Intelligence Report and the Analysis Against the Phishing Attack Which Uses a Social Engineering Technique

Dong Hwi Lee, Kyong Ho Choi, and Kuinam J. Kim*

Dept. of Information Security Kyonggi University
71 Chungjung-Ro, Sedaemun-Gu Seoul, Korea
dhclub@naver.com, econckh@kyonggi.ac.kr
harap123@daum.net

Abstract. The hacking aspect of recent times is changing, the phishing attack which uses a social engineering technique is becoming the threat which is serious in Information Security. It cheats the user and it acquires a password or financial information of the individual and organization. The phishing attack uses the home page which is fabrication and E-mail, and acquires personal information which is sensitive and financial information. This study proposes the establishment of National Fishing Response Center, complement of relation legal system, Critical intelligence distribution channel of individual and enterprise.

Keywords: Social engineering, Phishing, Security Mechanism.

1 Introduction

With the progresses of the information society and introduction of the ubiquitous environment, active networking is creating enormous wealth in the 21st century. However, various side-effects of informatization are also evident, such as hacking incidents in internet banking, data leakage in individuals and in public and private sectors and proliferation of various worms and viruses. What is more unsettling is the fact that in recent cyber-attacks, the number of cyber-crimes that cause financial damage are on the rapid increase. Such attacks threatening the cyberspace are becoming more and more integrated and sophisticated.

Internet phishing is among such changed pattern of cyber-attacks involving social engineering techniques. Accordingly, more systemic and integrative countermeasures are wanted. In this research, the evolving threats in cyberspace shall be examined and among them, statistical data on domestic and international internet phishing attacks, which involves social engineering, will be collected. In order to analyze the security demands in a more specific and detailed manner, real incidents of internet phishing attacks will be studied. Also, in order to understand the techniques in more detail, technical countermeasures currently employed domestically and internationally will be surveyed. Defense measures against phishing that suits the domestic context will be suggested.

* Corresponding author.

O. Gervasi and M. Gavrilova (Eds.): ICCSA 2007, LNCS 4706, Part II, pp. 185–194, 2007.

2 Incidents of Phishing and Statistic Analysis

2.1 Domestic and International Phishing Attack Incidents

The eBay incident in 2003 is one of the most well-known phishing attack incident abroad. The attackers falsely identified themselves as eBay and randomly sent e-mails that said, "due to security threat, your account is on temporary suspension" and "click the link to eBay homepage and re-enter your personal details". The victims followed the directions and had their credit card numbers, social security number and other personal information stolen.

Domestically, there was a financial fraud using loans as bait. The phishers posted articles on well-known Korean portal sites saying that "anyone who has more than 10 million in bank balance can have loans as much as 100 million". When the victims contacted the phishers, saying that they have to verify the identification of the contacting person, told them to connect to a prepared hoax web-site. Seeing the outlay of the web-site was similar to the web-sites of other banks, the victims inputted their personal information without doubting. When the security card codes did not match, the phishers called the victims guising as bank clerks to confirm the codes. From 12 victims, 120 million were stolen.

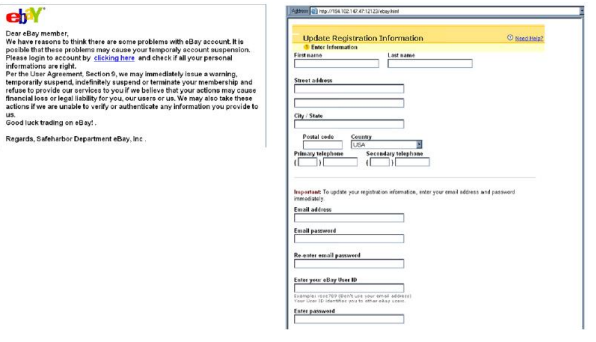

Fig. 1. Phishing attack using false identity as eBay[1]

