference or Defcon to discuss the impact of black hats and how they use vulnerabilities in computer security systems to commit crimes.

**9 Leap-A/Oompa-A**

security through obscurity – безопасность через неясность
instant messaging program - программа обмена мгновенными сообщениями
can fall prey - может стать жертвой
snarl network traffic – спутывать сетевой трафик

revenge [rɪ'vendʒ] – месть
What computer virus has landed the number one spot? – Какой компьютерный вирус займет первое место?

Maybe you've seen the ad in Apple's Mac computer marketing campaign where Justin "I'm a Mac" Long consoles John "I'm a PC" Hodgman. Hodgman comes down with a virus and points out that there are more than 100,000 viruses that can strike a computer. Long says that those viruses target PCs, not Mac computers.

For the most part, that's true. Mac computers are partially protected from virus attacks because of a concept called *security through obscurity*. Apple has a reputation for keeping its operating system (OS) and hardware a closed system - Apple produces both the hardware and the software. This keeps the OS obscure. Traditionally, Macs have been a distant second to PCs in the home computer market. A hacker who creates a virus for the Mac won't hit as many victims as he or she would with a virus for PCs.

But that hasn't stopped at least one Mac hacker. In 2006, the Leap-A virus, also known as Oompa-A, debuted. It uses the iChat instant messaging program to propagate across vulnerable Mac computers. After the virus infects a Mac, it searches through the iChat contacts and sends a message to each person on the list. The message contains a corrupted file that appears to be an innocent JPEG image.

The Leap-A virus doesn't cause much harm to computers, but it does show that even a Mac computer can fall prey to malicious software. As Mac computers become more popular, we'll probably see more hackers create customized viruses that could

damage files on the computer or snarl network traffic. Hodgman's character may yet have his revenge.

We're down to the end of the list. What computer virus has landed the number one spot?

*Answer the questions:*

1) How many viruses can strike a computer according to Hodgman?

2) Why are Mac computers partially protected from virus attacks?

3) Which viruses debuted in 2006?

4) What program did the Leap-A virus use to propagate across vulnerable Mac computers?

5) Does the Leap-A virus cause much harm to computers?

*Translate without dictionary:*

**Breaking into Song**

computer viruses can pose a serious threat - компьютерные вирусы могут представлять серьезную угрозу

the media overstates the impact of a particular virus - средства массовой информации преувеличивают влияние конкретного вируса

While computer viruses can pose a serious threat to computer systems and Internet traffic, sometimes the media overstates the impact of a particular virus. For example, the Michelangelo virus gained a great deal of media attention, but the actual damage caused by the virus was pretty small. That might have been the inspiration for the song "Virus Alert" by "Weird Al" Yankovic. The song warns listeners of a computer virus called Stinky Cheese that not only wipes out your computer's hard drive, but also forces you to listen to Jethro Tull songs and legally change your name to Reggie

**10 Storm Worm**

dread [dred] – ужасный, страшный

to batter – громить, разрушать

downloading the application – скачивание приложения

fake links - поддельные ссылки

The latest virus on our list is the dreaded Storm Worm. It was late 2006 when computer security experts first identified the worm. The public began to call the virus the Storm Worm because one of the e-mail messages carrying the virus had as its subject "230 dead as storm batters Europe." Antivirus companies call the worm other names. For example, Symantec calls it Peacomm while McAfee refers to it as Nuwar. This might sound confusing, but there's already a 2001 virus called the W32.Storm.Worm. The 2001 virus and the 2006 worm are completely different programs.

The Storm Worm is a Trojan horse program. Its payload is another program, though not always the same one. Some versions of the Storm Worm turn computers into *zombies* or *bots*. As computers become infected, they become vulnerable to remote control by the person behind the attack. Some hackers use the Storm Worm to create a *botnet* and use it to send spam mail across the Internet.

Many versions of the Storm Worm fool the victim into downloading the application through fake links to news stories or videos. The people behind the attacks will often change the subject of the e-mail to reflect current events. For example, just before the 2008 Olympics in Beijing, a new version of the worm appeared in e-mails with subjects like "a new deadly catastrophe in China" or "China's most deadly earthquake." The e-mail claimed to link to video and news stories related to the subject, but in reality clicking on the link activated a download of the worm to the victim's computer.

Several news agencies and blogs named the Storm Worm one of the worst virus attacks in years. By July 2007, an official with the security company Postini claimed that the firm detected more than 200 million e-mails carrying links to the Storm Worm during an attack that spanned several days. Fortunately, not every e-mail led to someone downloading the worm.

Although the Storm Worm is widespread, it's not the most difficult virus to detect or remove from a computer system. If you keep your antivirus software up to date and remember to use caution when you receive e-mails from unfamiliar people or see strange links, you'll save yourself some major headaches.

*Decide if there statements TRUE or FALSE:*

1) The public began to call the virus the Storm Worm because one of the e-mail messages carrying the virus had as its subject "230 dead as storm batters Asia."

2) The 2001 virus and the 2006 worm are the same programs.

3) The Storm Worm is a worm.

4) As computers become infected, they become vulnerable to remote control by the hacker.

5) Some hackers use the Storm Worm to create a *backdoor* and use it to send spam mail across the Internet.

6) Many versions of the Storm Worm fool the victim into downloading the application through links to news stories or videos.

7) By July 2007, an official with the security company Postini claimed that the firm detected more than 200 million e-mails carrying links to the Storm Worm during an attack that spanned several months.

8) Although the Storm Worm is widespread, it's the most difficult virus to detect or remove from a computer system

*Translate without dictionary:*

**Malware**

a software app – программное приложение
logging keystrokes - протоколирования нажатия клавиш

Computer viruses are just one kind of malware. Other types include spyware and some kinds of adware. Spyware spies on what a user does with his or her computer. That can include logging keystrokes as a way to discover login codes and passwords. Adware is a software app that displays ads to users while they use a larger application like a Web browser. Some adware contains code that gives advertisers extensive access to private information.

**Unit test 1**

*1 March the words with their definitions:*

| | |
|---|---|
| 1 Malware | a) are malicious program disguised as innocent-looking files or embedded within legitimate software. Once they are activated, they may affect the computer in a variety of ways: some are just annoying; others are more ominous, creating a backdoor to the computer which can be used to collect stored data. |
| 2 Viruses | b) is a type of software designed to hide the fact that an operating system has been compromised, sometimes by replacing vital executables. This malware allow viruses and malware to "hide in plain sight" by disguising as necessary files that your antivirus software will overlook. |
| 3 Worms | c) is a program that installs an additional component that feeds advertising, often by delivering pop-up ads or by installing a toolbar in your browser. |
| 4 Trojan horses | d) is the language the hacker used to create the worm. |
| 5 A backdoor | e) they don't actually cause any harm or replicate themselves. |
| 6 Spyware | f) created a bouncing ball graphic, but didn't seriously damage the infected computer. There are several joke programs that might make a computer owner think his or her computer is infected, but they're really harmless applications that don't self-replicate. |
| 7 Rootkit | g)is when the worm creates a backdoor into the computer's operating system, allowing a remote user to access and control the machine. |
| 8 Adware | h) means that Apple has a reputation for keeping its operating system (OS) and hardware a closed system - Apple produces both the hardware and the software. |
| 9 Visual Basic Scripting | i) are self-copying program that have the capacity to move from one computer to another without human help, by exploiting security flaws in computer networks. |
| 10 A buffer overflow problem | g) is software designed to collect information from computers for commercial or criminal purposes, is another example of malicious software. |
| 11 A virus hoaxes or fake viruses | k) which means when a machine running on these operating systems receives more information than its buffers can handle; it |

| | |
|---|---|
| | starts to overwrite adjacent memory. |
| 12 system-level compromise | l) are programs that spread by attaching themselves to executable files or documents. |
| 13 Ping-Pong | m) is one common term for a hacker who sets out to create computer viruses or compromise system security. |
| 14 A black hat | n) is a secret or undocumented means of getting into a computer system. |
| 15 Security through obscurity | o) is software created to damage or alter the computer data or operations. |

