YÖNETİM BİLİŞİM SİSTEMLERİ DERGİSİ
http://dergipark.gov.tr/ybs

Yayın Geliş Tarihi: 12.02.2019
Yayına Kabul Tarihi: 20.05.2019
Online Yayın Tarihi:29.05.2019

Cilt:4, Sayı:2, Yıl:2019, Sayfa:24-48
ISSN: 2148-3752

SWIFT ATTACK VIA PHISHING AGAINST MIS OF MOBILE BANKING SECURITY

Ahmet EFE*

Internal Auditing, Ankara Development Agency, Turkey

Doğa ATAKAN

Department of Computer Science, Yıldırım Beyazıt University, Ankara, Turkey

Ümmihan Gönül ALTUN

Department of Computer Science, Yıldırım Beyazıt University, Ankara, Turkey

Abstract: As technology is developed on the world, crime types continue to develop with it; recent research shows that even corporate banks can face weaknesses in the face of cyber-attacks. We have investigated the most severe attacks that the banking systems have been facing and tried to sketch out major measurements against hackers who are using phishing attacks to hack swift system. Web based managing accounts still includes numerous sorts of dangers. Phishing attacks can be particularly harming to banks and clients who do not play it safe against this sort of security hazard. Since phishing programmers utilize a few refined strategies, going from tricky attacks to DNS attacks, banks must refresh their safety efforts consistently.

Keywords. Mobile Banking Security, Fintech MIS, Phishing, Swift Attack

MOBİL BANKA YBS GÜVENLİĞİNE KARŞI SWIFT OLTALAMA SALDIRILARI

Özet: Dünyada teknoloji geliştikçe, suç türleri de artmaya devam etmektedir. Son araştırmalar, kurumsal bankaların bile siber saldırıların karşısında zayıf kalabildiklerini göstermektedir. Bankacılık sistemlerinin karşılaştığı en ciddi saldırıları araştırılarak "phishing" saldırılarını kullanan bilgisayar korsanlarının ne tür zararlar verebilecekleri ve bunlara karşı nasıl önlem alınabileceği çalışmamızda inceleme konusu edilmiştir. Web tabanlı hesaplar ve mobil uygulamalar çok sayıda tehlike içermeye devam etmektedir. Kimlik avı saldırıları, bu tür bir güvenlik tehlikesine karşı güvende olmayan banka ve müşterilere zarar verebilmektedir. Kimlik avı programcıları, zorlu saldırılardan DNS saldırılarına giden

* Contact Author: aefe@ankaraka.org.tr

birkaç rafine stratejiden yararlandıklarından, bankaların güvenlik çabalarını sürekli olarak yenilemeleri ve gelişen saldırı vektörlerine uygun yeni önlemler araştırmaları gerekmektedir.

Anahtar Kelimeler: Mobil Bankacılık Güvenliği, Fintech YBS, Kimlik Avı, Swift Saldırısı

INTRODUCTION

Against continuous attacks from the cyberspace, security systems of institutions continue to developing with new technologies. In the past few years, the detection times for systems have been relatively reduced. Security systems could be detected 416 days after the attack in 2011, this time down to 205 days in 2014 and 101 days in 2017. In 2018, this period has gone down to 96 days. The most important reason that makes the detection of the attacks difficult is the use of the identity information of the captured real persons in all of the attacks. Hacking of a mobile banking system may not be a very unusual event, despite the fact that it is invested so much in security and it is so tedious.

Cyber attackers can steal someone's identity information but cannot steal their behavior in a variety of ways. Behavioral analysis technology, for example, instantly alerts this threat when a cyber attacker, who steals an engineer's identity and enters the system, attempts to perform an action such as accessing a client account that the engineer would never normally do, stealing records. Measures can be taken by not detecting the attacking months, but by detecting the attempted attack.

Thanks to this technology, threats that are really important are separated from other alarms and brought to the fore. For example, a system with 30 thousand users generates over 10 thousand security alarms that it generates monthly. Behavioral analysis instantly breaks down behaviors that are high risk and abnormal, giving 30 threat alarms per month. In this way, IT experts can capture the real attack by examining maybe 30 threats instead of getting lost among 10 thousand threats per month.

Banks and financial institutions are currently targeting 24 percent of all cyber-attacks in EMEA (Europe, Middle East, Africa). 24 percent of the cyber-attacks in the EMEA region are targeted. In Asia Pacific, this ratio is 39 percent, while the global financial sector is at the highest risk by 20 percent. If Turkey is also taking place in the EMEA region where the second priority target of cyber-attacks in case of public institutions. While the rate of attacks on public institutions is 6 percent in the Americas and 7 percent in Asia Pacific countries, 18 percent of attacks in the EMEA region are directed at the public sector. The third sector in the EMEA target is the business world with 12 percent. The global average of attacks on the business world is around 16 percent (TBB, 2015).

In recent years, lots of financial institutions have begun to give mobile banking service such as mobile website banking ,SMS-banking ,mobile banking on

mobile phone to their customers but there are lots of threats that exist for the mobile platform. The primary purpose of the article is to make the technical analysis of the SWIFT (Society for Worldwide Interbank Financial Telecommunication) Infrastructure Attacks, make some analysis and give examples in order to find answers to some questions.

RESEARCH QUESTIONS

Mobile phones and mobile devices have become widely used in everyday life by providing advanced capabilities such as internet, positioning systems (GPS), and wireless communication and health applications. These mobile devices, which exist almost every moment of modern life, sometimes provide a significant benefit as saving a life, and sometimes they turn into a spy that cannot be separated from human beings. Therefore, mobile device security is an important issue that needs to be developed for intelligent mobile phones powered by internet, camera, GPS and many sensors (A.R. Flo, A. Josang, 2009).

Mobile devices, despite the ease of use they provide, must be run with smaller operating systems than computers because of limited battery, storage, and processor constraints. The most common operating systems used in these devices are the ANDROID and iOS operating systems. First introduced in 2008, the ANDROID operating system became the most popular mobile operating system in 2016, dominating 84.7 percent of the mobile phone market (Iclarified, 2016). In particular, ANDROID operating system users have the authority to install applications from unofficial application stores, forum sites and memory card, which allows mobile phones to infect harmful software. For example, a simple application installed by the user to learn only the weather information can have many grabbers (camera, GPS, microphone, contacts, memory access, etc.) in the phone. This application has been modified by users in ANDROID 6.0 Marshmallow version and later versions. In previous versions, this application cannot be made by the user with the authority to restrict permissions. It is a great security feature that a simple application can easily access IP camera, location information, microphone, memory card and many other IoT devices.