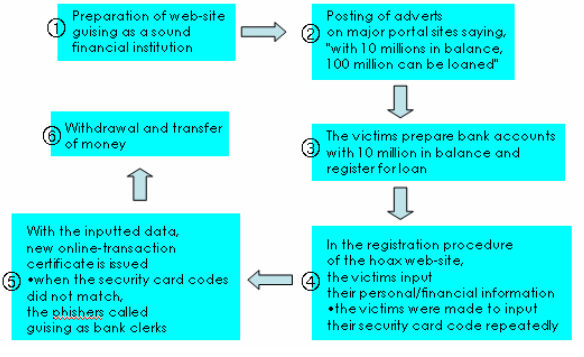

Fig. 2. Financial fraud using loans as bait[2]

2.2 Phishing Attack Statistics Domestically and Internationally

According to Anti-Phishing Working Group (APWG), the number of reported phishing attacks in the world increased from 6,957 in October of 2004 to 26,150 in August of 2006. The area of business that experienced the most number of phishing was finance sector which received 92.6% of all the phishing incident. ISP was 1.4% and retails was 4.1%.

According to statistics by Krcert/cc, the number of reported domestic phishing incidents was 1,087 in 2005 and the number in 2006 was at 986 in September of that year. The number of phishing web-sites found in the month of September that year reached 97.

The magnitude of recorded damage caused by phishing vary according to different research bodies due to reasons such as: reluctant financial institutions who avoid official announcement of phishing damage and the lack of awareness about damages caused by phishing. Ponemon estimates that the financial loss caused by phishing will reach $500 billion in the US alone. Gartner Group estimates that 2.4 million internet users were victims of phishing in the year of 2004 alone and the resulting financial damage would reach $1 trillion. According to APWG, the number of phishing attacks is increasing by the rate ot 50% every month. APWG also estimates that, due to

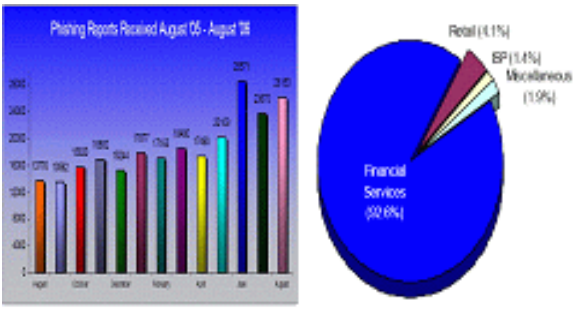

Fig. 3. Statistics on domestic and international phishing[5]

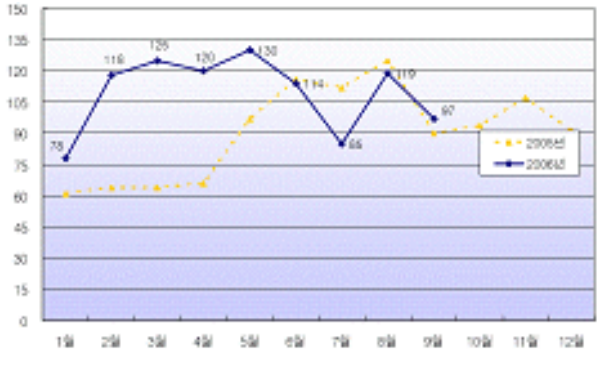

Fig. 4. Statistics on domestic phishing[6]

sophistication of phishing attacks, about 5% of users reply to phishing e-mails[1]. In view of such attack incidents and statistics, the dangers of phishing is increasing credibly. However, the level of awareness among internet users on the methods and sophistication of phishing is still insufficient.[3][4] Hence the danger of falling victim of phishing is very high.

According to domestic and international statistics, the number of phishing attacks is continually increasing and such problem does not stay exclusive of the borders of a country. In the early days of phishing, the e-mails were mainly in English and hence the number of domestic damage was low. But recently, phishing attacks are using web-sites with multilingual support[7] and hence it must realized that the problem of phishing is a worldwide one. Adequate countermeasures are needed.

3 Phishing Countermeasure Technique

Phishers use numerous techniques and methods to lure the victim to extract internet users' data. They combine technical methods and social engineering user deception - in other words, trickery - to execute their attack. The best technical defense mechanism against phiching would combine user-approach defense and defense on servers.

