CYBER ATTACKS AGAINST FINANCIAL INSTITUTIONS

In recent years, due to the development of computer technology and the ever-increasing application of electronic information systems, we can see significant development and change regarding the criminal offenses as well. In addition to the bank robberies committed with weapons or weapon-looking objects, various IT crimes against banks, credit institutions and their clients have now appeared. These attacks often cause more material and moral damage than the illegal activities using physical violence against financial instructions.

As of today, the classic attacks are the so-called bank robberies and safe cracking, which are physical attacks committed mostly by armed robbers or by using weapons. The success of these attacks today can be doubtful since the perpetrator cannot be sure about the amount of money available in a given bank, how much of that money he can actually take, or how the physical security or the security guards are there, but the attack may also fail because of the audacity of the employees or customers.

We can generally say that the characteristic of physical violence is that it is directed against one bank, or rather branch, and it endangers the lives and the physical integrity of the employees and customers in that particular location.

From the tactical perspective of the investigation, however, we can say that in the case of traditional attacks, the perpetrators will more likely to leave behind a trace that could lead to their identification, while the same can be difficult in the case of IT-related incidents, and the lack of physical evidence can complicate the procedure and prolong the investigation.

The number of bank robberies is largely dependent on each country's negative economic changes, unemployment rate and in some cases, the proximity of major holidays, such as Christmas.

At the same time, cyber-attacks against banks may not only be for financial gain but as we will see going forward, simply to take revenge or seek attention not for profit but rather to show off their power or cause damages.

1. ATTACKS MADE USING INFORMATION TECHNOLOGY

Considering the above, we can generally say that the characteristics of „bank robberies" using information technology are completely different.

These crimes are committed by intellectual and/or white collar criminals. In many cases, they operate across the borders using only the virtual space to paralyze or falsify the websites of the banks or obtain the clients' money. Most of them are foreigners, including mainly Bulgarian, Russian and Romanian perpetrators. However, we should also note the instances when they acquire bank cards to make purchases or withdraw money from ATMs.

1.1 Cyber-attacks against banks and financial institutions can be classified in three different categories

The first of these groups includes the attacks directly against the banks. Within this category, we can identify two subcategories: the outside attacks against banks, and the incidental or deliberate infection of the system with a virus by the banks' own employees.

The external attacks against financial institutions are targeted at obtaining the bank customers' information, and paralyzing or making the financial institution's website inaccessible.

In many cases, criminal activities committed in a computing environment aim for financial gain. In the case of cyber-attacks against banks, this is exponentially true, though they are often complemented by a sort of vengeance as well.

The most common attacks affecting the bank's informational technology systems, are the DoS or DDoS attacks, but we can also mention website vandalism (defacement) here.

In general, we can say that the motivation behind cyber-attacks can be the following:

- the attacker wants to make a profit, they may want to sell the users' data to a third party,
- the attacker aims to destroy or weaken the perception or the reputation of the service provider and so causing damages since less people will trust this provider following the attack,
- the attacker may have good intentions and wants to draw attention to system flaws,
- the attack can be a simple display of power or for their own entertainment,
- attempt to find opportunities to crack the system.

1.1.1 Website defacement

Website defacement means the cracking or changing of a website so that the attacker gains access to the files in the web server's document root library. This access happens through deletion or alteration through which the attacker makes arbitrary changes or amendment to the home page. This is called defacement.

The attackers usually deface high-traffic websites that reach many people, so they can use it to send messages to others and voice their opinions.

1.1.2 Denial of Service (DoS) Attack

"As a result of an attack, the target refuses to provide the service. The attacker vandalizes the given website while voicing their real or perceived lesion. As a result of the attack, the system denies users access to various services for which they would be otherwise entitled. Therefore, it blocks the website's activity by seizing critically important resources."[1]

In conclusion, the DoS attack is any attack that overloads a website and as a consequence, it makes the content that is available under normal conditions inaccessible for the users.