*2 Which malware*

a) popped up in the summer of 2001. Both worms exploited an operating system vulnerability that was found in machines running Windows 2000 and Windows NT.

b) was created in the spring of 1999 by a man named David L. This computer virus was based on a Microsoft Word macro.

c) got its name because one of the e-mail messages carrying the virus had as its subject "230 dead as storm batters Europe."

d) ‘s name means “admin” spelled backwards.

e) sent e-mail said that the message was a love letter from a secret admirer.

f) had two triggers.

g) infected a victim's computer through an e-mail message, replicated itself and then sent itself to people in the victim's address book in late 2001.

h) uses the iChat instant messaging program to propagate across vulnerable Mac computers.

i) caused more than $1 billion in damages before patches and antivirus software caught up to the problem.

j) behaved in different ways, similarities in the code that led security experts to believe they both were the work of the same person.

k) tempts recipients into opening a document with an e-mail message like "Here is that document you asked for, don't show it to anybody else." Once activated, the virus replicates itself and sends itself out to the top 50 people in the recipient's e-mail address book.

l) turn computers into zombies or bots. As computers become infected, they become vulnerable to remote control by the person behind the attack. Some hackers use the Storm Worm to create a botnet and use it to send spam mail across the Internet.

m) caused $10 billion in damages.

n) doesn't cause much harm to computers, but it does show that even a Mac computer can fall prey to malicious software

o) carried other harmful programs that could render a victim's computer inoperable. Depending on the version, this virus could act like a normal computer virus, a worm or a Trojan horse.

p) didn't spread through e-mail. Instead, once the virus infected a computer, it looked for other vulnerable systems. It contacted those systems and instructed them to download the virus.

q) initiated a distributed denial of service (DDoS) attack on the White House. That means all the computers infected with this virus tried to contact the Web servers at the White House at the same time, overloading the machines.

r) searched victim computers for e-mail addresses as part of its replication process. But it would also send a search request to a search engine and use e-mail addresses found in the search results.

s) 's primary targets were Internet servers. While it could infect a home PC, its real purpose was to bring Internet traffic to crawl.

t) was doubling its number of victims every few seconds. Fifteen minutes after its first attack, this virus infected nearly half of the servers that act as the pillars of the Internet

*3 Complete the text with words from the box:*

**What is Malware**

| flash drive | virus | antivirus software | wipe your computer clean |
|---|---|---|---|
| hard drive | malware | | |

We all know malware is out there ____ (1) includes applications that spy on you, corrupt your data, destroy your ____ (2) or give control of your machine to someone thousands of miles away. No matter what form it takes, it’s bad business. And since there are a lot of examples of malware in the wild, it may only be a matter of time before you become the victim of a malware attack.

The most important advice we can give anyone who believes he or she has a computer with malware on it is this: Don't panic. Also, don't assume that you need to ____ (3) and start from scratch. Often you can remove malware without having to erase everything else. You may lose some data in the process, but you probably won't lose everything.

First you need to determine if your computer has a ____ (4) at all. You might suspect your computer of having a virus if it seems to be sluggish. If your Web browser suddenly looks different or automatically goes to a site you don't recognize, that's a good indication that you've got some malware. If your computer is unstable and crashes fairly often, you may have a problem. And if you try to access files but receive a message saying they're corrupted, that's another sign.

If you do think your computer has a virus, you need to run ____ (5) to weed it out. Some viruses disable antivirus software -- they're clever that way. If you don't have any antivirus software, now's a good time to purchase or download an application. A few malware variants will try to block you from downloading antivirus software. If that's the case, you may need to download the software on another computer and transfer it to disk or a _____ (6) .

*4 Complete the table below:*

| | Type of malware | Was created in … year | Was created by (whom) | Spread | damage | Punishment of hacker created the malware |
|---|---|---|---|---|---|---|
| 1 Melissa | | | | | | |
| 2 ILOVEYOU | | | | | | |
| 3 The Klez Virus | | | | | | |
| 4 Code Red and Code Red II | | | | | | |
| 5 Nimda | | | | | | |
| 6 SQL Slammer /Sapphire | | | | | | |
| 7 MyDoom | | | | | | |
| 8 Sasser and Netsky | | | | | | |
| 9 Leap-A/Oompa-A | | | | | | |
| 10 Storm Worm | | | | | | |

*5 Work in pairs. Each student retells about 5 malwares using information from the table.*

**Unit 2**
**Hackers**
**Text 1**

**How hackers work**

summons ['sʌmənz] up thoughts– вызывает мысли

to harass ['hærəs] people - чтобы преследовать людей

defraud [dɪ'frɔːd] corporations - обманывать корпорации

infiltrating military computer systems – проникая в военные компьютерные системы

while there's no denying - хотя нет никаких сомнений

visionary ['vɪʒənri] – мечтатель

no one else could conceive [kən'siːv] - никто другой не мог представить себе

in this sense - в этом смысле

a unifying trait - объединяющая особенность

bordering on obsession - граничащее с одержимостью

bug [bʌg] - ошибка в компьютерной программе
to land a job - получить работу
as computers evolved - по мере развития компьютеров

intricacy ['intrikəsi] – запутанность, сложность

endeavour [en'devə] – попытка

Thanks to the media, the word "hacker" has gotten a bad reputation. The word summons up thoughts of malicious computer users finding new ways to harass people, defraud corporations, steal information and maybe even destroy the economy or start a war by infiltrating military computer systems. While there's no denying that there are hackers out there with bad intentions, they make up only a small percentage of the hacker community.

The term computer hacker first showed up in the mid-1960s. A hacker was a programmer - someone who hacked out computer code. Hackers were visionaries who could see new ways to use computers, creating programs that no one else could conceive. They were the pioneers of the computer industry, building everything from small applications to operating systems. In this sense, people like Bill Gates, Steve Jobs and Steve Wozniak were all hackers - they saw the potential of what computers could do and created ways to achieve that potential.

A unifying trait among these hackers was a strong sense of curiosity, sometimes bordering on obsession. These hackers prided themselves on not only their ability to create new programs, but also to learn how other programs and systems worked. When a program had a *bug* - a section of bad code that prevented the program from working properly - hackers would often create and distribute small sections of code called *patches* to fix the problem. Some managed to land a job that leveraged their skills, getting paid for what they'd happily do for free.

As computers evolved, computer engineers began to network individual machines together into a system. Soon, the term hacker had a new meaning - a person using computers to explore a network to which he or she didn't belong. Usually hackers didn't have any malicious intent. They just wanted to know how computer networks worked and saw any barrier between them and that knowledge as a challenge.

In fact, that's still the case today. While there are plenty of stories about malicious hackers sabotaging computer systems, infiltrating networks and spreading computer viruses, most hackers are just curious - they want to know all the intricacies of the computer world. Some use their knowledge to help corporations and governments construct better security measures. Others might use their skills for more unethical endeavors.

In this article, we'll explore common techniques hackers use to infiltrate systems. We'll examine hacker culture and the various kinds of hackers as well as learn about famous hackers, some of whom have run afoul of the law.

*1 Answer the questions:*

1) Why has the word "hacker" gotten a bad reputation?
2) When did the term computer hacker first show up?
3) Who was a hacker?
4) Why were Bill Gates, Steve Jobs and Steve Wozniak all hackers?
5) What was a unifying trait among these hackers?
6) What would hackers often create and distribute when a program had a bug?
7) Which a new meaning did the term hacker have?
8) What did hackers have instead of any malicious intent?