3.1 User-Approach Defense

As for the general internet user, defense against phishing attack remains very weak. This is due to the lack of awareness on the threats and lack of preparation of defense measures. Hence security organizations and social organizations are trying to provide education on various defense techniques so that the users will be more aware of phishing attacks. Such effort aims to reduce the numnber of phishing victims. The methods used are as follows:

- Blocking function in internet browser
- Blocking of advertisement e-mails
- Providing examples of phishing incident and statistics
- Adding electronic signature function in e-mails
- Notification of general security measures to be followed

3.2 Server-Level Defense

Corporations and organizations that provide their services mainly through the cyberspace are trying to materialize phishing defense techniques that will protect resources under their possession. Hence they are making efforts to educate the threats of phishing and to develop internal operations and techniques that will eliminate the causes of phishing. Here, the following methods are used:

- Distributing educatory materials on phishing incidents and damages
- Introducing corporate policy on protection of attacks
- Pre-verification on channels of data-flow between companies
- Verifying e-mails and introducing electronic signatures

- Developing web-application program for security
- Use of powerful certification system
- Protection of router and gateway
- Supervision of domain

Defense techniques currently being used against social engineering-based phishing attacks are web-site verification, verifying mail servers, electronic signature and others. The patent on mechanism that defends phishing attacks through URL spoofing has been made public. Also, world-wide corporations such as Google, G-Mail and Microsoft are providing means to protect their customers from phishing attacks.

Regardless of such defense efforts, there remains many issues that have to be death with. Firstly, the delivery of information on incidents and statistics is rather unilateral. It has been assessed that the general users' level of awareness of social engineering-based phishing is very low. This reveals the fact that education and publicity activities of public organizations and security companies are insufficient. Also, due to differences in internet environments of different countries, the patterns of phishing are different from country to country. Hence there is the need to analyze cases to create detailed defense measures.

Secondly, development of client-based security programs that can easily be used by general users is necessary. Although today's society is a information society, for the general user, it is difficult to comprehend the vastness and 'faceless' and anonymous nature of the cyberspace. Such circumstance calls for a safe web surfing program which operates taking consideration of the users' perspective. Through this, an environment should be created in which the security policies and guidelines are not 'handed down' from the center but the user themselves can identify and acquire information with ease.

Development of such technique can provide the foundation on which safe cyberspace can thrive even after hacking method expands from social engineering-based phishing to pharming, XSS, ActiveX, vishing and others. Particularly, with the forecast that the number of social engineering-based hacking will increase using loopholes in the security, the importance of building sound defense system is bigger than ever.

4 Technical Defense Measures

4.1 Reverse DNS Data Extraction

In reverse DNS, when the investigator asks to check, data extraction from initial database is attempted and when the searched data is not in the database, the data is obtained by connecting to paid Reverse DNS site. Such process is aimed to obtain newly created DNS data and to update the existing data.

The possibility of not finding the searched data in the database should be taken into consideration and use of paid DNS sites should be supported.

When sites are connected using Java language, it can be found that there exists a common pattern in the coded passwords.

4.1.1 Automatic Connection to the Site

```
public synchronized void http********Login() throws
Exception {

//modified by khj 2007.3.20

        //URL url = new
          URL("https://www.********.com/login/");

        URL url = new URL("https","www.****
        ****.com",-1,"/login/");


          HTTPURLConnection conn = new
        HTTPURLConnection(url);

          conn.setRequestMethod("POST");

          setHttpRequestProperties(conn);

          conn.setPostProperty("email",
getLoginEmail());

          conn.setPostProperty("key",
getLoginPasswd());

        conn.setPostProperty("r",
        "http://www.********.com/members/");
```

4.1.2 Requesting Data Extraction from Site

```
public void request(String host) throws Exception {


          if(host == null || host.length() <= 0)

                    throw(new UnknownHostException());

          this.targetHost = host.trim();

          logging(targetHost, getRemoteIP());

System.out.println("*****ReverseIP-requets : " + this.targetHost );

          isIP = Util.isIPAddress(targetHost);

          try {

                    ipAddrList = Util.getAllIPAddress(targetHost);

                    for(int i=0; i<ipAddrList.size(); i++) {

                              String ip = (String)ipAddrList.get(i);

                              logger.debug(i+") IP=["+ip+"]");

System.out.println("******ReverseIP-request : " + ip );
```

```
            }
        } catch(UnknownHostException e) {
            logger.error("Unknown host error."+ e.getMessage());
        } finally {
            http******Login();
            for(int i=0; i<ipAddrList.size(); i++ ) {
                String ip = (String)ipAddrList.get(i);
                logger.debug("Target IP=["+ip+"]");
                krCollect(ip);
                ******Collect(ip);
```

4.1.3 Data Collected Through Reverse DNS

Such collected data are saved in the database through pattern-matching method.