[1] PATAKI M., KELEMEN R.: Terrorism 2.0 (Case studies) downloaded: http://blszk.sze.hu/images/Dokumentumok/diskurzus/2013/k/pataki-kelemen.pdf , November 24, 2015

“Distributed denial of service attacks (DDoS) are rate-based attacks which originate from a large number of computers, usually infected workstations. These so–called "zombie" workstations form a widely distributed attacking network, the "botnet". It is easier to be protected against DoS attacks if the mechanism causing the attack is known, therefore the proper analysis of the attack by malicious traffic is extremely important when the website is unable to perform normal functions."[2]

1.1.3 Man in the middle attack

“During the man-in-the-middle attacks, the attacker compromises the communication between systems, so that for example, during http data transfer the target will be the TCP connection between the client and the server. In this case, the attacker hijacks the communication channel and pretends to be a partner for both parties hence making the two users believe that they are communicating directly with each other, while they are actually in contact with the attacker. In some instances, we could see pages that transmit confidential information without the proper encryption.”[3]

1.1.4 Poorly written applications

In many cases the poorly written applications can not only be vexatious, for example making the battery of the computing device go flat very quickly or slowing down the system, but the attackers can take advantage of the applications’ faults and gain access to them and get them under their control. The characteristics of a poorly written application are the weak input filter, imbedded and stored passwords, and weak cryptographic algorithms.

SQL injection

The SQL injection attack is the insertion of SQL codes through which nefarious SQL statements are inserted into an entry field for execution.[4]
Such attacks exploit the vulnerability of data-driven applications, such as web applications. The SQL injection is an attack based on the query of databases, which can have serious implications, for example, leaking confidential information, breach of data integrity, overriding access rules or commencing a DOS attack.[5]

XSS-Cross site scripting

The XSS is a type of computer vulnerability where a malicious Internet user inserts a code on a website that is visible to others. When such a malicious attacker discovers a possible surface

[2] http://tech.cert-hungary.hu/sites/default/files/uploads/nhbk_vedekezes_a_dos_tamadasokkal_szemben.pdf (downloaded on November 24, 2015)
[3] https://hu.wikipedia.org/wiki/Közbeékelődéses_támadás (downloaded on November 2, 2015)
[4] https://en.wikipedia.org/wiki/SQL_injection
[5] Fleiner Rita: Attacks based on SQL injection and their defense opportunities (Hadmérnök, Season III, Issue 4, December 2008. Page 118.)

for XSS attack, they can execute the attack through bypassing the access controls. For example, when a financial institution's website found in the browser does not come from the original source, it only appears to be the same. We can distinguish two different. types. One large group is the persistent type. In this case, a partial code is written in the database and it gets loaded from there during the running. They can appear during the download of each page since this is a consistently present malicious code. The other one is the non-persistent type, which means that the code fragments will be executed through queries or other methods. Various data can be accessed taking advantage these opportunities. The data-phisher running the code will find a plethora of chances to access information stored in the cookies, access stored passwords or even gain administrator rights in a system with several hundred users, then they can conduct illegal activities and misuse the information obtained there.

1.1.5 Worm, virus, spyware an more

Computer viruses are programs that replicate by reproducing themselves in a document or a computer program. They are generally malicious and aim to destroy the infected data and make them inaccessible, or in some cases, they are written to give unauthorized access to data stored in IT systems.

Worms are similar to viruses in copying themselves from computer to computer, which they can even do automatically. Their goal is to gain control over some of the services of the computer that send files or data to another computer. One of the characteristics of a worm is its ability to spread on its own, which also means the ability to multiply itself. The worms can send themselves to all the email addresses stored in a particular email application’s address book, and then do the same on the recipient’s computer when the user opens the infected messages. Thereby they increase the network traffic and can slow down even a bank network and the Internet. If a new worm is unleashed, it spreads very quickly while overloading networks, so the user will have to wait twice as long to view the webpages.

1.1.6 Spyware

Spyware, like viruses and worms, threaten not only the banks IT networks and devices but also the personal information and passwords of the users, or more specifically and adhering more to the subject of my study, the customers using online banking services. The spyware is a software that collects the passwords and data stored on a computer without the knowledge or permission of the user.

In many cases, the financial institutions’ internal network gets infected because of the employees’ irresponsibility when they bring a virus from home through an external drive, or inadvertently open a website, thus completely stopping the system or allowing access to the data stored in the internal system. These web sites may be illegal or web pages with harmful content.

There have been instances where the employees deliberately infected the network for various reasons. It is possible that the workers themselves want to take revenge for being laid

off or for other real or presumed damage, or effect an order of someone else in order to establish or maintain a business relationship, or to return a favor. However, it can also happen that their intention is to draw attention to the potential weak points of the bank's IT system which ends up exceeding their capacity and the originator cannot fix the error.

