DOI: 10.55643/fcaptp.5.46.2022.3883

CYBER THREATS OF THE BANKING SECTOR IN THE CONDITIONS OF THE WAR IN UKRAINE

Lev Kloba
Candidate of Economic Sciences, Associate Professor of the Department of Finance, Accounting and Analysis, Institute of Entrepreneurship and Advanced Technologies, Lviv Polytechnic National University, Lviv, Ukraine;
ORCID: 0000-0003-0223-6802

Taras Kloba
PhD in Economics, Big Data Competence Manager, SoftServe Inc., Lviv, Ukraine;
e-mail: fkd@kloba.com
ORCID: 0000-0002-3354-3648
(Corresponding author)

ABSTRACT

The article aims to determine the features of cyber-attacks and cyber threats to the banking sector under martial law in Ukraine. The global trends of cyber-attacks on the financial industry are analyzed, and the active use of SMS messages and e-mails with links or malicious code inside, active DDOS attacks, and attacks on the bank's infrastructure by attackers and cyber fraudsters are revealed. The legislation of Ukraine on cyber threats (including against critical infrastructure, which provides for banking institutions), the main types of attacks on the banking sector (Deepfakes, Zero Trust, phishing, DDoS, brute force, IDOR, XSS vulnerability, SQL injection, malware installation) and the analysis of public information on the chronology of the main cyber-attacks on the banking system of Ukraine during the war were studied. The study focused on the methods and types of penetration. Based on the analysis, a list of features of cyber threats to banks and their customers in the context of military aggression was formed, namely: the adaptability of the banking sector to the latest cyber threats; strengthening the responsibility of banks to the regulator, including financial; remote work of banking specialists, which generates an increase in the risk of human factor; rapid update of malware; psychological orientation of cyber-attacks.

The ways to minimize cyber risks are identified, which include: the most rapid update of protective software systems, vulnerability scanning in the banking infrastructure, penetration tests, bug bounty programs, and the active use of elements of game theory as a generator of negative cyberattack scenarios.

Keywords: cyber threats, cybersecurity, banking sector, martial law conditions

JEL Classification: D62, D82, G21, G32, H56

INTRODUCTION

Cyber frauds are becoming increasingly sophisticated because banks must keep up with the latest cybersecurity technologies. Any social upheaval, such as earthquakes, war, or country default, is an incentive for intruders to become more active, and therefore, understanding the main methods of cyber fraud and the peculiarities of cyber-attacks in the context of military operations in Ukraine is highly relevant, as it allows to respond quickly to the most significant challenges for both banking institutions and, to some extent, for bank customers.

LITERATURE REVIEW

In current conditions, the issue of cyber-attacks is quite relevant. It is covered in numerous both general scientific and specialized scientific works, for example, the works Analysis of the consequences of cyber fraud in the banking system of Ukraine (Yarovenko & Boyadzhyan, 2018) or Cybersecurity as an essential component of the national security protection system of European countries (A. Voitsikhovsky, 2018), etc. The legal framework for information and cybersecurity is reflected in the publication of Novytskyi V. (2022). At the same time, since the article's publication, the National Bank has updated the legal framework for cybersecurity. The monograph of Bakalynskyi (2020) formulated recommendations for building an effective information security system, but, again, without considering global and Ukrainian trends of our time. This problem is typical for other scientists, including Trofymenko O. et al. (2019), since the preparation

Received: 01/10/2022
Accepted: 24/10/2022
Published: 31/10/2022

of the study requires a long time, during which many circumstances can change, especially in the field of banking cyber-security.

Information is also actively disseminated through the Internet by specialized units of Ukraine, for example, the Cyber Police Department of the National Police of Ukraine (Cyber-attacks and Internet Fraud, 2022) or the State Centre for Cyber Defense of the State Service for Special Communications and Information Protection of Ukraine (CERT-UA, 2022), etc.

At the same time, the cyber-attacks on the banking sector have not been systematically studied, and if it has been reviewed, it was in the context of the country's economy. For example, the brief of the European Parliament Russia's war on Ukraine: Timeline of cyber-attacks (2022) highlights only a few cyber-attacks, and the text has political specifics. On the other hand, The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict (2022) actively explores the war's impact and cyber fraudsters' activity in the context of national security. Moreover, the information is formed as of February 24, 2022.

Thus, the information is either not grouped, irrelevant, or does not reflect the peculiarities of cyber-attacks in the context of hostilities but is general information.

AIMS AND OBJECTIVES

The article aims to determine the features of cyber-attacks and cyber threats to the banking sector under martial law in Ukraine. To achieve this task, it is necessary to explore the typical types of cyber-attacks on both banking institutions and bank specialists and customers, identify the features of such cyber-attacks, and formulate proposals to minimize losses from cyber risks.