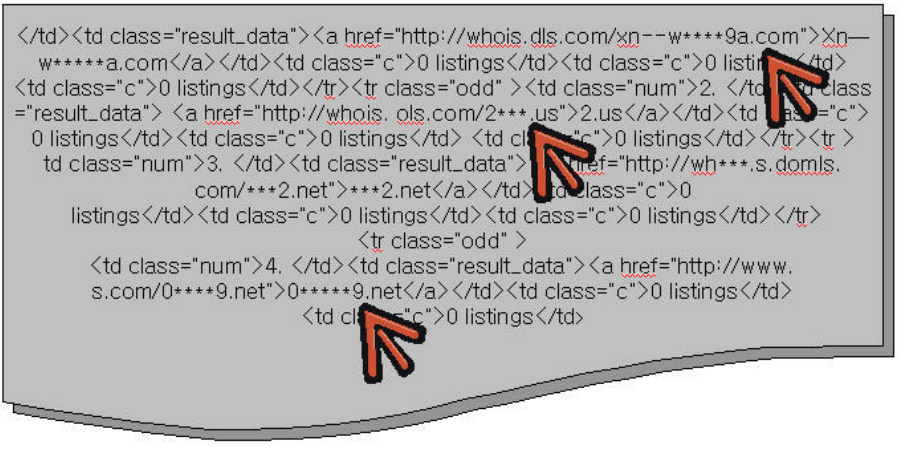

Fig. 5. Data collected through reverse DNS

4.2. National Phishing Response Center

Even though the defense technology against phishing is being developed, the number of phishing attacks using social engineering is on the increase. The threats in cyberspace are hence on the increase too and such threats should be blocked through integrated controlling via National Phishing Response Center.

National Phishing Response Center would carry out tasks such as: analysis of domestic internet environment and phishing incidents, prevention of forecastable

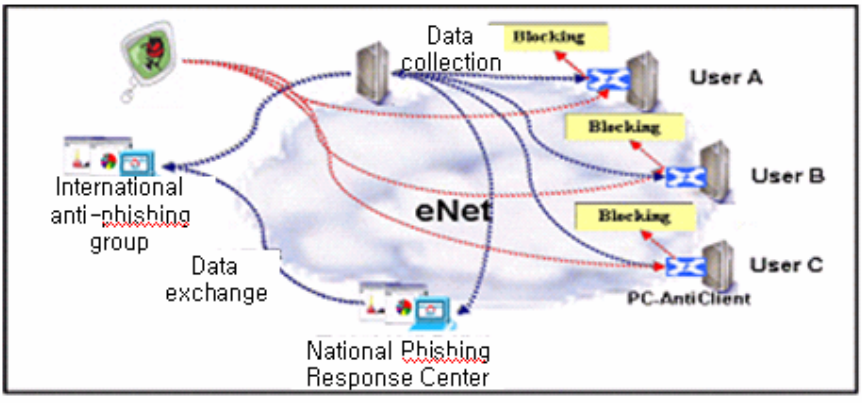

Fig. 6. National Phishing Response System

cyber-crimes, analysis of network packets and patrolling of data forging on web-servers. Such roles of the National Phishing Response Center would reduce the threats in the networking environment. Furthermore, building reverse DNS database and real-time detection of cyber-threats through central controlling of personal and other valuable data are required. Such measures shall enable quick-response system against cyber-threats. Here, in order assemble data to the central controlling body and to reduce the time gap between attack and response, secure program on clients are required. This is to prepare against the current pattern of phishing where the time-span of threat is very short of time but nonetheless inflicts extensive damage.