Intelligent mobile devices are a technology used by billions of people around the world. Mobile devices' usage rates have increased with the development of advanced capabilities and technologies such as the Internet, location systems (GPS), and wireless communications and health applications. Devices with mobile operating systems have become the target of malware developers as they have a large usage spectrum, increased usage rates and security considerations. In fact, many sensitive data, contact information, passwords and even credit card numbers are kept in these small devices (Masum E., Samet R, 2018).

Every day new functionalities and qualities are added to the exsting technologies that make life easier in the banking and finance sector. With increasing digitalization, cyber threats increase in the same way threatening users and

institutions. However, the cyber threats are not only increasing in number but also the methods used at the same time, the experiences and resources of the attackers are developing every year, and the attacks are becoming increasingly sophisticated. The SWIFT system, which has more than 11,000 financial transactions in more than 200 countries and more than 21 million transactions a day, is one of the most important players in the world's financial ecosystem. In many countries, when the banks were damaged and only from Bangladesh's Central Bank they had stolen $ 81 million, the attackers fully exploit security vulnerabilities in the banks' systems. SWIFT has published the Customer Security Program to combat cyber-attacks and to support its customers in this fight, although its system has not been compromised (Damodaram, 2016).

For this research, three questions are defined to find their answers:

- How do the phishing attacks occur?
- How the banks and clients are affected from the phishing?
- What Can Banks do for Providing Proper Cyber Security?

SWIFT SECURITY

SWIFT stands for the Society for Worldwide Interbank Financial Telecommunications. It is a messaging network that financial institutions use to securely transmit information and instructions through a standardized system of codes. SWIFT assigns each financial organization a unique code that has either eight characters or 11 characters. The code is called interchangeably the bank identifier code (BIC), SWIFT code, SWIFT ID, or ISO 9362 code.

- First four characters: the institute code (UNCR for UniCredit Banca)

- Next two characters: the country code (IT for the country Italy)

- Next two characters: the location/city code (MM for Milan)

- Last three characters: optional, but organizations use it to assign codes to individual branches. (The UniCredit Banca branch in Venice may use the code UNCRITMMZZZ.)

1. The Swift Attack

Attackers are using MS Office macros to infect target organizations with malicious software. After the macro runs, malicious software is downloaded on the target system and PowerShell+WMI scripts are executed. All existing Macro and downloaded PowerShell scripts are complicated by attackers, antivirus, etc. their systems have been compromised.

The virus, which has gained authority with the use of macros, is able to change the information in swift messages. Therefore, attackers can change the recipient's address or the amount. The bad thing is that it can delete the process from

the queue after it has been queued and processed. In addition, when it does not have a record, it cannot be noticed quickly.

After attackers seized the systems, they infected the backdoor software to be permanently in the system, as well as the tools to intercept swift data, collect Credit Card data. At the same time, the targets of attackers include ATM, POS data. Such attacks cannot prevent traditional security solutions, events and experiences are constant. In the same way, endpoint security solutions developed to prevent these and similar attacks and launched as "next-generation" are not being configured correctly and effectively by representatives and sales teams, putting institutions at risk seriously. The current screenshot belongs to the Office Word file used by the network targeting banks in Turkey to attack a bank in Russia for infection at the first stage.

2. Mobile Banking Attacks

Today, banks and financial institutions are targeting 24 percent of cyber-attacks in EMEA (Europe, Middle East, Africa). The security systems of the institutions against cyber-attacks continue to be strengthened with new technologies. In recent years, systems have been detectable more than a year after an attack took place, while the detection times are relatively low. Security systems were able to identify 416 days after the attack in 2011, while this period decreased to 205 days in 2014 and to 101 days in 2017. In 2018, this period has fallen to 96 days. The most important reason that makes the detection of the attacks difficult is the use of the identity information of the captured real persons in all of the attacks (Leukfeldt, 2016).

The SWIFT (Society for Worldwide Interbank Financial Telecommunication) system, which is one of the most important players in the world financial ecosystem, with more than 21 million financial transactions in more than 11.000 organizations of 200 countries, has also been the target of significant attacks in recent years. In many countries, where the banks have been damaged and $ 81 million was stolen only from the Central Bank of Bangladesh. The attackers took advantage of the security gaps in the banks' own systems and they are continuously searching for new vulnerabilities following zero day exploits. SWIFT has launched the Customer Security Program[*] to combat cyber-attacks and to support its customers in this fight, even though its system has not been damaged. According to a very recent news[†], T-Mobile, one of the largest telecom operators in the world, confirmed that it was attacked by a cyber-attack. The attack on August 20th 2018, 2

[*] The Customer Security Program (CSP) is a security framework created by SWIFT to contribute to the information security systems that its customers currently provide and maintain. CSP is a program based on standards such as ISO27002, PCI DSS, NIST which are not foreigners in the information security sector.

[†] For details see: https://www.forbes.com/sites/leemathews/2018/08/24/t-mobile-hackers-swipe-data-on-2-million-subscribers/#11c6b36e7a52

million T-Mobile user's personal information was passed into the hands of cyber attackers. The information included is T-Mobile customers' name and surname, invoice Zip code, phone number, e-mail address, account number and account type (prepaid or postpaid). The good news is that there is no sensitive information, such as credit card numbers, and sensitive information, such as a password, between stolen information. The blogs in deep web posted brief information about the cyber-attack and announced on Monday (August 20th 2018) that the attack was detected by security teams and was repulsed as soon as it was detected. No clear information was given on how cyber-attackers accessed servers or the number of customers affected. Now we can ask which countries are affected most?

Vietnamese

The assailants gathered data about the sort of PDF perusers utilized by a Vietnamese Bank. This data could undoubtedly be gotten through social building and the responses to apparently guiltless inquiries could imperil an establishment. Thusly, they made malware that focused the triumph of the particular form of the PDF peruser. Bank authorities perceived the circumstance and averted illicit cash exchanges.

Ecuadorian

After the attackers stole a representative's accreditations, they could get to the Bank's framework. The attackers at that point exploited the absence of control, for example, great email cleaning and ensuring that messages were sent, by changing the blade messages left in the email Outbox (monetary message containing cash exchanges) to attack.