*2 Find the synonyms in the text to these words:*

Chase; penetrate; purpose; appear; dreamer; first; peculiarity; error; to find a job; happen; a lot of

*3 Match two words to make collocations:*

| | |
|---|---|
| to harass | curiosity |
| to defraud | programs |
| hacker | networks |
| creating | corporations |
| a unifying | their skills |
| sense of | people |
| leveraged | trait |
| infiltrating | community |

*4 Complete the summary of the text:*

The word "hacker" summons up thoughts of ____ (1) computer users finding new ways to harass people, defraud corporations, steal information and maybe even destroy the economy or start a war by infiltrating military computer systems. Hackers were ____ (2) who could see new ways to use computers, creating programs that no one else could conceive. When a program had a bug - a section of bad code that prevented the program from working properly - hackers would often create and distribute small sections of code called ____ (3) to fix the problem. Hackers just wanted to know how computer networks worked and saw any barrier between them and that knowledge as a ____ (4).

*Translate without dictionary:*

**Super Phreak**

Before computer hackers, curious and clever individuals found ways to manipulate the phone system in a phenomenon called phreaking**.** Through phreaking, these individuals found ways to make long distance calls for free or sometimes just played pranks on other telephone users.

**Hacker Hierarchy**

Newbie ['nju:.bi] – новичок

hacking tools - хакерские утилиты
to boast [bəust] about their accomplishments - похвастаться своими достижениями
proprietary [prəˈpraiətəri] information - служебная информация

Psychologist Marc Rogers says there are several subgroups of hackers - *newbies*, *cyberpunks*, *coders* and *cyber terrorists*. Newbies are hackers who have access to hacking tools but aren't really aware of how computers and programs work. Cyberpunks are savvier and are less likely to get caught than a newbie while hacking a system, but they have a tendency to boast about their accomplishments. Coders write the programs other hackers use to infiltrate and navigate computer systems. A cyber terrorist is a professional hacker who infiltrates systems for profit - he might sabotage a company or raid a corporation's databases for proprietary information.

*Continue the sentences:*

1) Newbies are hackers who have access to hacking tools but …

2) Cyberpunks are savvier and are less likely to get caught than a newbie while hacking a system, but …

3) Coders write the programs other hackers use to …

4) A cyber terrorist is a professional hacker who infiltrates systems for profit ...

**Text 2**

## The Hacker Toolbox

hacking tools – хакерские утилиты
to rely upon - полагаться на
apart from their own ingenuity [ˌindʒəˈnjuːiti] - кроме их собственной изобретательности
log keystrokes - вход с помощью нажатия клавиш
the trial [traɪəl]and error method of hacking passwords - метод проб и ошибок взлома паролей
a brute force attack - перебор всех вариантов
Distributed Denial of Service (DDoS) - распределенный отказ в обслуживании
to intercept - перехватывать
wiretapping - прослушивание телефонных разговоров

The main resource hackers rely upon, apart from their own ingenuity, is computer code. While there is a large community of hackers on the Internet, only a relatively small number of hackers actually program code. Many hackers seek out and download code written by other people. There are thousands of different programs hackers use to explore computers and networks. These programs give hackers a lot of power over innocent users and organizations - once a skilled hacker knows how a system works, he can design programs that exploit it.

*Malicious hackers use programs to:*

- *Log keystrokes*: Some programs allow hackers to review every keystroke a computer user makes. Once installed on a victim's computer, the programs record each keystroke, giving the hacker everything he needs to infiltrate a system or even steal someone's identity.
- *Hack passwords*: There are many ways to hack someone's password, from educated guesses to simple *algorithms* that generate combinations of letters, numbers and symbols. The trial and error method of hacking passwords is called a *brute force attack*, meaning the hacker tries to generate every possible combination to gain access. Another way to hack passwords is to use a *dictionary attack*, a program that inserts common words into password fields.
- *Infect a computer or system with a virus*: Computer viruses are programs designed to duplicate themselves and cause problems ranging from crashing a computer to wiping out everything on a system's hard drive. A hacker might install a virus by infiltrating a system, but it's much more common for hackers to create simple viruses and send them out to potential victims via email, instant messages, Web sites with downloadable content or peer-to-peer networks.
- *Gain backdoor access:* Similar to hacking passwords, some hackers create programs that search for unprotected pathways into network systems and computers. In the early days of the Internet, many computer systems had limited security, making it possible for a hacker to find a pathway into the system without a username or password. Another way a hacker might gain backdoor access is to infect a computer or system with a *Trojan horse*.
- *Create zombie computers*: A zombie computer, or bot, is a computer that a hacker can use to send spam or commit *Distributed Denial of Service* (DDoS) attacks. After a victim executes seemingly innocent code, a connection opens between his computer and the hacker's system. The hacker can secretly control the victim's computer, using it to commit crimes or spread spam.
- *Spy on e-mail*: Hackers have created code that lets them intercept and read e-mail messages - the Internet's equivalent to wiretapping. Today, most e-mail programs use encryption formulas so complex that even if a hacker intercepts the message, he won't be able to read it.

*1 March the words with their definitions:*

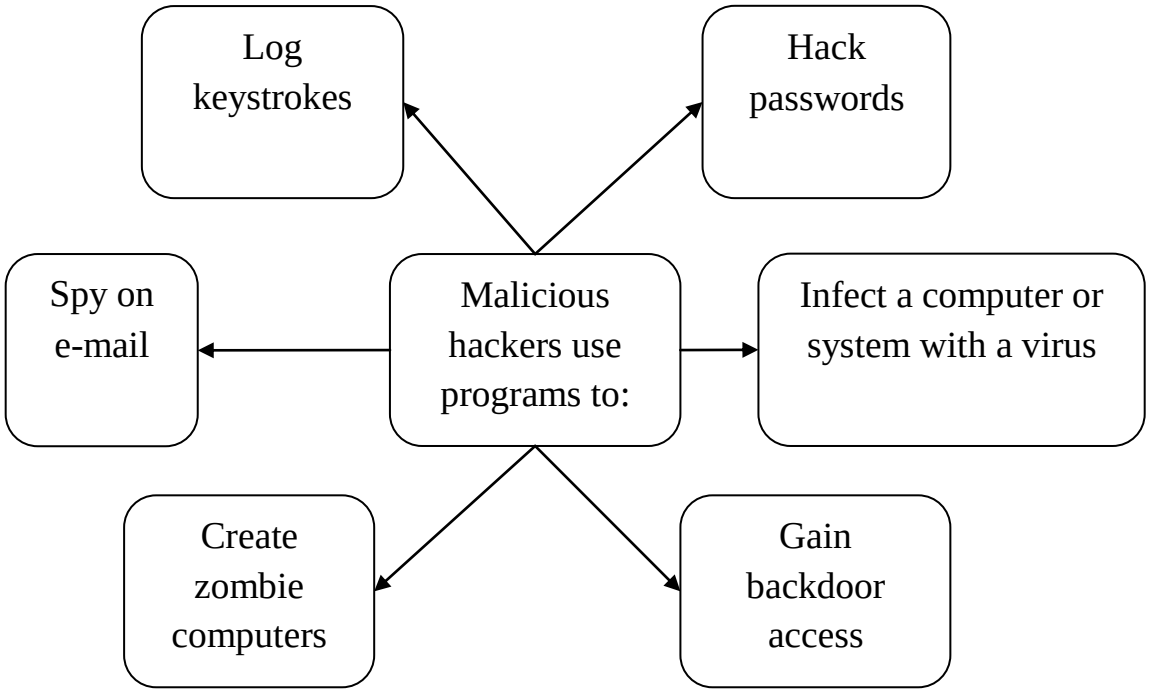
| | |
|---|---|
| 1 Log keystrokes | a) is a program that inserts common words into password fields. |
| 2 algorithms | b) are programs that search for unprotected pathways into network systems and computers. |
| 3 **a** brute force attack | c) are programs designed to duplicate themselves and cause problems ranging from crashing a computer to wiping out everything on a system's hard drive. |
| 4 a dictionary | d) is a computer that a hacker can use to send spam or commit |

| | |
|---|---|
| attack | *Distributed Denial of Service* (DDoS) attacks. |
| 5 Computer viruses | e) are the programs record each keystroke, giving the hacker everything he needs to infiltrate a system or even steal someone's identity. |
| 6 Gain backdoor access | f) is a code that lets hackers intercept and read e-mail messages - the Internet's equivalent to wiretapping. |
| 7 A zombie computer or bot | g) is the trial and error method of hacking passwords. |
| 8 Spy on e-mail | h) generate combinations of letters, numbers and symbols. |

*2 Answer the questions:*

1) What is the main resource hackers rely upon?
2) Do a lot of hackers actually program code?
3) What do different programs hackers use to explore computers and networks give hackers?
4) What programs allow hackers to review every keystroke a computer user makes?
5) How can hackers hack anyone's password?
6) How might a hacker install a virus?
7) How does a hacker gain backdoor access?
8) What is a zombie computer, or bot?
9) How can hackers intercept and read e-mail messages?

