Avrupa Bilim ve Teknoloji Dergisi
Sayı 31 (Ek Sayı 1), S. 982-985, Aralık 2021
© Telif hakkı EJOSAT'a aittir
Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
No. 31 (Supp. 1), pp. 982-985, December 2021
Copyright © 2021 EJOSAT
Research Article

Electronic Banking (e-Banking) Fraud with Phishing Attack Methods

Ilker Kara[1*]

[1*] Çankırı Karatekin Üniversitesi, Eldivan Tıbbi Hizmetler ve Sağlık Meslek Yüksek Okulu, Çankırı, Türkiye (ORCID: 0000-0003-3700-4825), karaikab@gmail.com

(First received 30 September 2021 and in final form 3 November 2021)

(**DOI:** 10.31590/ejosat.1002963)

ATIF/REFERENCE: Kara, İ. (2021). Electronic Banking (e-Banking) Fraud with Phishing Attack Methods. *European Journal of Science and Technology*, (31), 982-985.

Abstract

Every segment of the society was affected with the developments in technology, though it has empowered financial activities to be carried out quickly in the internet environment. Banking service, is one of the sectors with the most exhaustive use of technology, which have turned their services into online applications in order to respond quickly to the demands of individuals, commercial companies and to get more shares from the market area in an environment of economic competition. Although this innovation offers many advantages but it has also created many damsel for mischievous people. The most popular and well known outbreaks is phishing. Phishing attacks were designed to obtain a target person's key information, such as their password or credit card. For phishing attacks, fake web pages such as e-mail services, official institution web pages, banks, social media sites are organized and victims are expected to fall into this trap. Due to the high success rate of phishing attacks and the simplicity of preparation, attackers often resort to this method to achieve their goals. Even though security measures continue to be taken to battle this crime, the size of the threat continues to increase day by day. In this study, a forensic analysis of a Phishing attack case sample prepared using electronic banking (e-banking) fake website is performed. Detailed information about the fake website prepared from the analysis results was obtained and information about the attacker was obtained. It is evaluated that the approach and results used in the study will contribute to both the fight against this crime and future studies.

Keywords: Phishing Attack, E-Banking, Computer Forensic

Oltalama Saldırı Yöntemiyle Elektronik Bankacılık (e-Bankacılık) Dolandırıcılığı

Öz

Teknolojide yaşanan gelişmeler toplumun her kesimini etkilemesiyle birlikte özellikle finansal faaliyetleri internet ortamında hızlı bir şekilde yapılmasına olanak sağlamıştır. Teknolojik kullanımının en yoğun olduğu sektörlerin başında gelen bankacılık hizmetleri bireylerin ve ticari firmaların taleplerine hızlı cevap verebilmek ve ekonomik rekabeti ortamında pazar alanından daha fazla pay alabilmek için sundukları hizmetleri çevrimiçi uygulamalar haline getirmişlerdir. Bu getirilen yenilik birçok avantajı sunmakla birlikte kötü niyetli kişiler içinde yeni fırsatlar yaratmıştır. Bu saldırıların en popüler olanı otalama (Phishing) olarak bilinen türüdür. Phishing, hedefteki kişinin şifresini veya kredi kartı gibi önemli bilgilerini ele geçirmek öğrenmek için tasarlanmış saldırılardır. Phishing saldırıları için e-posta servisleri, resmi kurum web sayfaları, bankalar, sosyal medya siteleri gibi sahte web sayfaları düzenlenmekte ve mağdur kişilerin bu tuzağa düşmesi beklenmektedir. Phishing saldırıları yüksek başarı oranı ve hazırlanışı basit olması nedeniyle saldırganlar amacına ulaşmak için sıklıkla bu yönteme başvurmaktadır. Bu suçla mücadele edebilmek için güvenlik tedbirleri alınmaya devam edilse de tehdittin boyutu her geçen gün artmaya devam etmektedir. Bu çalışmada, elektronik bankacılık (e-bankacılık) sahte web sitesi kullanılarak hazırlanmış bir Phishing saldırı vaka örneğinin adli analizi yapılmıştır. Analiz sonuçlarından hazırlanan sahte web sitesi hakkında detaylı bilgiler elde edilmiş olup saldırgana ait bilgilere ulaşılmıştır. Çalışma kullanılan yaklaşım ve sonuçlarıyla, gerek bu suçla mücadeleye gerekse gelecekte yapılacak çalışmalara katkı sağlayacağı değerlendirilmiştir.