Bangladesh

The attackers in charge of the Bangladesh attack introduced SysMon (Microsoft Activity Monitoring) as a surveillance instrument to Swiftville. The product had Executive benefits and enabled assailants to screen representative connections utilizing the quick terminal in the Bank. Sysmon purportedly stacked with an angling attack focusing on a worker with access to the quick terminal. As indicated by the reports, it is expressed that the switchs which are situated to the Bank are not reasonable for the utilization of a low-estimated Corporate Bank are likewise the wellspring of the infringement.

Turkey

On 8 December 2016, a digital attack was made against Akbank, one of Turkey's biggest banks, and as far as anyone knows two other Turkish banks. Akbank discharged an announcement affirming the attack to their IT frameworks that it identified with the SWIFT framework and expressing that they had reacted to the attack instantly and played it safe. The bank likewise put forward that the greatest measure of hazard looked by the bank is USD $4 million which is secured by its protection arrangement.

The attack was like the one made against the Central Bank of Bangladesh in which the assailants accessed the bank's installment qualifications in the SWIFT System According to an article, the introductory attack vector was skewer phishing; the attackers focused on a worker with a Microsoft Office Document containing a malevolent full scale that downloads the Odinaff malware, attackers at that point picked up diligence and began exercises in the bank's system utilizing Windows parts. The utilization of 'honest to goodness' programming enabled attackers and malware to stay under the radar of antivirus programming which normally searches for obscure or new records. Assailants gathered Visa data and executed cash exchange by means of the SWIFT framework. Likewise observed in past Odinaff attacks the malware could shroud logs and SWIFT messages identified with the fake exchanges made by the assailants the attackers revamped the SWIFT message points of interest all together for the installment to be made to an address (Masum, 2018).

Turkey in carrying out the work on cyber security and large data STM announces new Cyber Threat Status Report[*]. In the new cyber threat report of the first 3 months of the year, STM's personal bank information can be captured through mobile applications that look innocent. The new generation of cyber threats out, 22 banks was taken goals from Turkey.

Recently, the form of attacks targeting mobile banking is now changing. In the Android operating system's store, a malicious software has been discovered that looks like an innocent weather app and targets mobile banking customers. Google Play 'Good Weather' this malicious software application called manifested as weather forecasts, it was targeted at customers of 22 banks from Turkey[†].

In fact, this application, which stands out as a harmful form of the well-known weather application Good Weather, preserves the weather forecast features, however, it can lock the infected devices remotely, access SMS messages and focus on stealing mobile banking information used over the mobile phone. Google Play Store, weather forecasting application is malicious software that 2 days after noticeable lifted; but it is estimated that malware may have affected more than 5 thousand users in this short period of time. The first application of the targets of reaching 5 thousand users in 48 countries, according to the Turkey's determination. Moreover, our country stands out as the most targeted country. Turkey 2 thousand 144 downloads have been identified. The closest download looks to be made from Syria with 202 pieces. Syria is followed by South Africa with 24 downloads (Masum, 2018).

ESET, the nearly simultaneous attacks wannacry draws attention to the growing but mainly Bankbot attacks targeting Turkey. The Bankbot trojan horse focuses on Turkish mobile banking customers to get their login information.

[*] For the reports and articles produced by STM and further details of the topic see: https://www.stm.com.tr/tr/yayinlar/makalelerraporlar

[†] For details see: https://katilimdunyasi.com/2017/04/11/mobil-bankacilik/

Bankbot, who want to watch movies over the phone, stating that it is necessary to a fake Flash Player application. Trojan horse infected by downloading the application. The malicious software detects legal banking applications on the device it is infected with and creates a fake form, allowing the user to enter their information into this form. Thus, mobile banking customers reach their login information. According to the latest determination Bankbot, he seems to have imitated a total of 16 banks for mobile banking applications in Turkey. The Bankbot Trojan horse is based on a public code. The code is shared free of charge in underground internet forums in Russia. According to ESET Security Researcher Lukas Stefanko, the main danger lies here. Stefanko notes that due to the free distribution of code, we can see more banking trojans in the coming period and the area of attack may expand. Lukas Stefanko, using 11 different servers, according to the findings so far, mainly reported that they were able to identify the affected users, including at least 640 from Turkey. The attackers' servers are in Dubai. Lukas Stefanko, ESET Security Researcher[*], warns that Flash Player applications should be paid attention and not downloaded from everywhere.

Many malware are being downloaded to mobile devices especially because of security problems on Android platform. malware targeting mobile applications that can neutralize the banks and banks in Turkey SMS confirmation message, users are taking over the banks and credit card information, login information, as well as their social media accounts. Malicious software that can disable the SMS confirmation from the bank can pass the double-factor SMS authentication step.

According to some experts[†], Turkish banks and even the banking system have a say and appreciation on the world at all times. General consensus among the experts, banks in Turkey at a level that can be called safe above the world average. Information security and effective identity management are now an important part of the strategic planning of Turkish banks. Information security, in the simplest way, is to protect the information assets that need to be protected in terms of privacy, integrity and accessibility with human, process and technology dimensions. Turkish banks have all the necessary technological products and certifications for information security. Fulfilling the requirements of these certifications addressing information security directly contributes to our banks both in terms of compliance and security. The lack of qualified personnel in the security area of the most significant shortcomings in Turkey. The information technology units of our banks generally have qualified personnel in the field of security, and invest in education and equipment on their systems and personnel.

The criteria such as the work of our banks' business units and how easily customers can use the systems can make it difficult to take some security

[*] For details see: http://katilimfinansdergisi.com.tr/siber-saldiriya-karsi-onlem-aliniyor/
[†] For details see: https://www.fraudandchargeback.com/tr/siber-saldirilara-karsi-bankalarimiz-ne-kadar-guvenli/

measures. Security; it is defined as a balance between the easy and fast execution of work and the safe execution of the work. In some cases, this balance is deteriorated in our banks; the ease of use of the customer outweighs the security, especially in some Internet and mobile banking products appear to occur in security weaknesses. As an example, in 2016, we can demonstrate the numerous cases of victimization and fraud that are related to the product called fast credit, which is defined to customers through internet and mobile banking.

Despite all these security investments and the measures taken so much, it is not unusual for our banks to be hacked. Because from the technical point of view, we can say that all institutions in the world can be hacked. None of the investments made can make systems un-hackable. But banks in general we can say safely at a level above the world average in Turkey.