METHODS

To achieve this goal, the methods of analysis and synthesis were used to identify the features of cyber-attacks on the banking sector in the period from January to August 2022, as well as the method of historical analysis to identify trends and efficiency of updating malware that attacked the critical infrastructure of Ukraine (including banks and the National Bank of Ukraine).

RESULTS

It is worth considering that no banking institution in the banking sector of Ukraine is interested in disseminating information about the cyberattack it has suffered. The reason for such secrecy is primarily the threat of increased reputational risk since such information, even if the cyberattack is repelled, can lead to an outflow of customers who, thinking on the principle of "there is no smoke without fire", will withdraw deposits, reducing the bank's liquidity. Another factor in the reluctance of banks to disseminate such information is that such information will attract the attention of other attackers who, having experience and the necessary tools, can go through the installed patches and again carry out a successful cyberattack on the bank's infrastructure.

Considering current trends, the National Bank of Ukraine has formed a separate tool for collecting and exchanging information about information security incidents - MISP-NBU of the Cyber Defense Center. In essence, this is a specialized website of the National Bank, which is built based on the open source platform MISP and is designed to organize the access of banks to the system of collection, processing, storage, and exchange of information of general organizational and technical nature in real-time, taking into account confidentiality requirements (On Approval of the Regulation on the Organization of Cybersecurity in the Banking System of Ukraine and Amendments to the Regulation on the Definition of Critical Infrastructure Objects in the Banking System of Ukraine, 2022). Thus, the banking sector and the regulator know all information security incidents.

The regulator carefully approached the issue of forming an effective cybersecurity system. Thus, together with the adoption of the Law of Ukraine "On Critical Infrastructure" (On Critical Infrastructure, 2021), the Regulation on the Organization of Cybersecurity in the Banking System of Ukraine (On Approval of the Regulation on the Organization of Cybersecurity in the Banking System of Ukraine and Amendments to the Regulation on the Definition of Critical Infrastructure Objects in the Banking System of Ukraine, 2022) was approved, which described precise requirements for the internal cybersecurity system of Ukrainian banks, among other things:

DOI: 10.55643/fcaptp.5.46.2022.3883

- the basic principles of cybersecurity organization in the banking system of Ukraine are fixed;
- the principles of organization of information exchange between banks and the regulator are highlighted;
- measures to ensure cyber protection of critical information infrastructure of banks were identified;
- requirements for conducting an independent audit of information security in the banking system of Ukraine, etc.

It is also worth noting that the regulator has clearly defined the bank's punishment for inadequate cyber security. According to the current Regulation on the Application of Enforcement Measures by the National Bank of Ukraine, cyber risks are equated to the risks of financial monitoring and the fine for violation of the relevant requirements of the legislation (Article 7.33 of the Regulation on the Application of Enforcement Measures by the National Bank of Ukraine) (On Approval of the Regulation on the Application of Enforcement Measures by the National Bank of Ukraine, 2017) will be 0.01 percent of the amount of the registered authorized capital of the bank.

Using the current performance indicators of some of the largest banks, we show in Figure 1 the amount of fines that banks will incur in case of 1 (one) violation.