3 Look at the scheme and retell the text:




*Translate without dictionary:*

## Hackers and Crackers

law-abiding – законопослушный
maliciously – злонамеренно
mischief - нанесение ущерба

Many computer programmers insist that the word "hacker" applies only to law-abiding enthusiasts who help create programs and applications or improve computer security. Anyone using his or her skills maliciously isn't a hacker at all, but a *cracker*.

Crackers infiltrate systems and cause mischief, or worse. Unfortunately, most people outside the hacker community use the word as a negative term because they don't understand the distinction between hackers and crackers.

**Text 3**

## Hacker Culture

to neglect [nɪ'glekt] – пренебрегать
bulletin board systems - электронная доска объявлений
accomplishments – достижения

to boast [bəʊst] - хвастаться
to upload – загрузить
to prove their claims - чтобы доказать свои претензии
law enforcement officials - сотрудники правоохранительных органов
at will – при желании
dedicate to – посвящать
a live broadcast section – раздел онлайн вещания
newsstand – газетный киоск

overwhelmingly [ˌəʊvə'welmɪŋli] - в подавляющем большинстве
a battleground – поле боя

to bolster ['bəʊlstə] security systems - укрепить системы безопасности
open source software - программного обеспечения с открытым исходным кодом
low-tech living arrangements – низкотехнологичные условия проживания

Individually, many hackers are antisocial. Their intense interest in computers and programming can become a communication barrier. Left to his or her own devices, a hacker can spend hours working on a computer program while neglecting everything else.

Computer networks gave hackers a way to associate with other people with their same interests. Before the Internet became easily accessible, hackers would set up and visit *bulletin board systems* (BBS). A hacker could host a bulletin board system on his or her computer and let people dial into the system to send messages, share information, play games and download programs. As hackers found one another, information exchanges increased dramatically.

Some hackers posted their accomplishments on a BBS, boasting about infiltrating secure systems. Often they would upload a document from their victims'

databases to prove their claims. By the early 1990s, law enforcement officials considered hackers an enormous security threat. There seemed to be hundreds of people who could hack into the world's most secure systems at will.

There are many Web-sites dedicated to hacking. The hacker journal *"2600: The Hacker Quarterly"* has its own site, complete with a live broadcast section dedicated to hacker topics. The print version is still available on newsstands. Web sites like *Hacker.org* promote learning and include puzzles and competitions for hackers to test their skills.

When caught - either by law enforcement or corporations - some hackers admit that they could have caused massive problems. Most hackers don't want to cause trouble; instead, they hack into systems just because they wanted to know how the systems work. To a hacker, a secure system is like *Mt. Everest*- he or she infiltrates it for the sheer challenge. In the United States, a hacker can get into trouble for just entering a system. *The Computer Fraud and Abuse Act* outlaws unauthorized access to computer systems.

Not all hackers try to explore forbidden computer systems. Some use their talents and knowledge to create better software and security measures. In fact, many hackers who once used their skills to break into systems now put that knowledge and ingenuity to use by creating more comprehensive security measures. In a way, the Internet is a battleground between different kinds of hackers - the bad guys, or *black hats*, who try to infiltrate systems or spread viruses, and the good guys, or *white hats*, who bolster security systems and develop powerful virus protection software.

Hackers on both sides overwhelmingly support *open source software*, programs in which the source code is available for anyone to study, copy, distribute and modify. With open source software, hackers can learn from other hackers' experiences and help make programs work better than they did before. Programs might range from simple applications to complex operating systems like *Linux.*

There are several annual hacker events, most of which promote responsible behavior. A yearly convention in Las Vegas called *DEFCON* sees thousands of attendees gather to exchange programs, compete in contests, participate in panel discussions about hacking and computer development and generally promote the pursuit of satisfying curiosity. A similar event called the *Chaos Communication Camp* combines low-tech living arrangements - most attendees stay in tents - and high-tech conversation and activities.

*1 March the words with their definitions:*

| | |
|---|---|
| 1 bulletin board systems (BBS) | a) promote learning and include puzzles and competitions for hackers to test their skills. |
| 2 "2600: The Hacker Quarterly" | b) are the hackers who try to infiltrate systems or spread viruses. |
| 3 Web sites like Hacker.org | c) is programs in which the source code is available for anyone to study, copy, distribute and modify. |
| 4 The Computer | d) are the hackers who bolster security systems and develop |

| | |
|---|---|
| Fraud and Abuse Act | powerful virus protection software. |
| 5 Black hats | e) is The hacker journal which has its own site, complete with a live broadcast section dedicated to hacker topics. The print version is still available on newsstands. |
| 6 White hats | f) is a event combining low-tech living arrangements - most attendees stay in tents - and high-tech conversation and activities. |
| 7Open source software | g) is a yearly convention in Las Vegas sees thousands of attendees gather to exchange programs, compete in contests, participate in panel discussions about hacking and computer development and generally promote the pursuit of satisfying curiosity. |
| 8 Linux | h) outlaws unauthorized access to computer systems. |
| 9 DEFCON | i) is programs might range from simple applications to complex operating systems. |
| 10 Chaos Communication Camp | j) is a system a hacker could host on his or her computer and let people send messages, share information, play games and download programs. |

*Answer the questions:*

1) What is *bulletin board systems* (BBS)?

2) Why do some hackers post their accomplishments on a BBS?

3) Why did law enforcement officials consider hackers an enormous security threat by the early 1990s?

4) Which Web-sites dedicated to hacking do you know?

5) Why do most hackers hack into systems?

6) Which Act outlaws unauthorized access to computer systems?

7) Who are *black hats* and white *hats*? What are their aims?

8) What is *open source software*, programs?

9) Why do thousands of attendees gather in Las Vegas?

10) What do you know about the *Chaos Communication Camp?*

**Text 4**

**Hackers and the Law**

nightmare ['naɪtmeə] – кошмар
slip in and out of computers undetected - проскользнуть в и из компьютеров незамеченными
hefty fine - высоки штраф
jail [dʒeɪl] time - тюремное заключение
minor offenses - незначительные преступления
six months' probation - испытательный срок шесть месяцев
a maximum sentence – максимальный приговор
the Department of Justice - Министерство юстиции
the financial damage - финансовый ущерб
an appropriate punishment - соответствующее наказание

vague [veɪg] – расплывчатый, неясный

legitimate [lə'dʒɪtɪmət] applications – приложение к закону

flaw [flɔː] – недостаток

prosecuting ['prɒsɪkjuːt] - уголовное преследование

to petition [pə'tɪʃən] – ходатайствовать
to hold a trial - в целях проведения судебного разбирательства
the Department of Defense - Министерство обороны

In general, most governments aren't too crazy about hackers. Hackers' ability to slip in and out of computers undetected, stealing classified information when it amuses them, is enough to give a government official a nightmare. Secret information, or *intelligence*, is incredibly important. Many government agents won't take the time to differentiate between a curious hacker who wants to test his skills on an advanced security system and a spy.

