THE MAIN FORMS OF MANIFESTATION OF CYBERCRIMES

Irina Bakhaya, PhD
"Hyperion" University of Bucharest, i.bakhaya@gmail.com

Abstract: *Cybernetic offenses have long been outside legal regulation except for the Copyright and Related Rights Act no. 8/1996 , which criminalizes software piracy, regulating only a part of this dangerous manifestation, and Law no. 16/1995 on protection of topographies of integrated circuits . Law no. 21/1999, for the prevention and sanctioning of money laundering introduced for the first time in the Romanian legislation the notion of "cybercrimes". As any social phenomenon, cybercrime represents a system with its own properties and functions, distinct in terms of quality from those of the component elements.*

Key words: cybercrime, computer attacks

JEL Classification: J24

Regulatory framework

In Romania, an important legal regulation currently applicable in the area of cybercrime is Law 161 of 04.09.2003 on certain measures for ensuring transparency and the exercise of public dignities, public functions and the business environment, prevention and sanctioning of corruption .

This law introduces 8 offenses, corresponding to the classifications and definitions presented with the analysis of the provisions of the Convention on Cybercrime, which have been grouped within Title III of the law - Preventing and Combating Cybercrime. The text was a rapid adaptation to the Romanian environment of the provisions of the Council of Europe Convention on Cybercrime and is an effective tool in the fight against this scourge.

The same facts are also provided for in the New Penal Code, most of them in Title VII, Chapter VI, except for the offense of child pornography through computer systems.

Within Law no. 161/2003 there are three categories of offenses incriminated:

- Crimes against the confidentiality and integrity of data and computer systems.
    - The offense of illegal access to a computer system ;
    - The offense of illegal interception of a computer data transmission ;
    - The offense of altering the integrity of computer data ;
    - The offense of disrupting the functioning of information systems ;
    - The offense of carrying out illegal operations with devices or software .
- Computer crimes
    - Computer aided counterfeiting fraud ;
    - Computer fraud offense.
- Child pornography through computer systems

Illegal access to a computer system

Article 42 criminalizes the act of illegal access to a computer system in a standard version (paragraph l) and two aggravated variants (paragraphs 2 and 3):

- Access, without right, to a computer system;
- Access, without right, to a computer system, in order to obtain computer data;
- Access to an information system, under paragraph (1) if the act was committed in breach of security measures.

The offense charged in Art. 42 makes clear the distinction between the three stages of access to a computer system: simple access (which is often purely accidental), access to the obtaining of information data (which is manifested most often) and access by violating security measures (which require technical knowledge and is more difficult to carry out).

Password Attacks. Password breaking in the network

To understand how hackers work for password attacks on networks, we chose Windows NT and UNIX operating systems as an example.

To retrieve passwords from a Windows NT network, a hacker must have access to at least one username and the NT implementation of the MD4 algorithm.

After copying the database (the only place where user holes and MD4 hash can be found), the hacker will perform a force attack or a dictionary attack against the password file.

Because only system administrators can access the sam directory (where Windows NT locates the password database), the only way for the hacker to find the database is either the console or a backup copy of the database (located, for example, on a repair disk). In other words, to reach the database, the hacker must have physical access to the console or a copy of the database. If the server and server backups are physically secure, the risk of attack through the password database is significantly reduced.

Password Brute Force Attack on Windows NT

When attacking a Windows NT installation, the first step of the hacker is to try a low-level password. If the Windows NT Account Lockout feature is not enabled, the hacker can try passwords until it obtains a supported network password. The password-guessing process can be automated by using a program that guesses passwords permanently, known as brute force password-cracking technique. A program that performs such attacks is widely available on the Internet. The Force Attack program will try passwords like aa, ab, ac, etc., until it tries every possible combination of characters. Finally, the hacker will get the password.

However, a brute force attack against a Windows NT network requires either the hacker to have console access to the server, or to have a copy of the password database. In the event that the hacker can run the attack by force against a static Windows NT password database, there are available several free password breaking programsthat can guess 16 characters log passwords in seven days at most.