2. ATTACKS AGAINST THE CUSTOMERS OF FINANCIAL INSTITUTIONS TO GAIN ACCESS TO THEIR INFORMATION OR MONEY

The attacks against the clients are in part through an IT system, such as e- mail, the Internet or by phone, while the rest happen through physical violence (credit card theft) or the duplication and data theft during the ATM or POS terminal cash withdrawal, or bankcard use.

2.1. „Nigerian scam - SCAM-419"[6]

Even today, the so-called Nigerian scams are still commonly used. They refer to a fraud through which the user will receive an email or a message through a social media site describing different stories to "borrow" money from the user, assuring them that they will certainly pay the money back. These frauds last over a relatively long period until they are able to scam the victims taking advantage of their goodwill and social sensitivity.

2.2. Spam or unsolicited mail

Spam, or unsolicited e-mails are messages that are sent out in large quantities with the same content to email addresses obtained from different sources to advertise games or websites that acquire the user's information after registration. Today, most email applications filter spam, but they can also be reported through the "NMHH" or biztonsagosinternet.hu websites.

2.3. Phishing

Phishing is one of the most common methods of gaining access to data, and it is also built on human trust. It is similar to spam. One of its types is when the customer's personal information and bankcard PIN or even their online banking login information are requested through email, telephone or text message. At the same time, there are more innocent-looking methods where they obtain the users' personal data by having them register to online quiz on social media sites, then they abuse this information.

3. COUNTERFEIT BANKCARDS

In recent years, the use of noncash payment options have surged, which has also led to the increased number of abuses associated with them. With reference to the title of this study, we will need to briefly mention the illegal activity related to the abuse of bank and credit cards, as a form of cyber-attacks and against banks.

[6] The SCAM 419 refers to the section of the Nigerian Criminal Code 419.§ which deals with the fraud, the charges and penalties.

The 2012 Act C-392.§ identifies three instances of the forgery of noncash payment instruments, all of which are be committed with intent of use:

- counterfeiting the noncash payment instrument,
- creating false noncash payment instruments,
- recording the data or the related security elements stored on noncash payment instruments with technical devices.

"We can bring up as an example the ATM abuses among others. Unfortunately, it still happens quite often that the criminals install a so-called skimmer on an ATM, which is a small data-recording device. But at the same time, they can also install miniature webcams, thermal cameras, fake keypads which can be printed even with a 3D printer. In addition, fake ATM openings or webcams facing the keypads are also common. The criminals' goal is to acquire the bankcard information of the careless bankcard users while they are using the ATMs. In many cases, the criminals are from Bulgaria, Romania, Serbia, Ukraine or possibly Russia."[7]

If they are successful in obtaining the client's information, they can make a clone card and misuse them.

There are also options where the illegal activity is committed through the recording radio frequency signals. They utilize this mostly with the nowadays popular Paypass payments. When using this payment method, it is enough to hold the card up to the POS terminal, and the two devices are communicating with each other through radio frequencies. The Paypass cards' data can be recorded with a new type of skimming device using radio frequency signals. The information stolen using this method is used to make purchases online, or they have pickpockets steal the Paypass-enabled cards.

"According to the methodological aid issued by the National Bank of Hungary, the following credit card abuses can be introduced the following way"[8]:

a. Cross-border: damage incurring during cross-border traffic, that is, damages related to the use of the service provider's cards while abroad.
b. Lost/stolen: damage caused by lost / stolen cards, i.e. abuses referring to damages or loss that is caused by cards that have been lost or stolen from the legitimate cardholder.
c. Card not received: abuse or loss caused by cards that the bank mailed to the cardholder but in which case the card did not arrive to its authorized owner, and an unauthorized person uses it for illegal transactions.
d. Fraudulent application: damage caused by a fraudulent card; this refers to the cases when the cardholder applies for a card using false information, receives the card from the bank, then uses this card to conduct unlawful transactions.
e. Counterfeit: damage caused by counterfeit cards. This includes all type of card counterfeiting, such as abuses using duplicate cards (skimming), the falsification of the personal data on actual bank cards.