Laws reflect this attitude. In the United States, there are several laws forbidding the practice of hacking. Some, like 18 U.S.C. § 1029, concentrate on the creation, distribution and use of codes and devices that give hackers unauthorized access to computer systems. The language of the law only specifies using or creating such a device with the intent to defraud, so an accused hacker could argue he just used the devices to learn how security systems worked.

Another important law is 18 U.S.C. § 1030, part of which forbids unauthorized access to government computers. Even if a hacker just wants to get into the system, he or she could be breaking the law and be punished for accessing a non public government computer.

Punishments range from hefty fines to jail time. Minor offenses may earn a hacker as little as six months' probation, while other offenses can result in a maximum sentence of 20 years in jail. One formula on the Department of Justice's Web page factors in the financial damage a hacker causes, added to the number of his victims to determine an appropriate punishment.

Other countries have similar laws, some much more vague than legislation in the U.S. A recent German law forbids possession of "hacker tools." Critics say that the law is too broad and that many legitimate applications fall under its vague definition of hacker tools. Some point out that under this legislation, companies would be breaking the law if they hired hackers to look for flaws in their security systems.

Hackers can commit crimes in one country while sitting comfortably in front of their computers on the other side of the world. Therefore, prosecuting a hacker is a complicated process. Law enforcement officials have to petition countries to *extradite* suspects in order to hold a trial, and this process can take years. One famous case is the United States' indictment of hacker Gary McKinnon. Since 2002, McKinnon fought extradition charges to the U.S. for hacking into the Department of Defense and NASA computer systems. McKinnon, who hacked from the United Kingdom, defended himself by claiming that he merely pointed out flaws in important security

systems. In April 2007, his battle against extradition came to an end when the British courts denied his appeal.

*1 Answer the questions:*

1) Which hackers' ability is enough to give a government official a nightmare?
2) What are laws in the United States against hackers?
3) Which the punishment does law provide for hackers?
4) Why is the definition of "hacker tools" vague?
5) When would be companies breaking the law?
6) Prosecuting a hacker is a simple process, isn't it?
7) What was McKinnon's blame?

*2 Match two words to make collocations:*

| | |
|---|---|
| 1 extradition | a) suspects |
| 2 government | b) access |
| 3 hacker | c) punishment |
| 4 to extradite | d) fines |
| 5 commit | e) hacker |
| 6 unauthorized | f) charges |
| 7 hefty | g) offenses |
| 8 curious | h) tools |
| 9 an appropriate | i) crimes |
| 10 minor | j) computers |

*3 Complete the sentences with collocations from the exercise 2:*

1) Many government agents won't take the time to differentiate between a ____ (1) who wants to test his skills on an advanced security system and a spy.

2) In the United States, the law 18 U.S.C. § 1029, concentrate on the creation, distribution and use of codes and devices that give hackers ____ (2) to computer systems.

3) Another important law is 18 U.S.C. § 1030, part of which forbids unauthorized access to ____ (3).

4) Punishments range from ____ (4) to jail time.

5) May earn a hacker as little as six months' probation, while other offenses can result in a maximum sentence of 20 years in jail.

6) One formula on the Department of Justice's Web page factors in the financial damage a hacker causes, added to the number of his victims to determine ____ (6).

7) Critics say that the law is too broad and that many legitimate applications fall under its vague definition of ____ (7).

8) Hackers can ____ (8) in one country while sitting comfortably in front of their computers on the other side of the world.

9) Law enforcement officials have to petition countries ____ (9) in order to hold a trial, and this process can take years.

10) Since 2002, McKinnon fought ____ (10) to the U.S. for hacking into the Department of Defense and NASA computer systems.

*Translate without dictionary:*

**Hacking a Living**

Hackers who obey the law can make a good living. Several companies hire hackers to test their security systems for flaws. Hackers can also make their fortunes by creating useful programs and applications, like Stanford University students Larry Page and Sergey Brin. Page and Brin worked together to create a search engine they eventually named Google. Today, they are tied for 26th place on Forbes' list of the world's most wealthy billionaires.

**Text 4**

**Famous Hackers**

questionable activities - сомнительная деятельность

usher [ˈʌʃə] – вводить

cumbersome [ˈkʌmbəsəm] – громоздкий

reap [riːp] – получить

juvenile [ˈdʒuːvənaɪl] – несовершеннолетний

intrusion [ɪnˈtruːʒən] – вторжение
a handle – дескриптор

violated parole [pəˈrəʊl] - нарушил правила условно-досрочного освобождения

notoriety [ˌnəʊtərˈaɪəti] – дурная слава
rumor [ˈruːmə] – слух, молва
corresponding company - соответствующая компания
to snoop around – совать свой нос в чужие дела

*Steve Jobs* and *Steve Wozniak*, founders of *Apple Computers*, were both hackers. Some of their early exploits even resembled the questionable activities of some malicious hackers. However, both Jobs and Wozniak outgrew their malicious behavior and began concentrating on creating computer hardware and software. Their efforts helped usher in the age of the personal computer - before Apple, computer systems remained the property of large corporations, too expensive and cumbersome for average consumers.

*Linus Torvalds*, creator of *Linux*, is another famous honest hacker. His *open source operating system* is very popular with other hackers. He has helped promote the concept of open source software, showing that when you open information up to everyone, you can reap amazing benefits.

*Richard Stallman*, also known as "rms," founded the *GNU Project*, a free operating system. He promotes the concept of free software and computer access. He works with organizations like the Free Software Foundation and opposes policies like Digital Rights Management.

On the other end of the spectrum are the *black hats* of the hacking world. At the age of 16, *Jonathan James* became the first juvenile hacker to get sent to prison. He committed computer intrusions on some very high-profile victims, including NASA and a Defense Threat Reduction Agency server. Online, Jonathan used the nickname (called a *handle*) "c0mrade." Originally sentenced to house arrest, James was sent to prison when he violated parole.

*Mitnick* gained notoriety in the 1980s as a hacker who allegedly broke into the North American Aerospace Defense Command (NORAD) when he was 17 years old. Mitnick's reputation seemed to grow with every retelling of his exploits, eventually leading to the rumor that Mitnick had made the FBI's Most Wanted list. In reality, Mitnick was arrested several times for hacking into secure systems, usually to gain access to powerful computer software.

*Kevin Poulsen*, or *Dark Dante*, specialized in hacking *phone systems*. He's famous for hacking the phones of a radio station called KIIS-FM. Poulsen's hack allowed only calls originating from his house to make it through to the station, allowing him to win in various radio contests. Since then, he has turned over a new leaf, and now he's famous for being a senior editor at “Wired” magazine.

*Adrian Lamo* hacked into computer systems using computers at libraries and Internet cafes. He would explore high-profile systems for security flaws, exploit the flaws to hack into the system, and then send a message to the corresponding company, letting them know about the security flaw. Unfortunately for Lamo, he was doing this on his own time rather than as a paid consultant - his activities were illegal. He also snooped around a lot, reading sensitive information and giving himself access to confidential material. He was caught after breaking into the computer system belonging to the New York Times.

It's likely that there are thousands of hackers active online today, but an accurate count is impossible. Many hackers don't really know what they are doing - they're just using dangerous tools they don't completely understand. Others know what they're doing so well that they can slip in and out of systems without anyone ever knowing.