3. Some Swift Attack Types

3.1. Phishing

The objective is to obtain confidential information from the real customer of the bank (for example, PINs, passwords, credit card numbers, etc.). It is based on social engineering. It works like attracting users to a fake website that looks a lot like the real bank's website. It is mainly done through links in emails (Ekawade, 2016).

3.2 Pharming

The objective is the same as with phishing (taking PINs, passwords, charge card numbers, and so on.). It did not depend on unadulterated social building. There are some specialized traps included (DNS reconfiguration). Generally, it requires a Trojan stallion/infection on the casualty's PC (Ekawade, 2016).

3.3Man in the middle

The assailant needs a trojan steed on the casualty PC. a man-in-the-center attack (MITM) resembles listening stealthily. Information is sent from point A (PC) to point B (server/site), and an assailant can get in the middle of these transmissions. They at that point set up devices customized to "tune in" on transmissions, catch information that is particularly focused as profitable, and catch the information. In some cases, this information can be changed during the time-spent transmission to attempt to trap the end client to uncover delicate data, for example, sign in accreditations. Once the client has fallen for the draw, the information is gathered from the objective, and the first information is then sent to the expected goal unaltered (Mishra R. 2016).

3.4 Salami Technique

Salami slicing/penny shaving where the aggressor utilizes an online database to grab the data of clients, that is bank/Visa subtle elements, deducting microscopic sums from each record over some stretch of time. These sums normally mean huge entireties of cash that is unnoticeably taken from the aggregate records. It is taking

the adjusted off decimal parts of bank exchanges and moving them into another Banks frequently utilize decimal places past the penny while ascertaining sums as far as premium. In the event that a client acquiring premium consistently has gathered $50.125 in premium, the division of the penny is adjusted by the bank's framework such an attack was apparently executed at a Canadian bank where an insider siphoned $70,000 from other client accounts into his own. A bank office chose to respect the client who had the most dynamic record. It ended up being a worker who had gathered $70,000 channeling a couple of pennies out of each record into his own. Taking such a little portion may appear to be irrelevant or even undetectable to the casualties, however when done crosswise over a large number of exchanges, the collection can be huge for the attacker (Chaudhry, 2016)

3.5 Man in the browser (MITB)

Man-in-the-Browser (MITB) attacks are utilized through Trojan malware that contaminates an Internet program. These attacks are to a great degree unsafe in light of the fact that they can be put away in hostile to infection programming and can take data about client composes in the program. It is feasible for the MITB to see the data in the scanner. Since no encryption has happened in the program, the security controls utilized by money related organizations have turned out to be incapable. Furthermore, if malware approaches client account settings, two-factor verification is likewise inadequate. Since the exchanges begin from client workstations, the counter extortion advancements that banks use to recognize malevolent action are additionally ineffectual (Ekawade, 2016).

Numerous banks have included extra security layers for settlement exchanges utilizing SMS-like notices. Indeed, an assailant could likewise be able to change the notice settings of clients 'ledgers in the event that they can take clients' certifications. Because of the way that MITB attacks, chip away at numerous system level gadgets, for example, the web application firewall, IDS and IPS frameworks experience issues finding these attacks locally on the customer side. Man in the program attacks can be spread to numerous frameworks by means of prevalent connections, accentuation interfaces or authentic site compromise. By tapping on a connection, the trojan can be introduced in the program as an extra so noxious programming can be seen as secure.

DETAILS OF PHISHING ATTACKS

What really distinguishes phishing is the form the message takes: the attackers masquerade as a trusted entity of some kind, often a real or plausibly real person, or a company the victim might do business. It is one of the oldest types of cyberattacks, dating back to the 1990s, and it is still one of the most widespread and pernicious, with phishing messages and techniques becoming increasingly sophisticated.

1 Phishing Kit

The accessibility of phishing packs makes it simple for digital culprits, even those with insignificant specialized aptitudes, to dispatch phishing efforts. A phishing unit groups phishing site assets and instruments that need just be introduced on a server. Once introduced, the assailant should simply convey messages to potential casualties. Phishing packs and in addition mailing records are accessible on the dim web.

Several locales, Phishtank and OpenPhish, keep swarm sourced arrangements of known phishing packs. Breaking down phishing packs permits security groups to track who is utilizing them. "A standout amongst the most valuable things we can gain from dissecting phishing units is the place accreditations are being sent. By following email tends to establish in phishing units, individuals can correspond on-screen characters to particular battles and even particular packs," said Wright in the report. "It shows signs of improvement. Not exclusively would we be able to see where qualifications are sent, yet we likewise observe where certifications claim to be sent. Makers of phishing packs normally utilize the 'From' header like a marking card, letting discover different units made by a similar creator (Eze, 2008).

2 Types of Phishing Attacks

2.1 Deceptive Phishing

The expression "phishing" initially alluded to account burglary-utilizing texting yet the most widely recognized communicate strategy today is a misleading email message. Messages about the need to confirm account data, framework disappointment expecting clients to re-enter their data, invented account charges, unwanted record changes, new free administrations requiring fast activity, and numerous different tricks are communicated to a wide gathering of beneficiaries with the expectation that the unwary will react by clicking a connection to or marking onto a sham site where their classified data can be gathered.

2.2 Malware-Based Phishing

It alludes to tricks that include running vindictive programming on clients' PCs. Malware can be presented as an email connection, as a downloadable document from a site, or by abusing known security vulnerabilities that a specific issue for little and medium organizations (SMBs) who are not generally ready to stay up with the latest.

2.3 Keyloggers and Screenloggers

They are specific assortments of malware that track console input and send pertinent data to the programmer by means of the Internet. They can insert themselves into clients' programs as little utility projects known as assistant protests that run naturally when the program is begun and into framework documents as gadget drivers or screen screens.

2.3 Session Hijacking

It depicts an assault where clients' exercises are checked until the point that they sign in to an objective record or exchange and build up their genuine qualifications. By then the malignant programming assumes control and can attempt unapproved activities, for example, exchanging stores, without the client's information.

2.4 Web Trojans

They fly up imperceptibly when clients are endeavoring to sign in. They gather the client's accreditations locally and transmit them to the phisher.