[7] Dr. MEZEI, K., Dr. TÓTH D.: IT crimes (http://ujbtk.hu/dr-mezei-kitti%E2%80%85-dr-toth-david-informacios-buncselekmenyek/, downloaded on November 14, 2015)

[8] P34-methodology study aid -MNB, https://www.mnb.hu/letoltes/p34-modszertani-segedlet.doc (downloaded on November 13, 2015)

f. Card not present: damages caused via e-mail, telephone or Internet. This refers to the abuses that are done using the card's information (regardless of how it was obtained) by an unauthorized holder of the card when making purchases via telephone, mail or over the internet. As the name of the category indicates, the actual card is not physically present during these transactions.
g. Other: damage caused by other type of abuse. This category includes all the abuses that do not belong to any of the above categories. However, they do not contain the damages due to overdraft by the authorized cardholder or the abuses that are committed by the actual cardholder using his/her own card.
h. Card Skimming: the acquisition of card data. This means the unauthorized acquisition of any information (i.e., the data on the chip or magnetic stripe, PIN) necessary to use the bankcard at ATMs and POS terminals in order make counterfeit cards with this information and then perform unauthorized transactions.
i. Card Trapping: the plastic acquisition of the card. The physical card and its PIN are obtained through an ATM transaction, then it is used to withdraw cash illegally.
j. Transaction reversal fraud: In this case the cardholder manipulates the ATM's operation after a successful cash withdrawal transaction so that the machine considers it a failed transaction and cancels the transaction while part or all of the cash is disbursed.
k. Cash Trapping: the unauthorized acquisition of cash. During the ATM transaction, the cardholder does not receive the cash despite receiving the receipt confirming the withdrawal. Assuming the ATM's malfunctioning, the cardholder leaves, and the scammers get the money stuck in the machine which was previously manipulated by them.

LEGAL REGULATION

According to the C. Law of 2012, the facilitation of the counterfeiting of noncash payment instruments is considered a state of affairs on its own. The criminal offense means an early criminal protection because the preparation for forgery of noncash payment methods is already punishable, though the preparation without an intention cannot be established. This criminal offense can be established without intent.

In the case of the abuse of noncash payment instruments, the legislature intends to protect primarily those account holders who can access the money on their account using a noncash payment instrument, such as a credit or debit card.

"In the state of affairs, the perpetrator behaviors are the illegal acquisition, transfer, hold, import, export or cross-country transport of the materials, devices, computer data needed for the forgery of the noncash payment instruments, or the unauthorized acquisition of the security elements related to them."[9]

"The acquisition as an unlawful activity means a longer period of time, that is, it can only refer to the actual acquisition and retention of an object."[10]

Why are these attacks are harmful?

[9] C Act 2012, Penal Code, 393 § (1) points a) and b)
[10] BH 1985.373.

On one hand, the attacks' goal is to acquire money. This can be called the 21st century white (collar) bank robbery since nobody's life or physical integrity is in danger; at the same time, however, they do not only attack one bank at a time but the banks' servers, from which they can obtain the clients' personal information, their bank account and bank card details, the content of their account, and even the money kept in the financial institution. These attacks are more sophisticated, but in my opinion, are more dangerous, since the data obtained can be of significant value because in addition to the money stolen from customers and banks, this information can also be traded by the criminals.

REFERENCES:

- BELOVICS E, MOLNÁR G, SINKU P. (2013): *Criminal Law II.* (HVGorac, Budapest 2013.) Pages 702-711.
- Dr. NAGY, Z (2009): *Crimes committed in computing environment.* (Ad Librum, 2009.)
- Dr. MEZEI, K., Dr. TÓTH D.: *IT crimes (http://ujbtk.hu/dr-mezei-kitti%E2%80%85-dr-toth-david-informacios-buncselekmenyek/, downloaded on November 14, 2015)*
- PATAKI M., KELEMEN R.: Terrorism 2.0 (Case studies) downloaded: http://blszk.sze.hu/images/Dokumentumok/diskurzus/2013/k/pataki-kelemen.pdf , November 24, 2015
- P34-methodology study aid -MNB, https://www.mnb.hu/letoltes/p34-modszertani-segedlet.doc (downloaded on November 13, 2015)
- C Act 2012, Penal Code
- BH 1985.373.
- http://tech.cert-hungary.hu/sites/default/files/uploads/nhbk_vedekezes_a_dos_tamadasokkal_szemben.pdf (downloaded on November 24, 2015)
- https://hu.wikipedia.org/wiki/Közbeékelődéses_támadás (downloaded on November 2, 2015)
- https://en.wikipedia.org/wiki/SQL_injection