Anahtar Kelimeler: Oltalama Saldırısı, e-Bankacılık, Adli Bilişim

[*] Corresponding Author: karaikab@gmail.com

1. Introduction

Phishing attacks are one of the oldest and most successful types of cyber-attacks that have been used since the use of internet-based web applications [1]. As the name suggests, in this attack, the attacker prepares a "bait" and waits for "fish" to be attached to this dish. In general, phishing attacks reach their victims via fake web pages or an e-mail containing malicious software [2]. It is designed to capture important information such as the identity information of the target person, phone or credit card, by imitating a corporate web page or sending e-mails that arouse curiosity and interest to the user such as gifts and discounts [3]. Web pages or e-mails are specially designed by the attacker so that the victim who falls into this trap feels safe during his transactions [4]. When the malicious links in the e-mail attachment reaching the victim or the links in the fake websites are clicked, the victim can be hunted, and the victims' computers can be captured by the attackers by running the infected files from the e-mails or malicious links on the web pages [5].

In another method, the attackers imitate a cleverly designed corporate website [6]. While preparing these fake websites, it gives the impression that it is operating on the corporate website at first glance by using images such as themes, pictures, tables or logos on the target site. Moreover, it can add some applications of the website it imitates to the fake website, and if the victim clicks on these links, it can redirect to the page of the corporate site. This situation is a complete deception. After establishing the trust of the victim, it directs the victim to enter the necessary information in the form on the fake website in order to win the transaction he wants to do or the reward or discount he promised. When the attack is completed, the information entered in the forms on the fake website is transmitted to the attacker. With this information obtained after the attack, it can perform banking transactions, empty the victim's accounts or sell this information to malicious people.

Although new methods have been developed to combat phishing attacks in researches from past to present, the number of victims of phishing attacks is increasing rapidly [7]. This is triggered by the simple preparation of the phishing attack, the high success rate and the low probability of catching the attacker. Forensic analysis has an important place in the fight against phishing attacks. As a result of forensic analysis, the attack strategy of the attacker can be determined, the websites prepared for the attack can be analyzed in detail, the preparation and working mechanism of these sites can be defined and the information of the attacker can be accessed [8].

Considering all these, in this study, forensic analysis of the website prepared for phishing attacks has been examined. This study mainly offers three contributions:

1. Attack strategy of the attacker,
2. Study, forensic analysis of e-banking website prepared for phishing attacks,
3. The results obtained from the sample case analysis selected in the study were evaluated.

This study is organized as follows: in section 2, a few of the relevant studies from the literature are reviewed. Part 3 conducted e-banking Phishing attack case forensic analysis. In the next section, forensic analysis used in 4 studies is evaluated. Finally, chapter 5 completes the work and evaluations are made to combat possible future Phishing attack.

2. Related Work

Although there has been work in the field of e-banking Phishing attack detection and analysis in the literature, this chapter is briefly reviewed focusing on some of the important ones.

While the attacker designs completely identical visually to the sites, impersonating in the web-based Phishing attack, he makes small changes that will not be noticed at first sight. In this method, known as name shuffle, some characters are used interchangeably (instead of the letter h or a instead of the letter o). This information is used in e-banking Phishing attack detection. Especially studies using the artificial intelligence approach are promising.