Dictionary password attack on Windows NT

Although a brute force attack requires long-term access to the Windows NT password file, a dictionary attack on a password file can be successful if the Account Lockout feature is not enabled. However, dictionary attacks can affect an off-line copy of that password file.

Generally, a Windows NT dictionary attack either passes the words in a dictionary through the Windows NT login prompt (if Account Lockup is inactive) either takes a list of dictionary words and

encrypts them one by one using the same encryption algorithm as NT to see if encryption results in the same one-way hash value (if the hacker has an off-line copy of the password database). If the hash values are equal, the password so identified will be the user's password.

The best solutions against dictionary attacks are: systematically changing passwords, running Kane Security Analyst on a regular basis or other system parsing application for password verification.

How do hackers break Unix passwords

To discover passwords from a Unix network, a hacker must have access to the network itself, or even be able to exploit a breach in a service (such as the sendmail bounce service) to reach the /etc/passwd file. Once it reaches the password file, the hacker also needs the 8-byte Unix one-way hash. After copying the password database, the hacker will run an attack - through brute force or dictionary - on the password file.

Since the /etc/passwd file is accessible to anyone on the Unix server, the hacker can reach the password database with minimal access rights to the server or even with no rights. Shadowing password shuffling or the use of superior password security programs is almost a necessity for Unix.

Unix brute force password attack

When a hacker attacks a Unix installation, the first step is to try a low-level password. Unlike Windows NT, Unix does not block user accounts after a certain number of lost login. Because Unix is tolerant, the hacker can use a brute force attack on a server without having access to the server at all. In the event the hacker can run and attack by force against a static password database in Unix, there are free password-breaking programs that can guess 16-character passwords in up to 10 days (depending on the connection speed). After obtaining the low-level password, the hacker will use that password to access the server and copy the /etc/passwd file.

After having a copy of the /etc/passwd file, the hacker can use a brute force attack to guess passwords until it finds an accepted network password. A hacker can automate the process of finding passwords using a program that performs this continuous operation.

The best way to protect against a brute force attack is to hide the password file so that the hacker can not access the passwords themselves, but only the tokens generated by the operating system. If the hacker is kept away from the hash values of passwords, he will not be able to run the brute force program because it will not be able to compare its own hash results with the values in the file.

Unix dictionary password attacking

If a raw force attack requires long-term access to the Unix password file, a dictionary attack may have more chances of success. However, dictionary attacks will also be successful on an off-line copy of the password file.

Generally, a dictionary attack on a Unix system either submits the words in a Unix login prompt dictionary (if the hacker attempts an online attack), or uses a wordlist and applies the hash function to each word using the same algorithm encryption as Unix does, to see if encryption reaches the same value of one-way hash (if the hacker has an off-line copy of the password database). If the values are equal, that word is the user's password.

The best protection against dictionary-based attacks is to cause users to regularly change their passwords, regularly run the Security Administrator Tool for Analyzing Networks (SATAN), or another password-analyzing system analysis program.

Free access attacks occur frequently in networks that use an operating system (including Unix, VMS or Windows NT) that incorporate free access mechanisms. These mechanisms are a particularly weak point of the systems. For example, for Unix operating systems, users can create trusted host files

that include hostnames (hosts) or where a user can access the system without a password. When connecting from such a system, the user just has to use the rlogin command or other similar command, with the appropriate arguments. Thus, a hacker can gain extensive control over the system by guessing the name of a free-access system or a host-username combination. And worse, most hackers know that many Unix system administrators configure ".rhosts" files in the root directory so that users can quickly move from one host to another using the privileges of the so-called superuser. Unix system administrators are starting to realize that using ".host" files can be a costly feature. These files allow a hacker to easily get unauthorized access to the root directory.

Attacks that exploit technological weaknesses include the free access attack discussed earlier, and many more. Each important operating system has its weak points. Some are easier to access than others. On the other hand, the probability that a hacker will detect such weaknesses is quite low. For example, a recent version of the Microsoft Internet Information Server product (Windows NT Auxiliary Product) contained an error with system destruction potential. The system would have given up if the hacker had inserted into his browser a unique URL with many digits when he would have accessed that site. The URL is very long and is unique to each system. The probability that hackers exploit this defect is very low. On the other hand, the likelihood that a hacker exploits the open-access host on a Unix system, due to the ease of access and existence of this file on multiple servers, is significantly greater than the probability of exploiting this program flaw.