2.5 Hosts File Poisoning

At the point when a client writes a URL to visit a site it should first be converted into an IP address before it is transmitted over the Internet. The larger part of SMB clients' PCs running a Microsoft Windowsoperating framework first gaze upward these "host names" in their "hosts" document before attempted a Domain Name System (DNS) query. By "harming" the hosts' record, programmers have a fake address transmitted, taking the client accidentally to a phony "twin" site where their data can be stolen.

2.6 System Reconfiguration Attacks

They change settings on a client's PC for vindictive purposes. For instance: URLs in a top picks document may be changed to guide clients to resemble the other similar sites

2.7 Data Theft

Unsecured PCs frequently contain subsets of delicate data put away somewhere else on secured servers. Absolutely PCs are utilized to access such servers and can be all the more effortlessly traded off. Information burglary is a broadly utilized way to deal with business secret activities. By taking secret correspondences, plan archives, legitimate assessments, representative related records, and so forth., criminals benefit from pitching to the individuals who might need to humiliate or cause financial harm or to contenders.

2.8 DNS-Based Phishing

Pharming is the term given to have record alteration or Domain Name System (DNS) - based phishing. With a pharming plan, programmers mess with an organization's host's records or area name framework so asks for URLs or name benefit restore a sham address and resulting interchanges are coordinated to a phony site. The outcome: clients are unconscious that the site where they are entering secret data is controlled by programmers and is most likely not even in an indistinguishable nation from the honest to goodness site.

2.9 Content-Injection Phishing

It portrays the circumstance where programmers supplant some portion of the substance of a genuine site with false substance intended to delude or mislead the client into surrendering their classified data to the programmer. For instance, programmers may embed malignant code to log client's certifications or an overlay, which can subtly gather data and convey it to the programmer's phishing server.

2.10 Man-in-the-Middle Phishing

It is harder to distinguish than numerous different types of phishing. In these assaults, programmers position themselves between the client and the honest to goodness site or framework. They record the data being entered yet keep on passing it on with the goal that clients' exchanges are not influenced. Later they can offer or utilize the data or qualifications gathered when the client is not dynamic on the framework.

2.11 Search Engine Phishing

It happens when phishers make sites with alluring (frequently excessively appealing) sounding offers and have them listed really with web indexes. Clients discover the locales in the typical course of scanning for items or benefits and are tricked into surrendering their data. For instance, con artists have set up false managing account locales offering lower credit expenses or preferred financing costs to different banks.

SOLUTIONS FOR PHISHING ATTACKS

There are different techniques that a bank can use to battle phishing attacks. These techniques are known as phishing attack countermeasures, which incorporate email what's more, site page personalization, security programming, the utilization of two-factor validation, and expanding client mindfulness. A portion of the techniques that this area prescribes to lessen the danger of phishing attacks will keep the clients from being tricked by web based phishing assailants.

1. Email Personalization

The least difficult route for banks to battle the trickiness of phishing attack messages is to incorporate customized data with all genuine correspondences. Money related establishments need to actualize individual identifiable data to separate their messages all the more plainly from phishing attacks all messages sent to clients ought to be customized for particular beneficiaries. Individual identifiable data may incorporate the client's name or different references of special data shared just between the banks and clients .For instance, if each email sent from the bank starts with the client's name and this email teaches the clients about this training, at that point the client will realize that any email which does exclude his or her name ought to be considered as a suspicious email. Individual identifiable data causes bank clients to guarantee that the email was sent by their banks. Since phishing attacks do exclude the client's close to home data, for example, a name, the misdirection of phishing attack can be lessened when banks actualize the email personalization

system. Indeed, banks are presently required to incorporate individual identifiable data to defend their client's certification information. The execution of this kind of procedure is troublesome, however it is successful.

2. Site Page Personalization

Another type of individual identifiable data is site page personalization. In this kind of customized data, the bank clients ask for a content or picture to be utilized alongside their passwords and usernames. In expansion, the clients need to go through two pages when going to their bank's site the principal page requires the client to give a username. At the point when the client name is legitimate, the client is given a customized page for entering the secret word. The second page is customized with the expressions or pictures that the client picked when he or she made the record. The bank ought to remind the client never to type in his or her secret key unless he or she perceives the picture as well as expressions on the secret key page.A phishing assailant will not know this customized data and will not have the capacity to reproduce it when endeavoring to fashion beguiling messages.

3. Assurance Programming

Phishing attacks are hard to foresee because they arrive in an assortment of techniques to get to client PCs furthermore, get qualification data, for example, usernames and passwords. As specified before, attackers could utilize malware projects to contaminate a client's PC. This kind of noxious attack could be introduced when the client visits a suspicious site or downloads an email connection. Along these lines, one of the most straightforward devices that a client can apply to keep phishing attacks from achieving his or her PC in any case is the counter infection and antispyware programming against programming incorporates PC programs that shield clients from infections and spyware by filtering the whole documents. These PC programs avoid phishing attacks by distinguishing programming that could divert clients to fake saving money sites. Another sort of programming that could be viable in avoiding phishing attacks is against lumberjack programming. Since most against programming is not adequate in distinguishing keyloggers, the counter lumberjack programming can help with distinguishing shrouded keylogger programs. The two banks and clients ought to introduce security programming onto their PCs. When they introduce these product programs, the client must empower them and guarantee they are breakthrough

4. Two-factor Validation

Banks should utilize powerful strategies to validate client personality. A more established strategy, known as singlefactor confirmation, is available to bargain from phishing attacks, so programmers can sidestep this confirmation moderately effortlessly. Consequently, banks ought to rethink depending on single-factor validation as their just control strategy, as it is not viable for high-hazard exchanges, which include getting to client data or exchanging assets to different gatherings. A prevalent and more grounded, other option to single-factor validation

is Solid Confirmation, which is moreover alluded to as two-factor validation. Two-factor confirmation is a strategy that requires the clients to display two distinct sorts of proof to build up their personality. Two-factor confirmation is normally alluded to as something a client has and something a client knows to begin with, something a client has ordinarily includes equipment or programming that furnishes the bank clients with an electronically created password or computerized endorsement. Each bank client has a one of a kind password or computerized declaration. The second factor, "something a client knows," normally implies a private secret word. Bank clients should utilize the two variables to give themselves a solid validation framework for empowering access to basic assets, for example, online banks. Two-factor validation frameworks are secure in light of the fact that assailants confront extraordinary trouble gaining both of these variables. The usage of two-factor verification is more grounded what's more, more secure than single-factor verification, such as a watchword alone. Phishing attacks can without much of a stretch catch a client's secret word, so the second factor for confirmation is compelling at lessening phishing attacks and in this manner significantly decreases the shot of online cheats (Eze, 2008).