*1 Read the text quickly and define who are their people: black hats or white hats.*

1 Steve Jobs
2 Steve Wozniak
3 Linus Torvalds
4 Richard Stallman
5 Jonathan James
6 Mitnick
7 Kevin Poulsen
8 Adrian Lamo

*2 Match people with their activities:*

| | |
|---|---|
| 1 Steve Jobs and Steve Wozniak | a) also known as "rms," founded the GNU Project, a free operating system. |
| 2 Linus Torvalds | b) hacked into computer systems using computers at libraries and Internet cafes. |
| 3 Richard Stallman | c) gained notoriety in the 1980s as a hacker who allegedly |

| | |
|---|---|
| | broke into the North American Aerospace Defense Command (NORAD) when he was 17 years old. |
| 4 Jonathan James | d) or Dark Dante, specialized in hacking phone systems. |
| 5 Mitnick | e) Some of their early exploits even resembled the questionable activities of some malicious hackers. |
| 6 Kevin Poulsen | f) became the first juvenile hacker to get sent to prison. |
| 7 Adrian Lamo | g) creator of Linux. |

*3 Who of the hackers*

a) would explore high-profile systems for security flaws, exploit the flaws to hack into the system, and then send a message to the corresponding company, letting them know about the security flaw?

b) outgrew their malicious behavior and began concentrating on creating computer hardware and software?

c) committed computer intrusions on some very high-profile victims, including NASA and a Defense Threat Reduction Agency server?

d) has helped promote the concept of open source software, showing that when you open information up to everyone, you can reap amazing benefits?

e) was arrested several times for hacking into secure systems, usually to gain access to powerful computer software?

f) works with organizations like the Free Software Foundation and opposes policies like Digital Rights Management?

g) is famous for hacking the phones of a radio station called KIIS-FM?

## Unit 3
## How it works
### Text 1

### How Trojan Work

enduring [ɪn'djʊərɪŋ] – давний
warrior ['wɒrɪə] – воин
to betray [bɪ'treɪ] – предать
to wreak havoc - нанести ущерб
Regardless of - независимо от того

One of the most enduring stories of the Trojan War, the most important conflict in Greek mythology, is the tale of the Trojan horse. Trying to find a way into the city of Troy, the great warrior Odysseus ordered his men to build a massive wooden horse, one big enough for several Greek soldiers to fit in. Once the structure was finished, he and several other warriors climbed inside, while the rest of the Greeks sailed away from Troy. One man named Sinon, however, stayed behind in order to deceive the Trojans, convincing them that his fellow Greeks had betrayed him and fled from the city. The wooden horse, he told the Trojans, was safe and would bring them luck.

After some discussion over the matter, the Trojans agreed to wheel the horse through their gates, unknowingly giving the Greek enemy access to the city. After proclaiming victory and partying all night, the citizens of Troy went to sleep - it was then that Odysseus and his men crept out of the Trojan horse and wreaked havoc on the city.

Although you've probably heard of the Trojan horse from Greek mythology, chances are you've also heard of Trojan horses in reference to computers. *Trojan horses* are common but dangerous programs that hide within other seemingly harmless programs. They work the same way the ancient Trojan horse did: Once they're installed, the program will infect other files throughout your system and potentially wreak havoc on your computer. They can even send important information from your computer over the Internet to the developer of the virus. The developer can then essentially control your computer, slowing your system's activity or causing your machine to crash.

Though they're not actually viruses, they're referred to as "Trojan horse viruses," "Trojan viruses," "Trojan horses" or just plain "Trojans." Regardless of what people call them, they all mean same thing. But what happened? How did you let this Trojan horse into your computer in the first place? And what can you do stop one from getting in?

So how do Trojan horses infect computers? Believe it or not, you have to do some of the work yourself. In order for a Trojan to infect your machine, you have to install the server side of the application. This is normally done by social engineering - the author of the Trojan horse has to convince you to download the application. Alternately, he or she might send the program to you in an e-mail message hoping you execute it. Again, this is why it is called a Trojan horse - you have to consciously or unconsciously run the .exe file to install the program - it doesn't propagate on its own like a virus. Once you execute the program, the Trojan server is installed and will start running automatically every time you power up your computer.

The most common way Trojan horses spread is through e-mail attachments. The developers of these applications typically use spamming techniques to send out hundreds or even thousands of e-mails to unsuspecting people; those who open the messages and download the attachment end up having their systems infected.

Sometimes, it's not even a person manually spreading malware - it's possible for your own computer to do so, if it's been infected already. *Crackers* - hackers who use their computer skills to create mischief or cause damage intentionally - can send out Trojans that turn innocent Web surfer's computers into *zombie computers*, so-called because the person with the infected computer rarely knows his system is under control. Crackers then use these zombie computers to send out more viruses, eventually creating networks of zombie computers known as *botnets*.

There are several things you can do to protect yourself from Trojan horses. The easiest thing to do is to never open any e-mails or download any attachments from unknown senders. Simply deleting these messages will take care of the situation. Installing antivirus software will also scan every file you download (even if it's from someone you know) and protect you from anything malicious. If you ever find your

computer has been infected with a Trojan, you should disconnect your Internet connection and remove the files in question with an antivirus program or by reinstalling your operating system. You can call your computer's manufacturer, your local computer store or a knowledgeable friend if you need help.

*1 Match the words and their definitions:*

| | |
|---|---|
| 1 warrior | a) to copy or move programs or information into a computer's memory, especially from the internet or a larger computer. |
| 2 to install | b)are hackers who use their computer skills to create mischief or cause damage intentionally. |
| 3 Trojan horse | c) so-called because the person with the infected computer rarely knows his system is under control. |
| 4attachment | d) produced and used to protect the main memory of a computer against infection by a virus. |
| 5 to download | e) a soldier, usually one who has both experience and skill in fighting, especially in the past. |
| 6 Crackers | f) a computer file that is sent together with an email message |
| 7 zombie computers | g) the software that tells the parts of a computer how to work together and what to do. |
| 8 antivirus software | h) a computer program that has been deliberately designed to destroy information, or allow someone to steal it. |
| 9 botnet | i) a group of computers that are by controlled by software containing harmful programs, without their users' knowledge. |
| 10 operating system | j) to put furniture, a machine, or a piece of equipment into position and make it ready to use. |

*2 Answer the questions:*

1)Which role did the Trojan horse play in the Trojan War?

2) What kind of program is the Trojan horse? How does it work?

3) How do Trojan horses infect computers?

4) Does the Trojan horse propagate on its own like a virus?

5) What is the most common way Trojan horses spread?

6) Who are crackers? How can they turn your computer into zombie computer?

7) What is botnet?

8) What is the easiest things you can do to protect yourself from Trojan horses?

9) What should you do if you ever find your computer has been infected with a Trojan?

*3 Translate into English:*

1) Троянский конь был построен воинами Одиссея чтобы проникнуть в город.

2) Программа «Троянских коней» скрывается в других программах, после установления которых вредоносная программа будет заражать другие файлы вашей системы и потенциально наносить ущерб вашему компьютеру.

3) Для того чтобы Trojan заразил ваш компьютер, необходимо установить серверную сторону приложения. Обычно это делается с помощью системы поиска - автор троянского коня должен убедить вас загрузить приложение.

4) Разработчики этих вредоносных приложений, как правило, используют методы рассылки спама, чтобы отправить сотни или даже тысячи электронных писем ничего подозревающим людям.

5) Взломщики могут отправить троянов, которые превращают веб-серфера в зомби-компьютеры.

6) Установка антивирусного программного обеспечения будет также сканировать каждый загруженный файл (даже если это от человека, которого вы знаете) и защитит вас от всех вредоносных программ.

**Text 2**

## How to Fix Your Zombie Computer

mortgage ['mɔː.gɪdʒ]- ипотека
trap [træp] – ловушка
become compromised – подвергаться опасности
zombie applications – зомби приложения
to convince [kən'vɪns] – убеждать

Your computer could be committing crimes right now. Even as you read this article, it could be working as part of a secret network of machines designed to bring down Web sites or flood e-mail boxes with ads for low mortgages. If the authorities link attacks back to your computer, you might take the fall even though you're not at fault.

Whether you call it a zombie computer army or a botnet, it's bad business - millions of computers have already fallen under the control of malicious hackers known as crackers. These crackers rely on several strategies aimed at getting you to download and execute a piece of malicious software, or malware. If you fall into the trap, your computer becomes compromised.

What can happen if your computer becomes a zombie? Zombie applications give crackers access to your machine, usually by exploiting security vulnerability or creating a backdoor entry point. Once a cracker establishes this link, he or she can manipulate your computer. Some botnet applications allow the cracker to control your computer remotely. Others give the cracker the ability to look at your private information and steal your identity.