Attacks that exploit shared libraries use shared libraries most commonly used in Unix. A shared library is a set of common program functions that the operating system loads into a RAM file at the request of each program. Hacker often replaces programs in shared libraries with new programs that serve their own purposes, such as permission for privileged access.

Attacks by TCP (Transport Control Protocol) hijacking

Perhaps the most dangerous threat to servers connected to the Internet is TCP hijacking. Although TCP prediction of frequency numbers and TCP hijacking have many common elements, the latter procedure is avoided because the hacker has access to the network by forcing it to accept its own IP address as a credible network address rather than by repeated attempts to test you have many IP addresses until you find the right one. The underlying idea behind TCP hijacking is that the hacker acquires control of a computer connected to the target network, then disconnects the computer from the network so that the server thinks the hacker has taken its real place.

Once the hacker successfully hijacks a credible computer, it will replace the IP address of the target computer within each packet with its own address and simulate the target sequence numbers. Security experts call this process "IP simulation". A hacker simulates a credible system address on his own computer using the IP simulation process. After the hacker simulates the target computer, this will use a smart sequence number simulation to become the target of the server.

A hacker can execute a TCP hijaching attack much more simply than an IP simulation attack. TCP hijacking also allows the hacker to ignore single-password test-response systems (for example, shared secret password systems) and compromise a host with more delicate security level.

Finally, TCP hijacking attacks are more dangerous than IP cancellation because hackers gain significantly higher access after a successful TCP hijacking than after a single IP simulation attack. Hackers desire more extensive access because this way they are able to intercepti ongoing transactions rather than simulating a computer and then starting transactions.

Session hijacking is a bit more popular than IP spoofing.

One reason for this is that it allows both importing and exporting data from the system. Also, session hijacking does not require the anticipation of the frequency numbers for the startup protocol, making it easier to perform, the framework of this rudimentary computer crime technique, the intruder finds an existing connection between two computers, usually a server and a client. Then, by penetrating unprotected routers or corresponding firewalls, the intruder detects important sequence numbers (TCP/IP addresses) as part of an information exchange between computers. After entering a legitimate

user's address, the intruder hijacks his session by invalidating the user's address numbers. After hijacking the session, the host computer disconnects the legitimate user and thus the intruder gets free access to the legitimate user's files.

The protection against session hijacking is very difficult, and the detection of such hijacking is difficult as well. For anti-hijacking protection, those regions of the system from where a hijacking attack may be launched must be secured. For example, unnecessary pre-defined accounts are removed and vulnerabilities are mitigated to protect firewalls and routers from unauthorized access. Also, the use of encryption is a valuable protection against hijacking. Detection of session hijacking is virtually impossible in the absence of a message from the hijacked user because the intruder appears in the system disguised as the user who has been hijacked.

Perhaps the most dangerous threat to servers connected to the Internet is TCP hijacking. Although the TCP prediction of frequency numbers and TCP hijacking have many common elements, the latter is safe because the hacker has access to the network by forcing it to accept its own IP address as a credible network address rather than by repeated attempts to test more IP addresses until finding the right one. The underlying idea behind TCP hijacking is that the hacker acquires control of a computer connected to the target network, then disconnects the computer from the network and tricks the server into thinking the hacker has taken the place of the real host.

An interesting type of illegal access, increasingly used today, is the social engineering attacks. These have become more common and more dangerous as more and more users connect to the Internet and internal networks. A common example of social engineering is that a hacker sends emails to users (or simply use the phone) to let them know that he is the system administrator. Often, messages require users to send their password by email to the administrator, because the system is in a flaw or will be temporarily disabled. A social engineering attack is mostly based on the ignorance of computer and network users. The best recipe against these attacks is the education of users.

Practice has shown that, in the vast majority of cases, the perpetrator acts to obtain computer data, which may mean:

- visual capture of these data on the monitor;
- entry into possession of an alphanumeric print (sheet of printed paper);
- running programs or applications that manage computer data (eg database management programs in an institution, e-mail programs, etc.).