4.3. Client Secure Program

In order to enable integrated phishing controlling service by the National Phishing Response System, client programs are installed onto users' personal computers. The client program enables data comparison with the Center, blocks connection to the

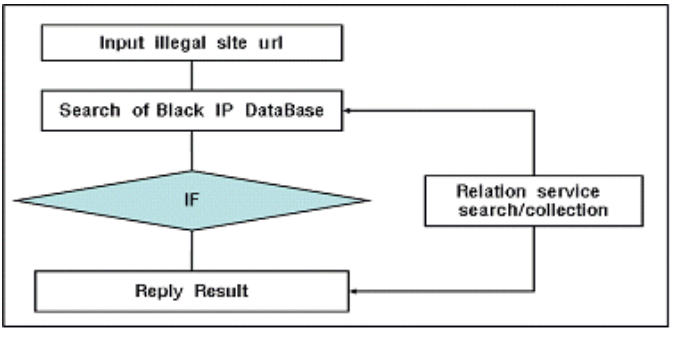

Fig. 7. Client Secure Program mechanism

phishing web-sites and allows automatic reporting. The two levels of system are connected together and enables comparison of phishing threats using database and through this, real-time threat detection and user protection is possible. Also, through automatic reporting function, secure web-surfing is provided to the users.

5 Performance Analysis

5.1. Analysis Environment

Security measures were experimented for 90 days on two large-scale networks that use speeds higher than 1G byte. In order to create uniform analysis environment, the testing was undertaken on actual operations on A-Network and B-Network of "K" organization. On A-Network, improved security measure that communicates with the National Phishing Response Center was applied and on B-Network, the existing measures were applied without modifications. Reinforcing of tested equipments and environment preparation stages were carried out for the testing. The "K" organization possesses 500 servers of various types, 10,000 client workstation-level computers and the number of internal users is 20,000.

The network had 500Mbps connection linking external network and the intranet and was multiple circuit network. At the entrance of the intranet, firewall system was positioned and beyond the firewall system, the intranet was formed. As for the structure of the intranet, server and PCs are connected, separate mail system exists in the servers and virus vaccines are installed on each PC.

The volume of traffic is large-scale, processing around 500 billion packets. At any one time, around 50,000 network sessions are connected. Lastly, as for security tools, there were 4 Giga bit Firewall systems with backup-line, 8 IDS (Sun V880), 4 Giga bit IPS, 2 VMS Servers and one ESM (Sun EMT3500).

Performance assessment and verification was conducted on the 90-day testing on networks A and B using ISAC statistics. Through the tests, the level of effectiveness of detection and blocking of phishing threats were measured.

5.2. Performance Analysis

As can be seen from the values in [Table 1], when the phishing blocking measure suggested in this paper are applied, early warning of threats is possible and consequently, adequate response can be undertaken.

Table 1. Number of detection phishing threats

	Network A	Network B
Month 1	142	15
Month 2	388	29
Month 3	289	12
Total	819	56

6 Conclusions

Phishing attacks using social engineering are becoming more sophisticated and diversified with extreme rapidity. If such proliferations of threats are left without appropriate countermeasures, dangers can spread to an extent which can shake even the foundation of electronic business. Defense measures and development of defense technology should be sought.

Systemic implementation of defense measures suggested in this paper should be headed by the government. Through such measures, the ever-present risks should be assessed and in order to reduce threats, policies and procedures should be provided. Also system should be developed which enables rapid reporting of attack incidents and provides fast and responsive directions to encountered threats.

Acknowledgments. This work was supported by a grant from Security Engineering Research Center of Korea Ministry of Commerce, Industry and Energy.

References

1. Korea Information Security Agency: The New Cyber Threat: Phishing (2005)
2. Ministry of Information and Communication republic of KOREA: Korea Information Security Agency, Guide for Phishing Prevention, online: www.boho.or.kr
3. Demopoulos Associates: User Phishing Awareness Survey (2005)
4. Princeton Survey Research Associates International: Spyware Survey Final Topline (2005)
5. Anti-Phishing Working Group: Phishing Activity Trends Report (August 2006)
6. Korea Information Security Agency: Report and Trend on Internet Incident (June 2006)
7. ahnlab spyzero, http://auction.ahnlab.com/badcode_view.asp?seq=7818