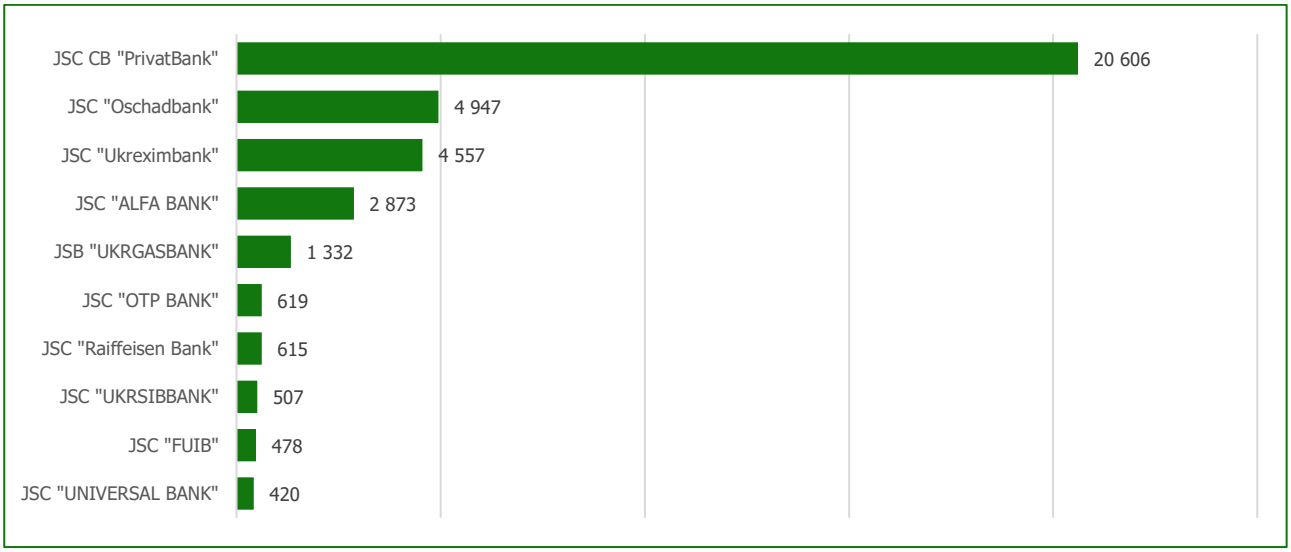

Figure 1. 0.01% of the authorized capital of the largest banks (authorized capital as of 01.08.2022), thousands UAH. (*Source: compiled by the author based on Supervisory Statistics, 2022)*

Thus, losses of banks because of violation of critical infrastructure security requirements and implementation of cyber threats against a particular bank due to the relevant shortcomings in its cyber resilience may manifest themselves in the loss of significant amounts of financial resources, which negatively affect banking activities, especially given the decline in economic activity of banks in the context of military operations in Ukraine.

Banks are obliged to monitor potential threats and risks in detail. At the same time, it is necessary to clearly distinguish the objects of such cyber-attacks. Thus, if we group the most typical cyber-attacks on the banking sector, we can identify the following things of attack:

- confidential or banking secrecy;
- banking infrastructure;
- customer and bank funds;
- websites of banks and regulators.

This list is not exhaustive but outlines attackers' primary areas of interest in cyber-attacks. Thus, banking/confidential secrecy allows fraudsters to influence customers in the bank in the future or sell confidential data to other interested parties. In addition, even a hint of compromising such data provokes increased panic among depositors.

The next target of cyber-attacks is the banking infrastructure. Successful attempts to access the Bank's infrastructure allow for gaining total control over the Bank's internal information systems, including payment, accounting, partially treasury, etc., which in turn provides for making unauthorized payments to fraudsters or third parties. In addition, having gained full or partial access (under certain conditions) to the banking infrastructure, attackers can blackmail the bank to make authorized payments in their favour.

Customer and bank funds in most cyberattacks are the final target and the main object. With the help of numerous tools, cybercriminals, having gained access to accounts, card numbers and CVV codes, SWIFT transaction numbers, and customer tokens, will be able to carry out the corresponding movement of funds in the direction of their accounts or accounts of third parties outside the jurisdiction of the Cyber Police Department of the Ministry of Internal Affairs of Ukraine.

Cyberattacks on the websites of banks and regulators are essentially psychologically destabilizing rather than financial. The vast majority of Ukrainian banks' websites do not have direct access to the bank's ABS, and, therefore, access to financial or banking secrecy. At the same time, web versions of online banking are more sensitive to attacks (brute force, XSS vulnerability, etc.)

Let us consider global trends in cybersecurity and protection against cyberattacks in terms of using the latest achievements in the field of IT. First of all, it is necessary to highlight the active use of serverless attack architecture and the use of cloud technologies (Clouds). Covid-19 and the subsequent transition of employees to work remotely have forced banking institutions to pay attention to the cybersecurity of SaaS solutions (remote workplaces). Their customers cannot protect data from attacks on their own - this should be the responsibility of specialists of enterprises and institutions, and they are not always good at it. The growth of attacks on microservices used by cloud service providers is predicted.

Deepfakes - they can be used to lull the vigilance of both living people and biometric access control systems. Such tools include masks popular in social networks and neural networks to build a visual copy of a client/bank specialist, etc.

Attacks on the supply chain cause an increase in the level of vulnerability of SCM systems, which are responsible for managing the flow of data and finances related to the bank's product or service.

ZeroTrust, as a default system protection model, evaluates each user or device requesting access to the system as unprotected and requiring re-authentication.

Growth of payments to cyber criminals. The $40 million received by hackers from CNA (Focus, 2022) for unlocking databases and system files suggests that records for data leakage and payments will be broken many times.

Let's consider the most common ways of cyberattacks in modern conditions and compare them with the chronology of attacks on the banking sector of Ukraine in 2022.

Let's start with phishing, the essence of which is the creation by fraudsters of an ordinary website or even a copy of a banking website from the outside, with the help of which they collect bank card numbers and CVV codes, passwords to online banking, account information, etc. under a standardized pretext. Phishing sites are diverse, but the main target of such sites are users of banking services - bank customers, namely their confidential information.

DDoS ((distributed) denial-of-service attack) is an attempt to disable a server with an avalanche of traffic. To do this, hackers combine virus-infected computers or devices into a botnet network and form such a volume of requests to the server that it is unable to process. No malicious code is introduced to the server - users simply cannot access the site because the server sorts the queue of fake requests. To protect against such attacks, the most important thing is the server architecture, which is configured for high loads from the moment of connection.