One of the most common botnet applications is spam distribution. According to Symantec's MessageLabs, the Cutwail botnet alone was responsible for 6.5 percent of all spam messages in February 2009. That means the computers of innocent victims are sending out millions of e-mail messages to people around the world.

Another botnet application is the distributed denial of service (DDoS) attack. The cracker first creates a large botnet by convincing victims to execute malware. Then the cracker arranges an attack on a particular Web server at a specific time. When that time comes, the botnet computers simultaneously send messages to the

target Web server. The sudden rush of Internet traffic makes the Web server unstable and brings it down. The victims of these attacks are often high profile targets like CNN and Yahoo.

So what do you do if you discover your computer is part of a botnet?

*1 Answer the questions:*

1) What crime could your computer be committing right now?
2) What is the aim of crackers several strategies?
3) What can happen if your computer becomes a zombie?
4) What is one of the most common botnet applications?
5) What is another botnet application?

**2 Read the text and complete the gaps with missing words:**

| | | | | | |
|---|---|---|---|---|---|
| firewalls | software | backups | malware | applications | computer |

**Recovering from a Botnet Attack**

The most effective botnet applications disable antivirus and spyware detection software. If your _____ (1) slows down even when you're not using several applications at once, you might have a zombie problem. If you encounter error pages or denials when you try to visit sites that offer antivirus or spyware programs, that's a dead giveaway that something is wrong.

The best way to get rid of a botnet application is also the most painful: a complete system wipe and backup restoration. You do back up your hard drive, don't you? You should perform regular _____ (2) just in case you have any sort of catastrophic failure.

If you have personal firewall software, you might be able to detect the specific application on your computer that's giving someone remote access to your machine. _____ (3) act as filters between your computer and the Internet. Most firewalls have multiple security settings. First, set your firewall to the maximum security level -- this should require notifications for any application seeking access to the Internet. Then, reboot your computer.

Keep a close watch on network requests. Jot down the names of any _____ (4) that are unfamiliar to you, particularly if you haven't done anything to activate that application. Don't allow any application you don't recognize or trust to access the Internet. If you get repeated requests from the same application, that's a good indication that it's responsible for turning your computer into a zombie.

You may need to do some research on the Web regarding the application to see if other people have identified it as_____ (5). You'll need to find a list of all the files associated with that application and where you can expect to find them on your computer. Only by removing all of the offending files can you be sure your computer is free of the malware. In fact, you may have to go through the process several times to be certain you've cleared everything away -- one piece of malware often invites other applications and programs to join the party, too.

Of course, this method is a little risky -- you could accidentally remove a file that your computer relies on to function. It's often a better idea to just wipe the computer completely rather than assume you've caught all the offending _____ (6).

The best advice we can give is to avoid becoming a victim in the first place. Next, we'll look at ways you can protect yourself from joining a zombie computer army.

*Translate without dictionary:*

**More Is Not Always Better**

Resist the temptation to download multiple antivirus or anti-spyware applications. These applications are resource-intensive and can cause your computer to process other applications slowly. They can also interfere with each other and make your system less stable. It's better to settle on one version of each application and stick with it.

**Text 3**

**How Firewalls Work**

firewall – брандмауэр
requesting system - запрашивающая система
to discard [dɪ'skɑːd] – отбрасывать
small chunks of data - небольшие порции данных

A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through.

You can easily see how a firewall helps to protect computers inside a large company. Let's say that you work at a company with 500 employees. The company will therefore have hundreds of computers that all have network cards connecting them together. In addition, the company will have one or more connections to the Internet through something like T1 or T3 lines. Without a firewall in place, all of those hundreds of computers are directly accessible to anyone on the Internet. A person who knows what he or she is doing can probe those computers, try to make FTP connections to them, try to make telnet connections to them and so on. If one employee makes a mistake and leaves a security hole, hackers can get to the machine and exploit the hole.

With a firewall in place, the landscape is much different. A company will place a firewall at every connection to the Internet (for example, at every T1 line coming into the company). The firewall can implement security rules. For example, one of the security rules inside the company might be:

Out of the 500 computers inside this company, only one of them is permitted to receive public FTP traffic. Allow FTP connections only to that one computer and prevent them on all others.

A company can set up rules like this for FTP servers, Web servers, Telnet servers and so on. In addition, the company can control how employees connect to Web sites, whether files are allowed to leave the company over the network and so on. A firewall gives a company tremendous control over how people use the network.

Firewalls use one or more of *three methods* to control traffic flowing in and out of the network:

- *Packet filtering* - Packets (small chunks of data) are analyzed against a set of filters**.** Packets that make it through the filters are sent to the requesting system and all others are discarded.
- Proxy service - Information from the Internet is retrieved by the firewall and then sent to the requesting system and vice versa.
- *Stateful inspection* - A newer method that doesn't examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, and then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. Otherwise it is discarded.

*Answer the questions:*

1) What is firewall?
2) How does a firewall help to protect computers inside a large company?
3) Why will a company place a firewall at every connection to the Internet?
4) What rules can a company can set up?
5) What are three methods Firewalls use to control traffic flowing in and out of the network ?
6) What is the method of Packet filtering?
7) What is the method of Proxy service?
8) What is the method of Stateful inspection?

**Text 4**

## Firewall Configuration

customizable – настраиваемый
four "octets" in a "dotted decimal number" - 4 «восьмерки» в «десятичном точечном номере»
domain names - доменные имена
router- маршрутизатор
gateway – шлюз
broadband connections - широкополосное соединение

Firewalls are customizable. This means that you can add or remove filters based on several conditions. Some of these are:

*IP addresses* - Each machine on the Internet is assigned a unique address called an IP address. IP addresses are 32-bit numbers, normally expressed as four "octets" in

a "dotted decimal number." A typical IP address looks like this: 216.27.61.137. For example, if a certain IP address outside the company is reading too many files from a server, the firewall can block all traffic to or from that IP address.

*Domain names* - Because it is hard to remember the string of numbers that make up an IP address, and because IP addresses sometimes need to change, all servers on the Internet also have human-readable names, called *domain names*. For example, it is easier for most of us to remember www.howstuffworks.com than it is to remember 216.27.61.137. A company might block all access to certain domain names, or allow access only to specific domain names.

*Protocols* - The protocol is the pre-defined way that someone who wants to use a service talks with that service. The "someone" could be a person, but more often it is a computer program like a Web browser. Protocols are often text, and simply describe how the client and server will have their conversation. The *http* in the Web's protocol. Some *common protocols* that you can set firewall filters for include:

- *IP* (Internet Protocol) - the main delivery system for information over the Internet
- *TCP* (Transmission Control Protocol) - used to break apart and rebuild information that travels over the Internet
- *HTTP* (Hyper Text Transfer Protocol) - used for Web pages
- FTP (File Transfer Protocol) - used to download and upload files
- *UDP* (User Datagram Protocol) - used for information that requires no response, such as streaming audio and video
- *ICMP* (Internet Control Message Protocol) - used by a *router* to exchange the information with other routers
- *SMTP* (Simple Mail Transport Protocol) - used to send text-based information (e-mail)
- *SNMP* (Simple Network Management Protocol) - used to collect system information from a remote computer
- *Telnet* - used to perform commands on a remote computer

A company might set up only one or two machines to handle a specific protocol and ban that protocol on all other machines.

*Ports* - Any server machine makes its services available to the Internet using numbered ports, one for each service that is available on the server. For example, if a server machine is running a Web (HTTP) server and an FTP server, the Web server would typically be available on port 80, and the FTP server would be available on port 21. A company might block port 21 accesses on all machines but one inside the company.

*Specific words and phrases* - This can be anything. The firewall will sniff (search through) each packet of information for an exact match of the text listed in the filter.

Some *operating system***s** come with a firewall built in. Otherwise, a software firewall can be installed on the computer in your home that has an Internet connection. This computer is considered a *gateway* because it provides the only point of access between your home network and the Internet.