Machine learning algorithms are widely used in Phishing attack detection. Zhang et al (2007) developed a model called CANTINA to detect keywords from URLs and HTML of websites [9]. In the results of the study, it was seen that it could detect 95% of websites designed for phishing attacks. Marchal et al (2014) proposed a model that takes advantage of URLs and Html features. This model has also removed 212 features of URL and HTML [10]. This model has used machine learning algorithms to determine whether a Phishing website is by manually extracting the features of websites. As a result of the study, it was concluded that the proposed model was 94.91% successful. Huang et al. (2019) used the Convolutional Neural Network (CNN) module to determine the URL character indexes of suspicious websites [11]. In the study, a data set consisting of 4.8 million URL addresses was used and they achieved a success close to 99%. In a similar study, Xiao et al. (2020) detected Phishing attacks at a high accuracy rate of 99.84% using a multi-layer sensor (MLP) in their study using the Convolutional Neural Network (CNN) module [12]. It is important to work on the detection and prevention of website-based Phishing attacks. Forensic analysis to be made after the phishing attack has an important place in detecting the criminals. In addition, forensic case analysis of website-based Phishing attacks;

It can provide access to important information such as attack strategies, determination of the techniques used and tracking the attacker. For this reason, case studies are critical to combating Phishing attacks.

3. Materials and Methods

In this section, the case example prepared for website-based phishing attacks and the business computer and analysis tools used in the analysis are introduced.

3.1. Dataset

In case analysis studies, it is extremely important that the selected sample is current and fully covers the problem. In doing so, an appropriate case for information security cooperation with companies operating in Turkey for example has been supplying one of the most recent examples.

3.2. Preparation of Analysis Environment

All analyzes were performed on a Lenovo V530 Intel Core i7 7500 U working computer with 128 GB + 512GB SSD and Windows 10 Pro operating system. Analyzes were performed using "HTTrack Website Copier 3. 49.2 (Free version)", "Wireshark 3.4.3 (Free version)". Since the sample analyzed is a real cyber-attack and forensic case, some information is presented in the study in disguise.

3.3. Forensic Case Analysis

In the analyzed example, cyber fraudsters were designed to direct customers to the bank's official websites and the website they set up, and to enter the information in the form on the fake website (Figure 1).

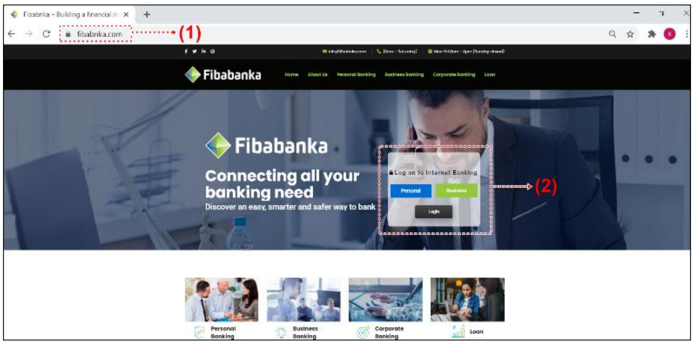
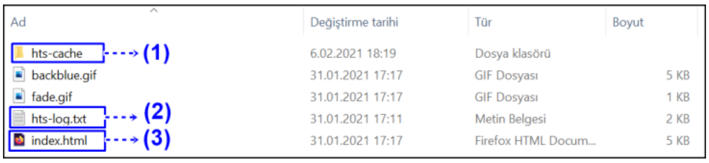

fibabnka.com
(1)
Fibabanka
Home About Us Personal Banking Business Banking Corporate Banking Loan
Fibabanka
Connecting all your banking need
Discover an easy, smarter and safer way to bank
Log on to Internet Banking
Personal
Business
Login
(2)
Personal Banking
Business Banking
Corporate Banking
Loan

Figure 1. Screenshot of the website prepared for phishing attacks.