Brute force is an attack in which a malicious program tries to gain access to the system or its individual protected areas by sending different combinations of characters to the server, hoping to pick up the same "login-password" pair. Banks have learned to block most of these attacks through two-factor verification and the mandatory use of special characters in customer logins and passwords. At the same time, the most common brute force scheme in cyber-attacks are:

- obtaining (hacking of low-protected systems, purchase of customer databases with logins, not necessarily bank logins, in the Darknet),
- brute-force online banking with login/password pairs that are identical.

This method can compromise many accounts of the Bank's customers. It is easier for the user to leave the login/password already used by him in other systems, or login = password, as it speeds up both registration and login.

IDOR vulnerability (insecure direct object reference). Unprotected objects in the case of such an attack can be URLs of pages, files, and directories that can be accessed by any user. In the most absurd cases, it is enough for a cybercriminal to add /admin to the address and get the opportunity to behave as an administrator, that is, add their content, replace or delete, and correspond on behalf of users of the site. This problem is solved by setting user roles and restricting access rights by the current regulations of the National Bank of Ukraine.

XSS vulnerability (cross-site scripting). An attack that uses vulnerabilities to inject HTML tags or JavaScript code into a website page. It is often used on dynamic websites and occurs if the developers do not take care of filtering the data that

DOI: 10.55643/fcaptp.5.46.2022.3883

the user enters on the site. Thus, it is enough for an attacker, for example, to insert a script into the message window in a chatbot and publish it, and as soon as the system processes the text, the script will run, and the attack will begin.

XSS is divided into three types depending on where the code is stored: stored if it is stored on the server and executed automatically; displayed if it is contained in a link; and DOM-based if it is executed in the browser. As a result, a hacker can change pages on the site or insert scripts into the code that provide the transfer of confidential information to third parties.

SQL injection. Similarly - that is, through user input on the page - hackers can change the GET or POST request, as well as cookies, to gain access to the database.

Installing malicious code via viruses or hyperlinks in phishing emails addressed to customers or bank staff. The victim of such an email launches a chain of codes that either opens access to the bank's information system from the inside or installs the necessary software package to block the operation of the banking infrastructure. This is not an exhaustive list of the capabilities of Trojans or other viruses. Still, this threat is one of the most common, requiring only patience and minimal knowledge of human psychology.

Previously, purely information tools of cyber-attacks were described. In most cases, not only these tools are used, but also social engineering and the use of insiders.

Social engineering as a tool is more typical not for cyber fraudsters, but for typical telephone fraud. At the same time, being combined with cyber fraud significantly expands the potential negative impact of the latter. An example of such a situation can be the deliberate use of malicious software from within the banking infrastructure (by insiders).

So, having considered typical cyberattacks, let's move on to the largest cyberattacks on the banking sector and bank customers in January-August 2022 (Picture 2).

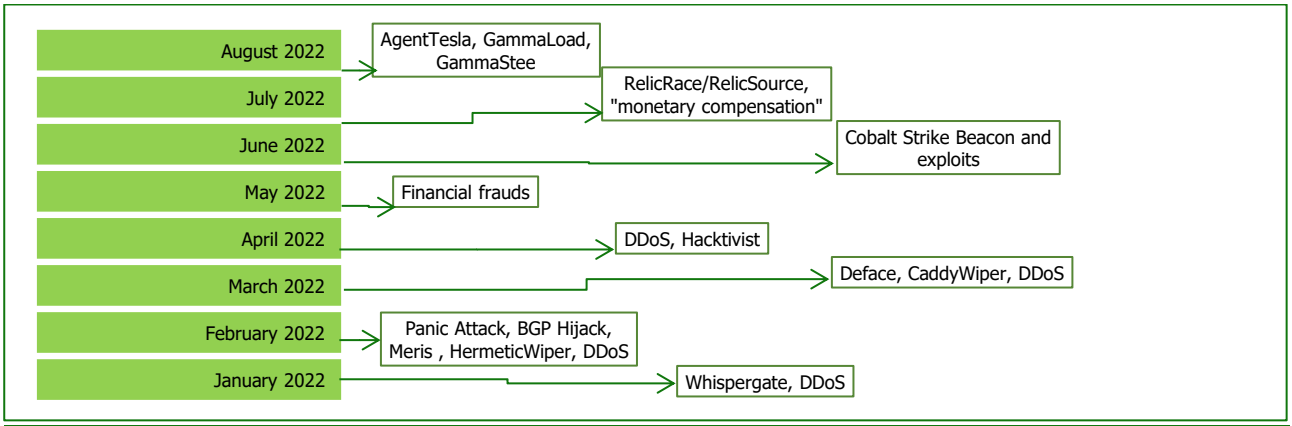

Figure 2. Chronology of cyber-attacks on the banking system of Ukraine in 2022. *(Source: compiled by the author based on (CERT-UA, 2022)*

Let`s consider in more detail the chronology of cyberattacks on the banking sector of Ukraine. We should start with the January events that preceded the invasion of Ukraine, as they raised the degree of distrust in the banking sector and specific banks.

