Computer crimes

Marcin Otorowski
Paulina Berdysz

Computer crime, cybercrime, e-crime, hi-tech crime or electronic crime generally refers to criminal activity where a computer or network is the tool, target, or place of a crime. Computer crime can broadly be defined as criminal activity involving the information technology infrastructure, including illegal access, illegal interception, data interference, systems interference or even misuse of devices. Today we will present you few kind of common computer crimes which are he most popular nowadays.

Computer crime?

Crimes

Salami shaving

We will start with a crime, that has very unusal name - Salami shaving. This is generally the process of draining small amounts of money from accounts. Actually, this issue is done by programmer, who changes instructions in program to drain very little amount of money to different account. The problem is, that user generally doesn't notice the loss of for example 5 gr, but if there are many transactions done, the total amount of stolen money is much higher.

The way to defend salami shaving is to check if the sums of payment are always correct.

DOS attack

In computer security, a denial-of-service attack (DoS attack) means trying to make a computer resource unavailable to its intended users. Typically the targets are high-profile web servers, and the attack's aim is to make the hosted web pages unavailable on the Internet. It is a computer crime that breaks the Internet proper use policy.

Attacks can be directed at any network device, including attacks on routing devices and Web, electronic mail, or Domain Name System servers.

A DoS attack can be perpetrated in a number of ways. There are three basic types of attack:
consumption of computational resources, such as bandwidth, disk space, or CPU time;
disruption of configuration information, such as routing information;
disruption of physical network components.

Trojan horses

The next kind of computer crime we will be talking about is a trojan. This name actually comes from Trojan Horse, which you should know from mythology. There are some confusions between trojan and viruses, but the distinction is rather simple – trojan appears to be an useful

program, but in the background it works in harmful way. There are two kinds of trojan horses – first is the case, when program was purposefully written to be malicious, and the second when it was corrupted by another application.

The results of running a trojan can be data loss, malware spreading, spying, installing a backdoor, doing some funny operations (like opening and closing CS all the time).. Preventing from trojan may be achieve by
leaving applications from unknown source unopened
installing firewall and antivirus
not using suspicious applications from e-mails and P2P

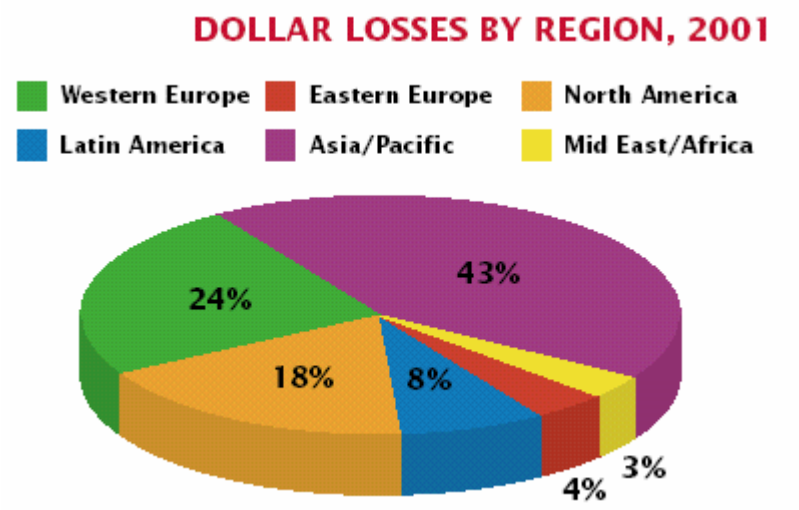
Trapdoors

In computing, a trapdoor is a hidden value or set of values that allows access to a program, computer system, or data. It is sometimes erroneously confused with a backdoor. It is a technique used in a computer crime that involves leaving within a completed program an illicit program that allows unauthorized – and unknown – entry.
Mail bombing

Next issue is mail-bombing. This is - in simple words - the process of sending huge volume of e-mails in coordinated way to specific receivers, so as to make Denial of Service. In Russia, mail bombing has been improved – sent e-mails have compressed text files attached, witch after compression are small, but unpacked can be bigger than 1 Megabyte. The problem is, that most of e-mail servers have built-in antivirus software, which scans attached files also. So, if there are thousands of files to check, and each of them has very big attachment, the probability of Denial of Service significantly grows up. The way of preventing includes using a good antivirus suite.

Software piracy

- Poland : 45th according to piracy level – 58 % of software in Poland is illegal
- Weighted average: 57.8%
- Vietnam – 92 %



The copyright violation of software refers to several practices when done without the permission of the copyright holder:

- Creating a copy and/or selling it. This is the act most people refer to as software piracy. This is copyright violation in most countries and is unlikely to be fair use or fair dealing if the work remains commercially available.

- Creating a copy and giving it to someone else. It is not infringing under specific circumstances such as fair use and fair dealing. In some countries, such as Israel, creating a copy is completely legal, as long as it was done for non-profit intentions.
- Creating a copy to serve as a backup. This is seen as a fundamental right of the software-buyer in some countries. It can be infringement, depending on the laws and the case law interpretations of those laws, currently undergoing changes in many countries.
- Renting the original software. Software licenses often try to restrict the usual right of a purchaser of a copyrighted work to let others borrow the work. In some jurisdictions the validity of such restrictions are disputed, but some require permission from the copyright holder to allow renting the software.
- Reselling the original software. Licenses often say that the buyer does not buy the software but instead pays for the right to use the software.

Piggybacking

Very interesting issue is piggybacking. It is basically using session established by another user, who didn't manage to log off. For instance, let's say that someone uses web interface of e-mail account, he didn't pressed log-off button and he did leave workstation. The next user is coming, he goes to the same web interface and notices, that he is logged in. This is exactly piggybacking. The way of preventing is very simple – always log off before leaving workstation.

A funny picture of computer crime

Spoofing

A computer crime that involves tricking a user into revealing confidential information such as an access code or a credit card number is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gains an illegitimate advantage. The best known kind of spoofing is "webpage spoofing," also known as phishing. In this attack, a legitimate web page such as a bank's site is changed into "look and feel" on another server under control of the attacker. The aim is to fool the users into thinking that they are connected to a trusted site, for example to harvest user names and passwords.

Defacing

Defacing is the process of changing information on another person's website, which of course requires technical and socio technical skills. Big companies with big websites are more affected by probability of being defaced. In 1997, hackers changed the website of Yahoo into slogan "Free Kevin" – and this was really harmful to Yahoo.

Hijacking

There are several kinds of hijacking such as credit card hijacking or IP hijacking. We will focus on Page hijacking which is a form of spamming the index of a search engine. It is achieved by creating a copy of a popular website which shows contents similar to the original one, but redirects web surfers to unrelated or unwanted websites. Spammers can use this technique to achieve high rankings in result pages for certain key words.

Summarise

As one of famous hackers once said – These are not systems that must be broken – the people are This is very actual according to the crimes we mentioned. They use some issues in security, but the weakest link is usually user as a part of system. Hope you will never have opportunity to be this weakest link. Thank you.

Sources

- http://en.wikipedia.org/wiki/Spoofing_attack
- http://en.wikipedia.org/wiki/Page_hijacking
- E.Glendinning, J.McEwan Information Technology, p.128 & 140, 2002 Oxford University Press