Figure 1 shows the web site home screen page and its contents prepared for phishing attacks. While preparing the offensive Phishing website, it is seen that a corporate bank completely copied its content. (1) The website domain name prepared by the attacker can be seen. When preparing the domain name, when looking carefully at the domain address designed as "https://fibabnka.com/", it was used in "fibabnka.com" instead of "fibabanka". So it can be seen that the letter "a" is missing. With this method, the attacker aims to avoid the attention of careless users. (2) It shows the prompting message for the victim to enter the personal and banking information in the prepared form.

HTTrack Website Copier is a website copying tool that enables the entire target website to be downloaded to the computer and enables the downloaded website to be viewed offline [13]. In order to examine the content of the suspect "https://fibabnka.com/" web site, HTTrack Website Copier 3.49-2 was downloaded to the business computer and the content of the suspect site was reached (Figure 2).

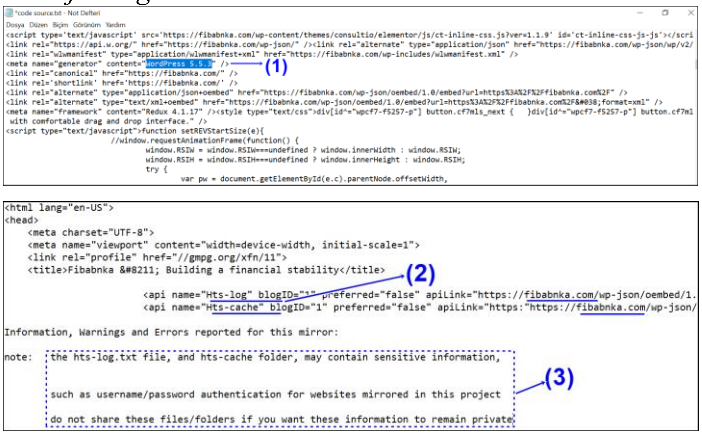


Ad	Değiştirme tarihi	Tür	Boyut
hts-cache (1)	6.02.2021 18:19	Dosya klasörü	
backblue.gif	31.01.2021 17:17	GIF Dosyası	5 KB
fade.gif	31.01.2021 17:17	GIF Dosyası	1 KB
hts-log.txt (2)	31.01.2021 17:11	Metin Belgesi	2 KB
index.html (3)	31.01.2021 17:17	Firefox HTML Docum...	5 KB

Figure 2. "https://fibabnka.com/" website content screenshot.

Figure 2 shows the content of the website "https://fibabnka.com/". (1) The hts-cache (historical traffic search-cache) folder contains the HTML pages, images and documents of the suspect https://fibabnka.com/ web page. (2) The "hts-log" file shows the records where the information the victims entered into the form is kept. (3) The "index" icon is downloaded and provides offline access to the content of the suspect https://fibabnka.com/ website.

The source code content was analyzed in order to examine the content and source code architecture of the website "https://fibabnka.com/" and to find more information about the website (Figure 3).


*code source.txt - Not Defteri
Dosya Düzen Biçim Görünüm Yardım
(1)
(2)
(3)

```
<script type='text/javascript' src='https://fibabnka.com/wp-content/themes/consultio/elementor/js/ct-inline-css.js?ver=1.1.9' id='ct-inline-css-js-js'></scri
<link rel="https://api.w.org/" href="https://fibabnka.com/wp-json/" /><link rel="alternate" type="application/json" href="https://fibabnka.com/wp-json/wp/v2/
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="https://fibabnka.com/wp-includes/wlwmanifest.xml" />
<meta name="generator" content="WordPress 5.5.3" />
<link rel="canonical" href="https://fibabnka.com/" />
<link rel='shortlink' href='https://fibabnka.com/' />
<link rel="alternate" type="application/json+oembed" href="https://fibabnka.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Ffibabnka.com%2F" />
<link rel="alternate" type="text/xml+oembed" href="https://fibabnka.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Ffibabnka.com%2F&#038;format=xml" />
<meta name="framework" content="Redux 4.1.17" /><style type="text/css">div[id^="wpcf7-f5257-p"] button.cf7mls_next {   }div[id^="wpcf7-f5257-p"] button.cf7ml
 with comfortable drag and drop interface." />
<script type="text/javascript">function setREVStartSize(e){
                        //window.requestAnimationFrame(function() {
                                window.RSIW = window.RSIW===undefined ? window.innerWidth : window.RSIW;
                                window.RSIH = window.RSIH===undefined ? window.innerHeight : window.RSIH;
                                try {
                                        var pw = document.getElementById(e.c).parentNode.offsetWidth,
```