Thus, in mid-January 2022, the websites of a few state organizations were interfered with, because of which, when visiting information resources, the user was displayed an image of provocative content. This included websites used by banks to check the credit history of customers.

An attempt of external hacker attacks by unknown persons from different countries on the information networks of the National Bank on January 14-15, 2022, is significant. However, the regulator's information systems operated normally, including the electronic payment system used by banks, the official website, and the NBU's internal computer network. The protection of the IT infrastructure was organized properly with the involvement of the NBU's Cybersecurity Center, other government agencies, banks, and financial institutions (The NBU's Information Systems Are Operating Normally, 2022).

In some cases, to disrupt the normal operation of automated systems at the final stage of the cyberattack, the attackers encrypt or delete data. For this purpose, at least two types of destructive malware were used, namely BootPatch (writing malicious code to the MBR of the hard drive-in order to modify it irreversibly) and WhisperKill (overwriting files with a

specific list of extensions with a sequence of 0xCC bytes of 1MB in length), or deleting data by manually removing virtual machines.

The most likely vector of the cyberattack is the compromise of the supply chain, which allowed to use of the existing trust to disable related information, telecommunications, and automated systems. At the same time, two more possible attack vectors are not excluded, namely the exploitation of OctoberCMS and Log4j vulnerabilities (Excerpt from Cyber Attack Research 14.01.2022, 2022).

Cyberattacks in February can be divided into five groups. Still, all of them were aimed at infrastructure elements, including banking institutions or contractors that ensured the effective operation of banks, to destabilize the situation in the country:

- Sending fake SMS messages to bank customers about violating the normal operation of ATMs of certain state financial institutions.
- Sending electronic mail messages among banking institutions about the mining of buildings and premises. According to the study results, it was determined that most of such letters were sent from the territories uncontrolled by the Ukrainian army.
- DDoS attacks on the web resources of Ukrainian banks, which, according to the results of the study, were organized by the Mirai and Meris botnets (360 Netlab On, 2022). Thus, the malicious information flow is directed through thousands of hacked Mikrotik routers and several other iOS devices. The above, with a high confidence level, suggests that the attacks used the available capacities of attackers provided as a service (DDoS as a Service), and the number of devices was about 30,000 machines.
- Preventing access to web resources in the gov.ua zone by performing a DDoS attack on DNS servers. The failure of several domain name servers led to temporary disruption of access to a significant number of web resources of state bodies due to the inability to determine the A-record (IP address) for the corresponding domain names. (DDOS Attack on gov.ua, 2022).
- Fraudulent manipulation of autonomous systems settings at the BGP protocol level. Thus, according to Cisco Cross-work (Cisco events, 2022), for more than two hours, starting from 15:30 on 15.02.2022, the prefix 217.117.7.0/24, which belongs to Inq-Digital-Nigeria-AS (AS16284), was announced on behalf of the autonomous system of Privat-bank (AS15742) through the autonomous system of the Nigerian telecommunications operator AS37148 (Information on Cyberattacks on February 15, 2022, 2022).

Among the March incidents, it is worth noting the detection by anti-virus software of CaddyWiper, malicious software that blocks the operation of a personal computer, which is downloaded from a link in a phishing email. CaddyWiper was intended, like the Petya virus, to infect all computers on the network (Editor, 2022).

DDoS attacks did not stop in April, as the specialists of the National Bank of Ukraine (CSIRT-NBU, as mentioned earlier) detected and investigated DDoS attacks, for the implementation of which cybercriminals placed malicious JavaScript code (BrownFlood) in the structure of web pages and files of compromised websites (mainly under the control of WordPress) (Research of DDOS Attacks, Brownflood Malicious JavaScript Code DDOS Attacks, 2022), as a result of which the computing resources of the computers of visitors to such websites are used to generate an abnormal number of requests to attack targets whose URLs are statically defined in the malicious JavaScript code.

In other words, site visitors formed a new botnet, which the attackers used to attack, including banking institutions.

The incident with the spread of malware on behalf of the Governmental Computer Emergency Response Team of Ukraine looks interesting for further research. Thus, in May, emails with the subject "Cyberattack" were actively sent on behalf of CERT-UA with an attachment in the form of a password-protected RAR-archive "UkrScanner.rar". During the investigation of the incident, it was found that the archive contains a file in SFX format, which in turn contains the CredoMap_v2 malware. Using HTTP POST requests, the stolen authentication data is sent to a web resource deployed on the Pipedream platform. According to cyber experts, this activity was initiated by the APT28 criminal group (APT28 Cyberattack with Credomap_v2 Malware, 2022).

