情 報 保 護 學 會 誌
第 16 卷 第 1 號, 2006. 2

사회공학적 공격방법을 통한 개인정보 유출기술 및 대응방안 분석

최 양 서*, 서 동 일*

요 약

개인정보 유출을 위한 공격이 발생하기 시작한 것은 이미 오래전이다. 이런 공격은 고도의 기술을 이용하여 사용자가 인지하지 못한 상황에서 시도되는 경우도 있었으나, 대부분의 경우, 정보보호에 대한 상식이 부족한 일반인들을 대상으로 자신의 중요 정보를 직접 제공하게 만드는 사회공학적인 공격 방법이 주류를 이루었다. 이러한 사회 공학적인 공격 방법은 비록 매우 허술해 보이지만, 해커들 사이에서는 아직까지도 가장 쉽게 정보를 획득할 수 있는 방법으로 인식되고 있다. 최근에는 피싱(Phishing), 파밍(Pharming) 등과 같은 사회 공학적인 공격 방법과, 인터넷이라는 전자 매체, 그리고, 고도의 공격 기술 등이 복합적으로 적용된 개인정보 유출 공격이 시도되고 있다. 이에 본고에서는 개인정보 유출을 위해 시도되는 공격에는 어떠한 방법들이 있는지 알아보고, 이들이 사용하는 기술적인 공격 방법에 대해 분석하며, 이를 극복하기 위한 방안에 대해 살펴보기로 한다.

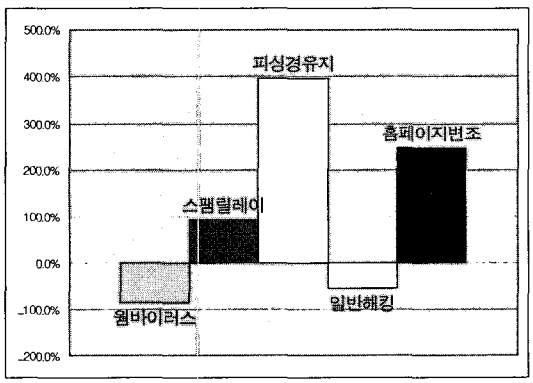
Ⅰ. 서 론

1990년대 최고의 천재 해커로 알려져 있는 케빈 미트닉은 미국 NORAD[17] 등을 해킹한 것으로 유명하다. 그러나, 케빈 미트닉은 기술적인 해킹뿐만 아니라, 사회 공학적인 방법을 가장 잘 사용한 해커로서도 매우 유명하였다. 특히, 케빈 미트닉이 몇 통의 전화만으로 모토롤라 최신 핸드폰의 핵심 소스코드를 얻어낸 것은 매우 유명한 일화이다. 10여년이 지난 지금도 사회 공학적인 방법을 통한 해킹은 여전히 가장 효과적인 해킹 방법으로 해커들 사이에 인식되고 있고, 최근에는 고도의 기술적인 해킹 방법들과 통합되어 널리 활용되고 있는 상황이다.

과거, 해커들이 해킹을 시도하는 가장 큰 목표는 자신의 실력을 과시하기 위한 것이었다. 그러나, 최근에는 정치적/사회적/경제적 이유로 해킹을 시도하기 시작하였다. 특히 정치/사회적인 이유보다 경제적인 이유로 해킹을 시도하는 경우가 크게 늘어나고 있는 상황이다.

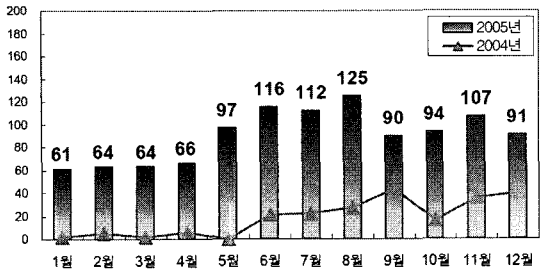
경제적인 이유로 해킹을 시도하는 경우 중 가장 널리 시도되고 있는 공격이 개인정보 유출 공격이다. 개인정보는 그 자체로 매우 높은 가격에 거래되기도 하며, 획득한 개인정보 또는 신용정보 등을 이용하여 물건을 구매하는 등의 불법적인 행위가 가능하기 때문에 많은 해커들의 획득 목표가 되고 있다.