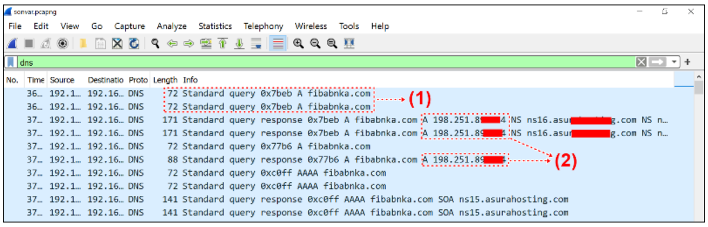
```
<html lang="en-US">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="profile" href="//gmpg.org/xfn/11">
    <title>Fibabnka &#8211; Building a financial stability</title>

                        <api name="Hts-log" blogID="1" preferred="false" apiLink="https://fibabnka.com/wp-json/oembed/1.
                        <api name="Hts-cache" blogID="1" preferred="false" apiLink="https:"https://fibabnka.com/wp-json/

Information, Warnings and Errors reported for this mirror:

note:   the hts-log.txt file, and hts-cache folder, may contain sensitive information,


        such as username/password authentication for websites mirrored in this project

        do not share these files/folders if you want these information to remain private
```

Figure 3. Screenshot of part of the source code architecture of the "https://fibabnka.com/" website.

When the suspicious "https://fibabnka.com/ website's content and source code architecture were examined, it was seen that the website was prepared using" Word Press ". (2) The home page address of your website shows the access link. (3) The folder where the website's records are kept. The log records of web sites are important in forensic analysis as they contain very valuable information. (3) In order to keep the information kept in the "hts-log" folder confidential (such as username / password authentication), this file should not be shared with other people. It is seen that it was made.

After the forensic investigation of the suspicious website content is completed, the focus is on accessing the information of the attacker. IP (Internet Protocol) is the address used by devices that are in data exchange with each other with the Internet network or any other computer network. Internet-based devices can thus detect each other's access addresses. Detecting the IP number of the suspicious website is one of the methods used to reach the attacker in forensic investigations. If the suspicious IP number can be detected, the internet subscriber to whom the IP number has been allocated can be determined. If this information is available, it can also allow the attacker to be traced.