Also, since May, phishing messages have been actively sent in social networks and phishing emails, for example:

- Urgent verification of cards for payments to each person from 9800 UAH.
- Get a VAT refund from the ECC PPC (Online Fraud with the Use of the Theme of "Monetary Compensation", 2022).
- Promotion from Privatbank: money for the survey.
- Cash assistance under the UN social program (Online fraud with the use of the theme "Cash assistance under the UN social program", 2022), etc.

DOI: 10.55643/fcaptp.5.46.2022.3883

In June, a mass mailing of emails with the subject "changes in salary with accruals.docx" was detected, which was distributed among Ukrainian organizations, including Ukrainian banks. It was found that the document contains a link to an external object (HTML file containing JavaScript code), the execution of which, after the exploitation of vulnerabilities CVE-2021-40444 and CVE-2022-30190, will lead to the launch of a PowerShell command, downloading the EXE file "ms-msdt.exe" file and infecting the computer with Cobalt Strike Beacon malware (Cyberattack on State Organizations of Ukraine with the Use of Cobalt Strike Beacon Malware and Exploits for Vulnerabilities CVE-2021-40444 and CVE-2022-30190, 2022)].

If we consider the above incidents, in our opinion, it is worth noting that the files are named in such a way that the victim is most interested in opening the file, and activating the hyperlink.

In July, the "Tax Service of Ukraine" allegedly sent out a malicious document "Imposition of penalties.docx", when opened, it would download an HTML file and execute a malicious JavaScript code (CVE-2022-30190), which, in turn, would ensure the download and launch of the Cobalt Strike Beacon malware (compilation date: 16.06.2022 - and therefore, it is the most updated software) (Cyberattack of the UAC-0098 Group on Critical Infrastructure Objects of Ukraine, 2022).

August is characterized by the continuation of the general trends of cyber frauds via email (from compromised accounts and to private email addresses) of HTML droppers (including UTF-16 encoding) that initiate the GammaLoad.PS1 delivery chain to the victim's computer.

The attackers' goal is to steal files with a specific list of extensions, as well as browser authentication data, for which GammaSteel.PS1 and GammaSteel.NET are used, respectively. GammaSteel.PS1 is probably a PowerShell implementation of the previously used HarvesterX.

In addition, one of the attackers' tactics is to infect a Microsoft-embedded template file with a macro whose code generates URLs and adds it to the document being created as a link (the so-called "Remote template injection") ((Cyberattacks of Group UAC-0010 (Armageddon): GammaLoad, GammaSteel, 2022). These script actions lead to the infection of all documents created on a particular computer and their further distribution by the user.

Summing up, let us note the main features of cyber threats and cyber-attacks on the Ukrainian banking system during January - August 2022:

- Characteristic features of cyber threats do not differ significantly from global trends, phishing emails, DDoS attacks still remain essential tools of criminals.
- The banking sector is actively adapting to new challenges in the cyber sphere, where, along with new regulations governing cybersecurity, the Regulation on the use of cloud services by banks under martial law in Ukraine was approved, which resulted in the transfer of part of the bank's functionality to the cloud, and therefore diversification of risks.
- The NBU has significantly increased the liability of banks for violations of cybersecurity requirements.
- A significant number of banking specialists, working remotely (as a result of COVID-19), are exposed to significant risks due to the possibility of infection of personal computers, especially those that are their personal property, as they receive not only corporate but also personal mail, can open malware and affect the banking network.
- Malware develops as quickly as possible and is used as soon as possible after compilation, which allows it to pass some (or all) filters of cybersecurity systems.
- The human factor is the greatest threat in terms of cybersecurity, as technical means are being improved as much as possible, and unauthorized actions of personnel will occur as long as the bank's personnel are involved in its activities.
- Some cyber-attacks have a psychological orientation - to make Ukrainians panic and take rash steps that could potentially lead to the loss of all funds from their accounts. Also, DDOS attacks can provoke the population to actively withdraw funds from the banking sector, which will reduce liquidity and lead to a slowdown in the development of the country's economy as a whole

In general, cybersecurity policies should become more flexible, but no less secure, for example, key management (password and certificate lifecycle), remote access, use of cloud systems, etc.

DISCUSSION

The main feature of cyber-attacks is the psychological nature and focus on the implementation of the so-called human factor. Technically, banks are able to defend themselves and respond quickly to cyber threats, while at the same time a bank specialist can open access to the internal perimeter of the bank to attackers with one click.

The discussion points in this article are the allocation of specific cyberattacks against the background of the general spectrum of cyberattacks on the banking sector of Ukraine. Thus, there are almost no technical features of such cyberattacks, as well as losses of banks and the banking sector in general from cyber criminals. At the same time, the peculiarities of cyber threats may change radically, as the identification of new vulnerabilities of bank software systems, the search for new intrusion tools, etc. reveal new opportunities for cyber fraudsters to manipulate information.