5. Client Mindfulness

Since most phishing attacks start with false messages, banks ought to organize client mindfulness. In addition, clients need to teach themselves about the peril of phishing attacks. A substantial number of phishing attacks can be avoided if the clients are caution what's more, careful of the dangers. Banks should help clients with their mindfulness by refreshing them of security hones. Normal updates will guarantee that clients can recognize real messages and sites. It is basic that banks advise their clients of the perils of phishing attacks and what countermeasures are accessible. In particular, banks must guarantee that they appropriate data to their clients with respect to how to discuss safely with their monetary organization Banks ought to give rules to their clients, too. The reason for the rules is to illuminate the client about the main manners by which the bank will speak with them. This sort of mindfulness ought to be directed always and in a way that is simple for the clients to get it. Rules can be given in two distinctive ways. Right off the bat, rules can be given to the clients as records at the season of client enlistment. Besides, rules can likewise be shown as "security directions" on the bank's site and appeared to the client before login. A case of a general rundown of directions that most banks distribute is as takes after (Eze, 2008).

- The bank will never request that clients give their "username, secret word, Mastercard number, full name, financial balance number, and so forth via mail"

- Bank clients ought to never react specifically to any messages that contain critical solicitations for individual data.

- An official email messages will never contain any connections or application structures to be filled in.

- Bank clients ought to dependably visit the bank's site by composing the bank's address into the web program.

Besides, clients ought to confirm that the safe site signs are available in their programs, for example, the https association and bolt symbol, previously entering their delicate data into the web program.

6. Layered security architecture

Layered security is the process of taking multiple measures on the protected system. We can see examples of this in the current life. For example, a person who uses a fence to protect his house will not only be safe with fencing, but also a safe door, maybe an alarm, a window protection and additional security measures. The aim here is to make the malicious people who can overcome an obstacle stick to other obstacles.

The security of the layered security concept in the world of information is an in-depth security, and the concept of defense-in-Depth has an important place in information security. It has been developed against the idea that all of the measures taken against the attackers will be overcome in some way. When these measures can be overcome one by one, it is based on the thesis that the attackers' work will become more difficult and the success rate of attack will decrease. However, a completely secure system connected to the Internet or a network cannot be installed (Iclarified, 2016)

Let us explain the concept of in-depth security with a practical example.

1. Layer: Boundary device

2. Layer: Border firewall

3. Layer: DMZ firewall

4. Layer: (NIPS) Network based attack prevention system

5. Layer: Netflow abnormality detection system

6. Layer: Antivirus system

7. Layer: (HIPS) Host-based intrusion prevention system

7. Isolation of SWIFT System from Other Systems

SWIFT system infrastructure in a different place than other systems to be exposed to attacks from other systems should be prevented.

8. Supervised Account Use

As with the general security protocols, only authorized users should be given access to the SWIFT system, access to unauthorized users should be closed, maintenance should only be opened in case of emergency, and only for certain persons.

9. Internal Network Data Flow Security

Privacy, integrity and account verification systems are used to protect and control the SWIF system and its connected users (Razak LT. 2016)

10. Updates

The software and hardware used by the SWIFT system and its affiliated users must be used within the life span specified by the manufacturer and must be completed in a timely manner during the update.

11. System Tightening

The system tightening should be done in the SWIFT system in the secure zone and the users connected to it.

12. Physical Safety

Physical access to sensitive equipment should be restricted and monitored.

13. Password Policies

The more strict and complex the password policies are, the greater the password security.

14. Multistage Input Validations

When logging into the system, multi-step verification systems should be used as well as password security.

15. Account Management

The user accounts opened for access to the SWIFT system must be created from personal accounts, which have the minimum authority to have. Their duties and powers must be taken into account, unnecessary authorizations should be avoided.

16. Token Management

Caution should be exercised in handling and storage cancellation of session verification tokens.

17. Malware Protection

Note that malware protection is installed and up-to-date on all systems.

18. Software Integrity

All software related to the communication interface and SWIFT must be checked for integrity.

19. Database Integrity

Periodically check the SWIFT database integrity periodically.

20. Log Mechanism and Management

The working health and instant follow-up of the log mechanism are important for the control of abnormal activities, the logging mechanism should be run and followed well.

21. Cyber Events Response Planning

In order to intervene in cyber incidents, it is important to take action according to a specific team and attack type and to take action as soon as possible.

22. Cyber Security and Awareness Training

All employees who have access to SWIFT or who work in relevant substructures should receive annual cyber security and awareness training (Defuel, 2003)

23. Back Office Data Flow Security

Back office data flow, infrastructure data control, integrity security authentication systems must be checked and audited (Konoth, 2016)

24. External Transmission Data Protection

Sensitive data must be encrypted when leaving the secure network. It should be checked that no meaningful data is obtained when examined and analyzed.

25. User Session Integrity

Logon and privacy control of users connected to the secure network must be controlled.

26. Vulnerability Screening

Vulnerability scans should be performed with software that conforms to industry standards.

27. Out of System Critical Activities

Critical activities outside the system should be performed with maximum safety by applying security procedures within the system.

28. Staff Review Process

It is necessary to periodically examine the profiles and behaviors of persons with access to the SWIFT structure before and after the assignment.

29. Physical and Logical Password Storage

User controls must be stored logically and physically controlled by certain people in a controlled manner.

30. Attack Detection

Intrusion detection and system monitoring must be performed instantaneously to monitor and prevent unauthorized access.

31. Penetration Tests

Penetration tests should be carried out at least once a year with industry-standard applications, and the results of automated tests should be checked manually.

32. Scenario and Risk Analysis

Scenario-based preparation will increase the rate of action taking at the time of the attack, so the scenario diversity and preparation should be tried and tested regularly.

DISCUSSION

Threats, which are important by this technology, are distinguished from other alarms and highlighted. For example, a system with 30,000 users generates more than 10 thousand security alarms per month. Behavioral analysis provides a 30-month-old threat alarm by instantly decomposing behaviors that are really high-risk and abnormal. In this way, IT professionals, instead of being lost between 10 thousand threats per month, perhaps by examining only 30 threats can capture the real attack. The new security technology developed against cyber-attacks is based on an analysis of behavior. Even if attackers try to infiltrate the identity information of an engineer working at the target institution with an e-mail, attacking (phishing) attack and try to infiltrate the system with the authority of the engineer. There are some important points that I find useful in remembering about the cyber-attacks against the banners, if we take a brief look at them (Chiu, 2016);

▪ Banks are tempting targets for cybercriminals. The money is there and a very important part of the cybercriminals is motivated by money.