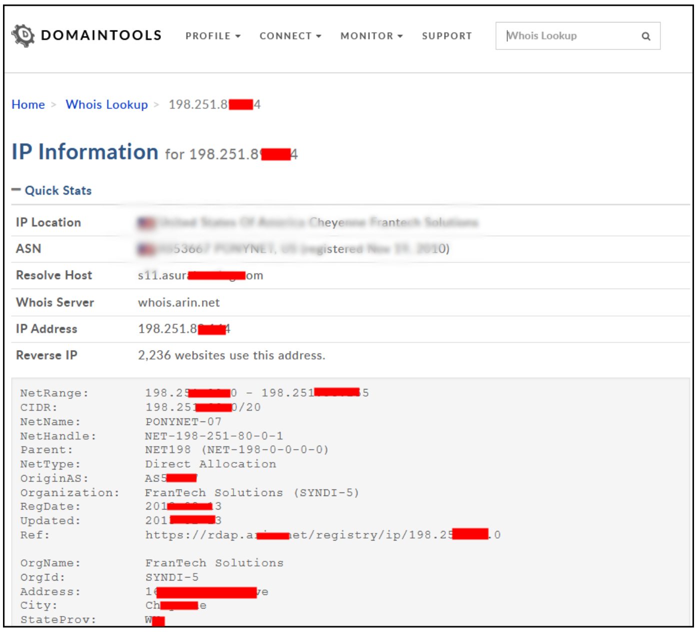
Wireshark program is an open source internet and network packet analyzer. Thanks to the Wireshark program, it is used for the detection of the IP number of the suspicious website and for forensic investigations. The network traffic of the website "https://fibabnka.com/" was analyzed using the Wireshark program. Since the Wireshark program will display all internet and network packet traffic on the computer on which it is running, only the suspicious "https://fibabnka.com/" website is entered and the internet and network packet traffic about this site is filtered (Figure 4).


sonvar.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
(1)
(2)

```
No.  Time Source  Destinatio Proto Length Info
     36…  192.1…  192.16…  DNS     72 Standard query 0x7beb A fibabnka.com
     36…  192.1…  192.16…  DNS     72 Standard query 0x7beb A fibabnka.com
     37…  192.1…  192.16…  DNS    171 Standard query response 0x7beb A fibabnka.com A 198.251.8[redacted]4 NS ns16.asu[redacted]g.com NS n…
     37…  192.1…  192.16…  DNS    171 Standard query response 0x7beb A fibabnka.com A 198.251.89[redacted]4 NS ns16.asu[redacted]g.com NS n…
     37…  192.1…  192.16…  DNS     72 Standard query 0x77b6 A fibabnka.com
     37…  192.1…  192.16…  DNS     88 Standard query response 0x77b6 A fibabnka.com A 198.251.89[redacted]4
     37…  192.1…  192.16…  DNS     72 Standard query 0xc0ff AAAA fibabnka.com
     37…  192.1…  192.16…  DNS     72 Standard query 0xc0ff AAAA fibabnka.com
     37…  192.1…  192.16…  DNS    141 Standard query response 0xc0ff AAAA fibabnka.com SOA ns15.asurahosting.com
     37…  192.1…  192.16…  DNS    141 Standard query response 0xc0ff AAAA fibabnka.com SOA ns15.asurahosting.com
```

Figure 4. Screen shot of "https://fibabnka.com/" site IP number detection with Wireshark program.

Figure 4 shows the IP number detection of the "https://fibabnka.com/ site" with the Wireshark program. (1) Shows the suspect domain name searched. (2) The suspect site "https://fibabnka.com/" The IP number is visible. After the suspect IP number was detected, the information regarding the IP number was searched at "https://whois.domaintools.com" (Figure 5).



Home > Whois Lookup > 198.251.8[redacted]4

IP Information for 198.251.8[redacted]4

— Quick Stats

IP Location	[redacted]
ASN	[redacted]
Resolve Host	s11.asur[redacted]om
Whois Server	whois.arin.net
IP Address	198.251.8[redacted]4
Reverse IP	2,236 websites use this address.

```
NetRange:       198.25[redacted]0 - 198.251[redacted]5
CIDR:           198.25[redacted]0/20
NetName:        PONYNET-07
NetHandle:      NET-198-251-80-0-1
Parent:         NET198 (NET-198-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS5[redacted]
Organization:   FranTech Solutions (SYNDI-5)
RegDate:        201[redacted]3
Updated:        201[redacted]3
Ref:            https://rdap.a[redacted]et/registry/ip/198.25[redacted].0

OrgName:        FranTech Solutions
OrgId:          SYNDI-5
Address:        1[redacted]e
City:           Ch[redacted]e
StateProv:      W[redacted]
```

Figure 5. Screen shot of "https://whois.domaintools.com" query of detected suspect IP number.