By obtaining computer data it is understood including copying them to external storage media (Floppy Disk, CD, Memory Stick, Card etc.). If there is only a copy of the data, the deed will fall under the provisions of Article 42 paragraph 2. However, if the perpetrator transfers the data to an external medium (in the case of moving or migrating data to that storage medium), the provisions of Art. 44 of the law, which refers to the "alteration of the integrity of the information tiles" will apply. Simply copying computer data from a computer's hard disk or any other storage medium to an external media device is not likely to affect the integrity of that information in any way, but transferring them may also involve deleting them from the original location.

Generally, owners, owners, or lawyers choose to protect their IT systems by standard security measures.

Protection may be either physical (isolation of the computing technique in a secured enclosure, mechanical key or metal key, manual control of the power supply etc.) or logical (by passwords, access codes or encryption).

Under paragraph 3, the perpetrator will act on the computer system targeted by forcing these protections.

At the physical level, forcing involves the decommissioning of mechanical security devices through various mechano-chemical-electric means. At the logical level, we have password attacks.

Password attacks are, historically, one of the most preferred method hackers use for online networks. In the beginning, hackers tried to enter the networks by entering a login identifier and a password. They tried a password after another until they found the right one. However, hackers realized they had the ability to write simple programs to try out passwords in the system. In general, these simple programs were running in turn each word in the dictionary in an attempt to find a password. Thus, automatic password attacks have quickly become known as dictionary-based attacks. Unix operating systems are particularly vulnerable to dictionary attacks, because Unix does not automatically exclude the user after a certain number of attempts to enter the network, unlike other operating systems that inactivate a username after a fixed number of typing of incorrect passwords. In other words, a hacker can try thousands of times to connect to a Unix system without shutting down the connection or automatically alerting the system administrator.

Some hackers have even been successful in using Unix services like Telnet or FTP to get access to publicly accessible password files. The operating system encodes passwords in such files. However, since each Unix system encodes its password file using the same algorithm (a math function), a hacker can ignore the encoding of this file using an Internet-based algorithm. This algorithm is embedded in several "burst" tools, often used in the hacker community.

From a physical point of view, the consequence is the change that the incriminated action has produced in the foreign world. Sometimes this change may involve changing a situation or state, sometimes it can materialize in a material transformation to the material object of the offense.

In practice, the consequence of the simple form of demoted access is the transition to a state of uncertainty of the computer system and / or its resources (hardware, software, etc.).

If the purpose of unauthorized access was to obtain computer data, the state of uncertainty of the computing system is doubled by the state of uncertainty of the computer data stored there or processed by it.

Violation of security measures will, however, result in an effective transformation into the material object of the offense, the security measure being, in this case, an integral part of the information system.

From the legal point of view, in terms of the consequences that the incriminated action has on the social value that is the legal object, the consequence is precisely the state of danger, of threat, to "computer domicile" or "computer space".

Conclusion

Practically, at present, easy access to information and communication technology is one of the premises for the well functioning of modern society. Cyberspace is characterized by lack of borders, dynamism and anonymity, generating both opportunities for the development of the information society based on knowledge and risks to its functioning (at individual, state and even cross-border level).

The more information based a society is, the more vulnerable it becomes, and the security of cyberspace needs to be a major concern of all the actors involved, especially at the institutional level, where the responsibility for developing and applying coherent policies in the field is concentrated.

References

[1] Arădăvoaice Gh., Crăiniceanu I.,

[2] Niţă D. "Threats, vulnerabilities and risks", Antet Publishing House, Bucharest, 2004

[3] Bari Ioan "Contemporary Global Issues", Economic Publishing House, Bucharest, 2003

[4] Buş I. "Psychology and Crime. Theoretical Foundations ", ASCR Publishing House, Cluj-Napoca, 2005

[5] Gabriel T. Angheluş Cyber Terrorism, Terrorism Today Magazine, vol. I, July, 2006

[6] Marin Gheorghe "Effect-Based Operations - Concept and Response to the Risks and Threats of the Contemporary Security Environment", Military Sciences Magazine no. 2 (15), VIII, Bucharest, 2008