Тагирова Лиана Харисовна,
Тюменский государственный университет,
Институт математики и компьютерных наук,
студентка ИБ-156,
lianatagirova598@gmail.com

Сизова Людмила Владимировна,
Тюменский государственный университет,
Институт математики и компьютерных наук,
Кафедра иностранных языков и межкультурной профессиональной коммуникации естественнонаучных направлений,
старший преподаватель,
l.v.sizova@utmn.ru

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

Liana Kh. Tagirova,
the University of Tyumen,
Institute of Mathematics and Computer Science,
student of IS-156,
lianatagirova598@gmail.com

Lyudmila V. Sizova,
the University of Tyumen,
Department of Foreign Languages and Intercultural Professional Communication in Natural Sciences,
senior lecturer,
l.v.sizova@utmn.ru

Computer Crimes

Аннотация: В статье рассматривается одна из самых серьезных проблем 21 века. Преступления, связанные с денежными средствами, известны с давних времен, но сейчас они стали более изощренными с технической точки зрения. Данные преступления с использованием компьютера совершаются мошенниками, личности которых неизвестны. Очень быстро растет число покупателей, приобретающих товары через платежные системы в интернете. Они рискуют «открыть» свои данные киберпреступнику. В статье представлена информация о различных видах компьютерных преступлений, таких как хищение компьютерных данных, несанкционированный доступ к компьютерным системам с целью исказить или уничтожить информацию, использование компьютера для совершения противозаконной или мошеннической деятельности. Авторы статьи надеются, что читатели получат больше информации по данной проблеме и узнают, как не стать жертвой подобных преступлений.

Ключевые слова: компьютерные преступления, несанкционированный доступ, распределенная атака на отказ в обслуживании, атака методом «грубой силы», ботнет.

Abstract. The article considers one of the most serious problems of the 21-st century. Money related crimes has a long history but now they become more technologically creative. These crimes involving computers are nameless and faceless. The number of customers purchasing goods via the Internet through payment service providers is growing rapidly. They run the risk of "opening" own data to a cybercriminal. The article provides the information about different types of computer crimes such as the theft of computer data, unauthorized access to a computer system in order to damage or destruct the information, use of a computer to commit illegal or fraudulent activities. The authors of the article hope the readers can be better informed of the problem and how to prevent being a victim.

Key words: computer crimes, unauthorized intrusion, DDoS, brute force attack, botnet.

Crimes existed long before computers, but many forms of crime have involved computers since the twentieth century. At that time, the term “computer crime” was coined. It describes a criminal activity involving computers.

According to Donna Batten "computer crime is the use of a computer to take or alter data or to gain unlawful use of computers or services". With the increasing prevalence of the computer and other technological devices, the amount of computer crimes has skyrocketed. In 1987, a report by Ernst and Whinney found that approximately $3-5 billion was lost each year due to computer crime. The increased money loss can be attributed to the growing accessibility of the Internet, for Internet service providers were starting to develop large customer bases.

A few years later, the Computer Emergency and Response Team at Carnegie-Mellon university found that between 1991 and 1994, the percent of intrusions in the United States increased by a whopping 498%. They also found that the number of individual homes and office locations affected by computer cri mes went up by 702%.

To help combat the exploding amount of computer crimes, a new team was for med under the FBI- the National Computer Crime Squad. This team worked exclusively on cases involving computer crimes, and between 1991 and 1997, it investigated over two hundred individual cases.

As technology has no set form, there are many different avenues of attack that a victim can fall susceptible to. The types of attacks listed below are just a short sampling of existing threats.

Let’s have a look at Brute-Force Attack. This type of attack is typically used as an end-all method to crack a difficult password. A brute-force attack is executed when an attacker tries to use all possible combinations of letters, numbers, and symbols to enter a correct password. Any password can be cracked using the brute-force method, but it can take a very long time to finish. The longer and more intricate a password is, the longer it will take a computer to try all of the possible combinations.

The following recommendations will help you to do it if a password attack is possible:

1. Use a combination of letters, special characters and numbers for a password. It would be perfect if the password contains 16 characters. It will take over 200 years for an attacker to guess such a password.

2. Don’t save your password in web browsers.

3. Change your password from time to time. Do not enter usernames and passwords in public places where video is installed.

4. Don’t use the same password for different accounts.

5. If possible, use two-factor authentication to confirm your identity.

Now let’s consider another type of attack. A denial-of-service (DoS) attack is a special form of cyber attack that focuses on the interruption of a network service. This is achieved when an attacker sends high volumes of traffic or data through the target network until the network becomes overloaded. Think of a man juggling; he may be able to juggle quite well when using three or four balls, but if someone throws more balls into the fray and he tries to continue juggling with an increasing amount of balls, he may lose control and drop them all. This is what happens when a network becomes overloaded.

Typically, a DoS attack is carried out by one computer or one central location of computers. A popular sub-category of DoS attacks is distributed denial-of-service (DDoS) attacks. A DDoS attack varies from a regular DoS attack in which there are multiple computers involved. The computers all work together by means of the Internet to send traffic to the target network.

Another term commonly associated with DoS attacks is "botnet". A botnet is a group of computers that an attacker has taken control of for nefarious purposes. The true owner of a computer often does not even realize that his/her computer has been compromised. The compromised computers can be referred to as "bots" or "zombies" because they are under an influence other than their own. Using a botnet, an attacker has the computing power necessary to launch a DDoS attack, making it easier to overpower a target network.

DDOS attacks are often a consequence of personal grievances, political, religious and other differences, the provocative behavior of the victim.

But are there any ways to protect your computer from such attacks?

Today it is impossible to be fully protected from DDoS-attacks because absolutely secure systems do not exist. Besides, the human factor plays a big part because any mistake set up by a system administrator can lead to very disastrous consequences. However, despite all this, at this moment there are a lot of software and hardware protection means and organizational methods of confrontation. The following is a brief list of the main methods.

1. Software. There is modern software and hardware on the market. They are able to protect small and medium businesses from weak DDoS attacks. These funds usually represent a small server.

2. Reverse DDOS traffic used for the attack on the attacker. The attacked server allows you not only to repel the attack successfully but also damage the server of the attacker.

3. The use of equipment for DDoS attacks, for example, DefensePro® (Radware), SecureSphere® (Imperva), Perimeter (MFI Soft), Arbor Peakflow®, Riorey, Impletec iCore, and etc.

4. The acquisition of the service for protection against DDoS attacks will be helpful in case of exceeding flood the bandwidth of a network channel.

This is not a complete list of recommendations on protection against DDOS. The most important is that a user should keep a weather eye open.

It is necessary to emphasize the main points:

1. The users should know about new occurrences of attacks.

2. The users should know how to cope with these problems.

References:

1. Senft, S., Galecos, F. (2008). Information Technology Control and Audit. Third edition. Auerbach Publication, 804 pages.

2. Senft, S., Galecos, F. & Davis, A. (2012). Information Technology Control and Audit. Fourth edition. Auerbach Publications, 776 pages.

3. https://computercrimeinfo.com/

4. http://firdaus7387.blogspot.ru/2016/11/introduction.html

5. http://www.referenceforbusiness.com/small/Co-Di/Computer-Crimes.html

6.https://solmazp.wordpress.com/2010/08/01/some-recommendation-for-cybercrime-prevention-in-internet/