As a result of the query of the detected suspicious IP number, it could be seen that the information of the attacker could be accessed.

4. Discussion and Conclusion

In this study, a forensic case analysis of the e-banking website prepared for phishing attacks was made. The attack strategy and the methods used by the attacker were examined on a real attack example. Analysis results offer three important advantages such as (1) the working logic of the e-banking website prepared for phishing attacks, (2) the strategy of the attack, and (3) the ability to trace the information of the attacker. However, the Phishing attack case analysis includes some difficulties. Since the phishing attack can use different designs according to the fiction chosen, the detection and analysis approach may differ depending on the case, although it is similar to the other attack examples. For this reason, forensic case studies make a great contribution to the work done in this field and the fight against phishing attacks. Although there are many studies in the literature to detect fake websites designed for phishing attacks, it is seen that new strategies have been developed to circumvent these methods recommended by attackers. For example, for approaches based on the detection of suspicious URL information, attackers hide this information from fake websites they create [13]. This situation causes great difficulties in combating phishing attacks.

For these reasons, we believe that the forensic analysis proposed in the study needs to be repeated with more up-to-date examples to reinforce and support it. Finally, we believe the study will raise awareness in combating e-banking websites designed for phishing attacks. As a future study, we plan to investigate with different sample data sets in the detection and analysis of the e-banking website prepared for phishing attacks.

References

[1] Ghazi-Tehrani, A. K., & Pontell, H. N. (2021). Phishing Evolves: Analyzing the Enduring Cybercrime. Victims & Offenders, 16(3), 316-342.

[2] Kara, I. (2021). Don't Bite The Bait: Phıshıng Attack for Internet Bankıng (e-bankıng). 16(5), 1-12.

[3] Hajiali, M., Amirmazlaghani, M., & Kordestani, H. (2019). Preventing phishing attacks using text and image watermarking. Concurrency and Computation: Practice and Experience, 31(13), e5083.

[4] Kara, İ. (2020). Security Risks and Safeguard Measures in Social Media Usage. Avrupa Bilim ve Teknoloji Dergisi, 10-15.

[5] Kara, I. (2019). A basic malware analysis method. Computer Fraud & Security, 2019(6), 11-19.

[6] Subasi, A., & Kremic, E. (2020). Comparison of adaboost with multiboosting for phishing website detection. Procedia Computer Science, 168, 272-278.

[7] Jain, A. K., & Gupta, B. B. (2018). Two-level authentication approach to protect from phishing attacks in real time. Journal of Ambient Intelligence and Humanized Computing, 9(6), 1783-1796.

[8] Kara, I. (2021). Cyber-Espionage Malware Attacks Detection and Analysis: A Case Study. Journal of Computer Information Systems, 1-18.

[9] Zhang, Y., Hong, J. I., & Cranor, L. F. (2007, May). Cantina: a content-based approach to detecting phishing web sites. In Proceedings of the 16th international conference on World Wide Web (pp. 639-648).

[10] Marchal, S., François, J., State, R., & Engel, T. (2014). PhishStorm: Detecting phishing with streaming analytics. IEEE Transactions on Network and Service Management, 11(4), 458-471.

[11] Huang, Y., Yang, Q., Qin, J., & Wen, W. (2019, August). Phishing URL detection via CNN and attention-based hierarchical RNN. In 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 112-119). IEEE.

[12] Xiao, X., Zhang, D., Hu, G., Jiang, Y., & Xia, S. (2020). CNN–MHSA: A Convolutional Neural Network and multi-head self-attention combined approach for detecting phishing websites. Neural Networks, 125, 303-312.

[13] Chowdhury, T., & Vidalis, S. (2012, September). Collecting evidence from large-scale heterogeneous virtual computing infrastructures using Website Capture. In 2012 Third International Conference on Emerging Intelligent Data and Web Technologies (pp. 211-217). IEEE.