▪ Individually, our accounts are being targeted more frequently. It is normal if we think that the measures taken by the banks are more than the measures taken on our personal computers. Bank customers are easier targets than the bank itself.

▪ All systems can be hacked. None of the investments made can make the systems become "hackable".

▪ Criminals are not "curious children". The image of "hackers are a little curious, good intentions" from movies is far behind. Today cybercriminals are criminal groups that are well educated, have high technical skills, do not have resource problems and are really aiming to steal money.

▪ The IT security unit does not make all the decisions. Criteria such as the work of the bank's business units and how easily the customers can use the systems can make it difficult to take some safety precautions. Security; is a balance that needs

to be set up between running the business safely and easily and quickly. In some cases, security may outweigh the ease of use of the customer in some cases.

Web based managing an account includes numerous sorts of dangers. Phishing attacks can be particularly harming to banks and clients who do not play it safe against this sort of security hazard. Since phishing programmers utilize a few refined strategies, going from tricky attacks to DNS attacks, banks must refresh their safety efforts consistently. Besides, banks ought to guarantee that the exchanges amongst themselves and their clients are secure. Banks must utilize some sort of refreshed counter measure, for example, two-factor validation, alongside other insurance programming programs. They will likewise advantage hugely from instructing their clients about phishing attack dangers and about the manners by which unapproved access to the clients' money related data could happen while giving the means that they can take to secure their budgetary data. Bank users require being careful with phishing attacks by figuring out how to distinguish suspected phishing messages. There are a few signs to distinguish an attack sent by email. In phishing attack, assailant may copy an image of a genuine organization, duplicate the name of an organization or utilize the genuine name of a representative, which used to guarantee you that you are accepting email from the organization or bank. In addition, clients ought not to react to any bonus or a demand of losing an existing financial balance, which may leave your information in danger (Konoth, 2016).

Additionally, bank clients must check the wellspring of data from approaching sends with the goal that they could make beyond any doubt, whether it is a phishing attack. Additionally, clients should realize that banks never send an e-mail to their clients ask for requesting usernames and passwords. In the event that the clients get an email requesting for certification data, they ought to instantly check their bank site by composing their bank site address into the web program. As said earlier, clients' mindfulness ought to be the best need of banks in term of fighting the phishing attack. Phishing is quickly developing and harming both banks and clients on the off chance that they do not play it safe against security dangers. At last, once bank clients learn about their rights and duties.

Because there are many openings in mobile environments, they should always be more careful in the work and operations that can be done in these environments. The construction of infiltration facilities by independent organizations in these environments will contribute to the preliminary detection of many openings. Finally, it is inevitable that the use of mobile environments, which are becoming more and more widely used, becomes more effective in our lives and that work and operations are more performed in these environments. Being always aware of the responsibility of the users in resolving the security vulnerabilities that may be caused by the threats and threats that may be encountered in these environments will enable the users to communicate in a safer environment.

Internet, being used in Turkey at the beginning of the 1990s, came to be a part of our lives is indispensable in time. Emerging technologies in parallel without

the need to go to the branch that is connected to the internet anywhere, anytime safely internet banking emerged that allows you to make transactions of the day. Internet banking in Turkey, as well as all over the world was rapidly spreading. The spread of internet banking technology in the financial sector and in this case the use of cyber abuse with the increase in the number of users experienced attacks began to occur. In this case, the financial sector served as the locomotive of the country's economy was also effective.

While the importance of information for banks is in an indisputable position, the protection of this information has gained a particular importance. Banks are also constantly work to do in this manner the reliability of internet banking for R & D projects have started to implement. Banks have been carrying out studies to provide secure service to their customers with internet infrastructures at international standards. The people who used to be the target of the attack, but now everyone who has a smart phone, these threats are faced.

Different scenarios can apply to swift exploitations. According to a report prepared by Turkish Banking Associations (TBB) there are some scenarios that usually happen (TBB, 2015). The e-mail addresses of the companies engaged in international trade are seized by fraudsters who abuse information systems. The IBAN information on the proforma invoice sent by the contractor firm via e-mail is deleted and the IBAN information of another account belonging to the hacker is written and this proforma invoice is notified to the contractor company's e-mail address and the other company which is the buyer of the goods. The amount sent for the goods is transferred to the accounts of the malicious persons instead of the real company engaged in trade and thus the balance is captured.

Scenario 1: Gridağ Dış Tic. Ltd. Sti. accounts for 50K US dollars from Leymun company located in Iran, but Ankara branch's high-turnover business company specify to AliBank that it is their own money. AliBank officials investigated the situation through the correspondent bank and sent the e-mail address of the customers in Ankara branch. It was defined that the proforma invoice was changed by Gridağ Tic. Ltd. Sti. The proforma invoice, presented by the company as the buyer of money, proved to be fake.

Scenario2: The e-mail address of a foreign company in which Aras Petrol has a commercial relationship has been seized by scammers. The hackers, using spear phishing technique by a fake e-mail, sent to Aras Petrol, which included fake documents, and asked to transfer the traded 500K US dollar to a different account abroad. Aras Petrol has been doing business with the company with which it has established a trade relationship. For this reason, it is never suspected of the notification made by e-mail, and fulfills the request and sends the amount to the account that is reported in the e-mail content. Shortly thereafter, the company returns to Aras Petrol for the fact that the payment still does not arrive. In this way, the recipient's e-mail address is captured by hackers and the amount is sent to hackers.

CONCLUSIONS

In cyber security, ensuring customer awareness is at least as critical as the measures that banks take against cyber-attacks. Instead of dealing with the necessary technical applications, cyber-attackers can sometimes go to the bank to deceive their customers. In the end, it is a more attractive option for people to take advantage of their momentary snapshots against the time they will lose. Therefore, the fact that customers cannot hide their confidential information from third parties brings about a security problem. In this context, using the social engineering method, it is important to consider the possibility of learning the answers to the password or security questions of the bank customers. Responsibilities in this regard fall to bank customers. Customers should not share their confidential information with anyone, including bank representatives. In addition, customers should not use the same passwords in different applications. Of course, customers need not keep their personal information anywhere in the digital environment. It is important for the users of mobile banking to use anti-virus software on their computers while performing these operations. Customers should consider all these situations.