With *a hardware firewall*, the firewall unit itself is normally the gateway. A good example is the Linksys Cable/DSL router. It has a built-in Ethernet card and hub. Computers in your home network connect to the router, which in turn is connected to either a cable or DSL modem. You configure the router via a Web-based interface that you reach through the browser on your computer. You can then set any filters or additional information.

Hardware firewalls are incredibly secure and not very expensive. Home versions that include a router, firewall and Ethernet hub for broadband connections can be found for well under $100.

*1 Which protocol:*

a) is used to perform commands on a remote computer.

b) is used to break apart and rebuild information that travels over the Internet.

c) is used to download and upload files.

d) is used to send text-based information (e-mail).

e) is the main delivery system for information over the Internet.

f) is used for Web pages.

g) is used by a router to exchange the information with other routers.

h) is used to collect system information from a remote computer.

i) is used for information that requires no response, such as streaming audio and video.

*2 March the words and their definitions:*

| | |
|---|---|
| 1 IP addresses | a) is the pre-defined way that someone who wants to use a service talks with that service. |
| 2 Domain names | b) The firewall will sniff (search through) each packet of information for an exact match of the text listed in the filter. |
| 3 Protocols | c) are often text, and simply describe how the client and server will have their conversation. |
| 4 Ports | d)mean that a software firewall can be installed on the computer in your home that has an Internet connection. |
| 5 Specific words and phrases | e) are 32-bit unique numbers, normally expressed as four "octets" in a "dotted decimal number." |
| 6 operating systems with built in a firewall | f) has a built-in Ethernet card and hub. Computers in your home network connect to the router, which in turn is connected to either a cable or DSL modem. You configure the router via a Web-based interface that you reach through the browser on your computer. |
| 7 a hardware firewall | g) are human-readable names that all servers on the Internet also have |

**Text 5**

## Why Firewall Security?

There are many creative ways that unscrupulous people use to access or abuse unprotected computers:

*1) Remote login* - When someone is able to connect to your computer and control it in some form. This can range from being able to view or access your files to actually running programs on your computer.

*2) Application backdoors* - Some programs have special features that allow for remote access. Others contain bugs that provide a *backdoor* or hidden access that provides some level of control of the program.

*3) SMTP session hijacking* - SMTP is the most common method of sending e-mail over the Internet. By gaining access to a list of e-mail addresses, a person can send unsolicited junk e-mail (*spam*) to thousands of users. This is done quite often by redirecting the e-mail through the SMTP server of an unsuspecting host, making the actual sender of the spam difficult to trace.

*4) Operating system bugs* - Like applications, some operating systems have backdoors. Others provide remote access with insufficient security controls or have bugs that an experienced hacker can take advantage of.

*5) Denial of service* - You have probably heard this phrase used in news reports on the attacks on major Web sites. This type of attack is nearly impossible to counter. What happens is that the hacker sends a request to the server to connect to it. When the server responds with an acknowledgement and tries to establish a session, it cannot find the system that made the request. By inundating a server with these unanswerable session requests, a hacker causes the server to slow to a crawl or eventually crash.

*6) E-mail bombs* - An e-mail bomb is usually a personal attack. Someone sends you the same e-mail hundreds or thousands of times until your e-mail system cannot accept any more messages.

*7) Macros* - To simplify complicated procedures, many applications allow you to create a script of commands that the application can run. This script is known as a macro. Hackers have taken advantage of this to create their own macros that, depending on the application, can destroy your data or crash your computer.

*8) Viruses* - Probably the most well-known threat is computer viruses. A virus is a small program that can copy itself to other computers. This way it can spread quickly from one system to the next. Viruses range from harmless messages to erasing all of your data.

*9) Spam* - Typically harmless but always annoying, spam is the electronic equivalent of junk mail. Spam can be dangerous though. Quite often it contains links to Web sites. Be careful of clicking on these because you may accidentally accept a cookie that provides a backdoor to your computer.

*10) Redirect bombs* - Hackers can use ICMP to change (redirect) the path information takes by sending it to a different router. This is one of the ways that a denial of service attack is set up.

*11) Source routing* - In most cases, the path a packet travels over the Internet (or any other network) is determined by the routers along that path. But the source providing the packet can arbitrarily specify the route that the packet should travel. Hackers sometimes take advantage of this to make information appear to come from a trusted source or even from inside the network! Most firewall products disable source routing by default.

Some of the items in the list above are hard, if not impossible, to filter using a firewall. While some firewalls offer virus protection, it is worth the investment to install anti-virus software on each computer. And, even though it is annoying, some spam is going to get through your firewall as long as you accept e-mail.

The level of security you establish will determine how many of these threats can be stopped by your firewall. The highest level of security would be to simply block everything. Obviously that defeats the purpose of having an Internet connection. But a common rule of thumb is to block everything, and then begin to select what types of traffic you will allow. You can also restrict traffic that travels through the firewall so that only certain types of information, such as e-mail, can get through. This is a good rule for businesses that have an experienced network administrator that understands what the needs are and knows exactly what traffic to allow through. For most of us, it is probably better to work with the defaults provided by the firewall developer unless there is a specific reason to change it.

One of the best things about a firewall from a security standpoint is that it stops anyone on the outside from logging onto a computer in your private network. While this is a big deal for businesses, most home networks will probably not be threatened in this manner. Still, putting a firewall in place provides some peace of mind.

*1 Define the ways that unscrupulous people use to access or abuse unprotected computers:*

a) ____ Some programs have special features that allow for remote access. Others contain bugs that provide hidden access that provides some level of control of the program.

b) ____ is a small program that can copy itself to other computers. This way it can spread quickly from one system to the next. They range from harmless messages to erasing all of your data.

c) ____ In most cases, the path a packet travels over the Internet (or any other network) is determined by the routers along that path. But the source providing the packet can arbitrarily specify the route that the packet should travel.

d) ____ is usually a personal attack. Someone sends you the same e-mail hundreds or thousands of times until your e-mail system cannot accept any more messages.

e) ____ When someone is able to connect to your computer and control it in some form. This can range from being able to view or access your files to actually running programs on your computer.

f) ____ is the electronic equivalent of junk mail. It can be dangerous because of containing links to Web sites.

g) ____ is the most common method of sending e-mail over the Internet. By gaining access to a list of e-mail addresses, a person can send unsolicited junk e-mail (*spam*) to thousands of users.

h) ____ Hackers can use ICMP to change the path information takes by sending it to a different router.

i) ____ To simplify complicated procedures, many applications allow you to create a script of commands that the application can run.

j) ____ the hacker sends a request to the server to connect to it. When the server responds with an acknowledgement and tries to establish a session, it cannot find the system that made the request.

*2 Use the right form of the verb in brackets (remember that there are passive and active voices):*

The level of security you (to establish) (to determine) how many of these threats (to stop) by your firewall. The highest level of security (to be) to simply block everything. Obviously, that (to defeat) the purpose of (to have) an Internet connection. But a common rule of thumb is to block everything, then (to begin) (to select) what types of traffic you (to allow). Computers in your home network (to connect) to the router, which in turn (to connect) to either a cable or DSL modem.

Сводный план 2013г., поз. 227

Луара Дмитриевна Сергеева

# ПРОФЕССИОНАЛЬНО-ОРИЕНТИРОВАННЫЙ АНГЛИЙСКИЙ ЯЗЫК

Методические указания по чтению и переводу текстов
для студентов специальности 5В100200- Системы информационной безопасности

Редактор А.Т. Сластихина

Специалист по стандартизации Н.Қ. Молдабекова

Подписано в печать_____ Формат 60х84 1/16

Тираж 50 экз. Бумага типографская № 1

Объем 3,0 уч. – изд. л. Заказ__1500__. Цена тг.

*Копировально-множительное бюро*
Некоммерческого акционерного общества
«Алматинский университет энергетики и связи»
050013, Алматы, Байтурсынова, 126.