CONCLUSIONS

In general, numerous attempts of cyberattacks on the banking sector were recorded during the period under review. Banks officially successfully repelled such attacks (unsuccessful attempts will not be widely covered due to the need to reduce reputational threats). The main features of cyber-attacks on the banking sector are numerous DDOS attacks, active use of phishing emails and malicious blocker codes. Summarizing the above, we will form a list of measures to minimize/avoid cyber-attacks and cyber threats to the banking sector:

- Prompt updating of software versions to the current ones, which will allow closing the identified software and cybersecurity vulnerabilities as soon as possible.
- Conducting penetration testing, which will identify problems of cooperation of software systems of banks, bottlenecks and ensure high efficiency of response to unexpected cyber-attacks.
- Vulnerability scanning of both existing bank systems and its infrastructure, as well as IT service projects that are under development to form the necessary list of improvements.
- Bug bounty for the detected vulnerabilities, which will allow to quickly identify the vulnerabilities of the bank's IT services not by fraudsters and make appropriate adjustments to the code.
- The use of game theory methods, since in modern conditions one-step scripts are rarely used, usually using 2 or more step tools for hacking banking services and infrastructure, and therefore game theory will allow you to consider the IT service from the maximum number of scenarios.

At the same time, these measures may not be enough, as cybercriminals are actively improving the malicious code, as well as actively using additional tools to expand the possibilities of penetrating the internal information infrastructure of the bank.

REFERENCES

1. *360 Netlab on.* (2022, February 16). Twitter. Retrieved September 23, 2022, from https://twitter.com/360Netlab/status/1493797519725367302
2. CERT-UA. (2022, April 28). cert.gov.ua. Research of DDoS attacks that are carried out as a result of the defeat of websites using the malicious JavaScript code BrownFlood. Retrieved September 23, 2022, from https://cert.gov.ua/article/39923
3. CERT-UA. (2022, August 10). cert.gov.ua. *UAC-0010 (Armageddon) group cyberattacks: GammaLoad, GammaSteel malware. Retrieved September* 23, 2022, from https://cert.gov.ua/article/1229152
4. CERT-UA. (2022, February 18). cert.gov.ua. *Information about cyber-attacks on February 15, 2022* Retrieved September 23, 2022, from https://cert.gov.ua/article/37139
5. CERT-UA. (2022, January 26). *Fragment of the study of cyber-attacks on 14.01.2022*. Retrieved September 23, 2022, from https://cert.gov.ua/article/18101
6. CERT-UA. (2022, July 14). cert.gov.ua. Online fraud with the use of "monetary compensation" theme Retrieved September 23, 2022, from https://cert.gov.ua/article/761668
7. CERT-UA. (2022, June 2). cert.gov.ua. Cyberattack on Ukrainian state organizations using Cobalt Strike Beacon malware and vulnerability exploits *CVE-2021-40444 і CVE-2022-30190*. Retrieved September 23, 2022, from https://cert.gov.ua/article/40559