In order to raise the awareness of the customers and the formation of awareness of the tasks of the banks are falling. Banks should periodically provide the necessary information to their customers. In addition, customers should not skip the question of whether banks are making changes to their customer information in a telephone or digital environment. In such a case, the client should not share his / her information. You can also use the name of the bank to receive incoming calls, SMSs or mails. In this case, customers, telephone fraud, e-mail containing virus software, you should be careful in many cases as harmful attachments.

When the news site you are commenting on is cyber-attacked, your password is also captured among the information. After that, the pirates are emailing you, demanding something. They also know the password 'they can give the ransom they want. To avoid such dangers in terms of the password' less important, more important 'we need to make a rating. In it, not only numbers and specific dates, but different characters should be used. We can provide security.

In this study we tried to make give some information, analyze swift and phishing attacks and assess different measures. For this research, three questions were defined to find their answers:

- How does the phishing attack occur?

Now, phishing attack evolved as “spear phishing” that is particularly designed for your specific weaknesses and targeted to you disguising their real face in order to convince that you are a trusted party using your current credentials.

- How the banks and clients are affected from the phishing?

The staff and customer credentials can be taken by attackers therefore unauthorized financial transactions can happen.

- What Can Banks do for Providing Proper Cyber Security?

First of all, banks need to take a series of measures to ensure cyber security. Banks should increase these measures or develop the techniques they use together with the developing technology. Here on the security measures to follow closely the developments in Turkey and the world could be useful. Banks can make an assessment of these risks first and prevent any attack by investing in cyber security. Banks should perform various safety tests at regular intervals. They also apply a variety of tests to identify security vulnerability; they should then take a different precaution against any security breaches that may arise.

To summarize, the measures taken by banks to ensure such security are not sufficient. It is also important that people do not share their password and security information with anyone. In order to provide reasonable assurance against phishing the following measure are strongly recommended:

- Do not open any link that you are not sure of the source
- Do not share your password and financial information with anyone who reaches you by phone, short message service (SMS) or email, regardless of any information.
- Check if any campaign content belongs to the relevant brand, from the brand's original and trusted internet address.
- Make sure that the link used is exactly the same as the original and trusted Internet address of the relevant brand.
- Do not reply to emails and sites that ask for your personal information, even if the bank logo and name are used.

REFERENCES

A.R. Flo, A. Josang, (2009). “Consequences of BOTNETs Spreading to Mobile Devices”, 14th Nordic Conference on Secure IT Systems, Oslo,

Arachchilage NAG, Love S, Beznosov K. (2016). Phishing threat avoidance behaviour: An empirical investigation. Computers in Human Behavior, 60, 185-197.

Balk R, Yap BK, Loh C, Wong HD. (2009). To trust or not to trust: the consumer's dilemma with e-banking. Journal of Internet Business, 6,1-27.

Chaudhry JA, Chaudhry SA, Rittenhouse RG. (2016). “Phishing Attacks and Defenses”. International Journal of Security and Its Applications, 10, 247-256.

Chiu CL, Chiu JL, Mansumitrchai S. (2016). Privacy, security, infrastructure and cost issues in internet banking in the Philippines: initial trust formation. International Journal of Financial Services Management, 8, 240-271.

Damodaram R. (2016). “Study on phishing attacks and anti-phishing tools”. International Research Journal of Engineering and Technology, 3.

Ekawade S, Mule S, Patkar U. (2016).” Phishing Attacks and Its Preventions”. Imperial Journal of Interdisciplinary Research, 2.

Eze CU, Yih CG, Ling NT, Gan G. (2008). “Phishing: a growing challenge for Internet banking providers in Malaysia”. Communications of the IBIMA, 5, 133-142.

Iclarified, (2016), “İnternet: Worldwide Smartphone Growth Goes Flat in Q1 2016”, Apple Market Share Drops to 15.3%, http://www.iclarified.com/54990/worldwide-smartphone-growthgoes-flat-in-q1-2016-apple-market-share-drops-to-153-chart , 17.02.2017.

Jolly V. (2016). “The Influence of Internet Banking on the Efficiency and Cost Savings for Banks’ Customers”. International Journal of Social Sciences and Management, 3, 163-170

K. D. Mitnick and W. L. Simon, “The Art of Deception: Controlling the human element of security”. Wiley Publishing Inc, 2002

Konoth RK, van der Veen V, Bos H. (2016). “How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication”. In Proceedings of the 20th International Conference on Financial Cryptography and Data Security.

Leukfeldt ER, Kleemans ER, Stol WP. (2016). Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks. British Journal of Criminology, 9.

M. Alnatheer and K. Nelson, "A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context,” in 7th Australian Information Security Management Conference, 2009, no. December, pp. 1-3.

Masum E., Samet R, (2018) “*Mobil BOTNET ile DDoS Saldırısı*” Bilişim Teknolojileri Dergisi, CİLT: 11, SAYI: 2, DOI: 10.17671/gazibtd.306612

Mishra R. (2016). “Review: Phishing Attack Types & Preventive Measures”. Imperial Journal of Interdisciplinary Research, 2.

Razak LT. (2016). “The Effect of Security and Privacy Perceptions on Customers' Trust to Accept Internet Banking Services: An Extension of TAM" Mohammed A. Al-Sharaf,“Ruzaini A. Arsha," Emad Abu-Shanab and “Nabil Elayah" Faculty of Computer Systems and Software Engineering, UMP. Journal of Engineering and Applied Sciences, 100, 545-552.

S. Defuel, (2003), "Information Security Culture -From Analysis to Change,” South African Compute. J., vol. 21, pp. 46-52, 2003.

Salami Fraud by M. E. Kabay, (2006). “Computer Information Systems”, PhD, CISSPAssociate Professor, Norwich University, Northfield VT

Swanink R, Poll E, Schwabe P(2016). “Persistent effects of man-in-the-middle attacks”, 23-32.

TBB, (2015), “Bankacılıkta Dolandırıcılık Eylemleri Tespit Ve Önleme Yöntemleri”, İSTANBUL, https://www.tbb.org.tr/gec/KTPV14.pdf

Vaciago G, Ramalho DS. (2016). “Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings”. Digital Evidence & Elec. Signature L. Rev., 13, 88.