DOI: 10.55643/fcaptp.5.46.2022.3883

8. CERT-UA. (2022, June 20). cert.gov.ua. *Cyberattack of UAC-0098 group on critical infrastructure facilities of Ukraine.* Retrieved September 23, 2022, from https://cert.gov.ua/article/339662
9. CERT-UA. (2022, May 14). cert.gov.ua. *Online fraud using the theme of "financial assistance under the social program OOH* Retrieved September 23, 2022, from https://cert.gov.ua/article/40263
10. CERT-UA. (2022, May 60). cert.gov.ua. *Cyberattack of APT28 group with the use of malicious program CredoMap_v2.* Retrieved September 23, 2022, from https://cert.gov.ua/article/40102
11. *CERT-UA.* (2022, September 20). cert.gov.ua. Retrieved September 23, 2022, from https://cert.gov.ua/
12. *Cisco events* (2022). Retrieved September 23, 2022, from https://cert.gov.ua/
13. *DDOS attack on gov.ua.* (2022, February). Hostmaster. Retrieved September 23, 2022, from https://www.hostmaster.ua/news/?pr20220216
14. Editor. (2022, April 13). *CaddyWiper: New wiper malware discovered in Ukraine.* WeLiveSecurity. Retrieved September 23, 2022, from https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/
15. European Parliament. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks*. europarl.europa.eu. Retrieved September 23, 2022, from https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf
16. *The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict*. (2022, February 24). Harvard Business Review. Retrieved September 23, 2022, from https://hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict
17. Bakalynskyi, O. (2022). Model and methods for determining the design characteristics of information security management systems. Retrieved September 23, 2022, from https://www.researchgate.net/publication/348788054_Model_ta_metodi_viznacenna_proektnih_harakteristik_sistem_upravlinna_informacijnou_bezpekou_Monografia
18. Voytsikhovskyi, A. (2018, January 1). Cyber security as an important component of the national security protection system of European countries. Retrieved September 23, 2022, from https://www.academia.edu/39795468/+
19. *Information systems of the National Bank are working as usual. (2022, January 14). Official website of the National Bank of Ukraine*. Retrieved September 23, 2022, from https://bank.gov.ua/ua/news/all/informatsiyni-sistemi-natsionalnogo-banku-pratsyuyut-u-shtatnomu-rejimi
20. *Cyber-attacks and Internet Fraud (2022). Cyber Police Department of the National Police of Ukraine.* Retrieved September 23, 2022, from https://cdn-cms.fstatic.com/uploads/848224/normal_5c608a5a0a090.pdf
21. *Supervisory statistics. (2022, September 20). National Bank of Ukraine*. Retrieved September 23, 2022, from https://bank.gov.ua/ua/statistic/supervision-statist#4
22. Novytskyi, V. (2022). Strategic principles of ensuring information security in modern conditions. Information and law, (1(40), 111–118. Retrieved September 23, 2022, from http://il.ippi.org.ua/article/view/254349. DOI:10.37750/2616-6798.2022.1(40).254349
23. *On the approval of the Regulation on the use of influence measures by the National Bank of Ukraine. (2012, July 17). Official web portal of the Parliament of Ukraine.* Retrieved September 23, 2022, from https://zakon.rada.gov.ua/laws/show/z1590-12#n16
24. *On the approval of the Regulation on the organization of cyber protection in the banking system of Ukraine and amendments to the Regulation on the identification of critical infrastructure objects in the banking system of Ukraine. (2022, July 12). Official web portal of the Parliament of Ukraine.* Retrieved September 23, 2022, from https://zakon.rada.gov.ua/laws/show/v0178500-22#Text
25. *About critical infrastructure. (2021, November 16). Official web portal of the Parliament of Ukraine.* Retrieved September 23, 2022, from https://zakon.rada.gov.ua/laws/show/1882-20#n467
26. Trofymenko, O., Prokop, Y., Loginova, N., & Zadereyko, O. (2022, September 23). Cybersecurity of Ukraine: analysis of the current state. Information Protection, Vol. 21, 3. Retrieved September 23, 2022, from http://dspace.onua.edu.ua/bitstream/handle/11300/12213/statya_Trofymenko_Prokop_Loginova_Zadereyko_CYBERSECURITY%20OF%20UKRAINE.pdf?sequence=1&isAllowed=y. DOI: 10.18372/24107840/21/13951

27. Fokus, R. (2022, September 23). Hackers hacked the largest US insurance company and received a $40 million ransom. FOCUS. Retrieved September 22, 2022, from https://focus.ua/uk/technologies/483266-hakery-vzlomali-krupneyshuyu-strahovuyu-kompaniyu-ssha-i-poluchili-40-mln-vykupa

28. Yarovenko, A. M., & Boyajian, M. M. (2018, July 18). Analysis of the consequences of cyber fraud in the banking system of Ukraine. http://economyandsociety.in.ua/journals/18_ukr/116.pdf

Кльоба Л., Кльоба Т.

КІБЕРЗАГРОЗИ БАНКІВСЬКОГО СЕКТОРА В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

Метою статті є визначення особливостей кібератак та кіберзагроз банківського сектора в умовах воєнного стану в Україні. Проаналізовано загальносвітові тенденції кібератак на фінансовий сектор та виявлено активне використання SMS-повідомлень та електронних поштових повідомлень із посиланнями чи шкідливим кодом усередині, активні DDOS-атаки, атаки на інфраструктуру банків. Досліджено законодавство України щодо кіберзагроз , висвітлено основні типи атак на банківський сектор (Deepfakes, ZeroTrust, фішинг, DDOS, брутфорс, IDOR, XSS-уразливість, SQL-ін'єкція, установлення зловмисного програмного забезпечення) та проведено аналіз публічної інформації щодо хронології основних кібератак на банківську систему України в умовах війни. На основі проведеного аналізу сформовано перелік особливостей кіберзагроз для банків та їхніх клієнтів в умовах воєнної агресії, а саме: адаптивність банківського сектора до новітніх кіберзагроз; посилення відповідальності банків, у тому числі й фінансової, перед регулятором; віддалена робота банківських фахівців, що породжує зростання ризиків людського фактора; швидке оновлення шкідливого програмного забезпечення; психологічне спрямування кібератак.

Визначено шляхи мінімізації кіберризиків, до яких варто віднести: максимально оперативне оновлення захисних програмних комплексів, сканування вразливостей, тести на проникнення, bug bounty-програми та активне використання елементів теорії ігор як генератора негативних сценаріїв кібератак.

Ключові слова: кіберзагрози, кібербезпека, банківський сектор, умови воєнного стану

JEL Класифікація: D62, D82, G21, G32, H56

DOI: 10.55643/fcaptp.5.46.2022.3883