이와 같은 상황에서 앞서 언급한 사회 공학적인 방법이 개인 정보 또는 신용정보를 획득하기 위한 공격 기법에 통합되어 시도되고 있는데, 가장 널리 활용되는 대표적인 공격이 피싱(Phishing)이다.



[그림 1] 해킹 종류별 증감률(2004년-2005년)[1]

* 한국전자통신연구원 네트워크보안구조연구팀 (yschoi92, bluesea@etri.re.kr)



〔그림 2〕 월별 피싱 경유지 신고건수(2004년-2005년)[1]

실제로 그림 1, 그림 2에서 알 수 있듯이, 피싱 공격에 활용된 피싱 경유지 통계를 살펴보면 지난 2004년에 220건이 보고된데 비해, 2005년에는 1,087건으로 394%가 증가되었다. 이는 약 4배가 증가한 것으로 타 공격 형태의 증가율에 비해 압도적으로 높은 수치이다[1].

이와 같이, 최근에는 개인정보를 사회 공학적인 방법을 이용한 공격을 통해 획득하려는 시도가 매우 많은 상황이다. 이에 본고에서는 사회 공학적인 공격 방법이 무엇인지에 대해 알아보고, 개인정보 유출을 위해 활용되는 공격 기법에 대해 정리한 후, 가장 대표적인 개인정보 유출 공격 방법인 피싱과 파밍에 대해 자세히 기술하기로 한다. 또한, 피싱과 파밍을 극복할 수 있는 방법에 대해 추가적으로 논의하도록 한다.

Ⅱ. 사회 공학적 공격과 개인정보 유출공격의 정의

2.1 사회 공학적 공격의 정의

사회 공학적 공격 기법이란, 고도의 기술이 접목된 해킹기술과는 전혀 무관한 것으로, 기술적인 방법을 이용하는 것이 아니라, 인간의 심리적인 면을 이용하여 개인 정보 또는 신용 정보와 같은 중요한 정보를 획득하거나, 타인 스스로가 악의적인 결과를 발생하는 행위를 하도록 유도하는 것을 말한다.

사회 공학적인 공격은 단순한 정보획득의 차원뿐만이 아니라, 악성 소프트웨어의 실행을 유도하는 데에도 널리 사용되어져 왔다. 예를 들면, 앞서 언급한 케빈 미트닉의 사례뿐만 아니라, 최근 가장 큰 문제가 되고 있는 피싱, 그리고 바이러스 유포를 위한 악의적인 행동 유도 등이 이에 포함될 수 있다. 실제로 지난 2001년에 큰 문제가 되었던 "안나 쿠르니코바" 바이러스의 경우에도, 첨부 문서가 마치 안나 쿠르니코바의 누드 사진인 것처럼 속여, 해당 파일을 실행하도록 유도하였던 것이다.

이 외에도, 성적인 내용이나, 관리자를 사칭한 메일, 유용한 소프트웨어인 것으로 위장한 첨부 파일, 믿을 만한 업체를 사칭한 메일 등 다양한 방법을 통하여 해커에 의해 발송된 메일이 안전한 것으로 착각하도록 유도하는 경우가 있었다.

이와 같은 사회 공학적인 공격 방법은 공격을 당하는 피해자가, 이와 같은 공격 형태에 대한 지식이 없는 경우, 쉽게 당할 수 있으며, 실제로 아직도 많이 활용되고 있는 공격 방법이다. 이와 같은 형태의 공격에 피해를 받지 않기 위해서는 정보보호에 대한 의식 향상이 가장 필요하다.

2.2 개인정보 유출 공격의 정의

개인정보 유출 공격이란 다양한 방법을 통해 개인의 중요 정보를 획득하고, 획득한 타인의 개인정보를 악의적으로 이용하는 행위를 말한다. 이와 같은 개인정보 유출은 고도의 해킹 기술을 이용하여 이루어지는 경우도 있으나, 앞서 설명한 사회 공학적 공격 방법을 이용하여 시도되는 경우가 대부분이다.

최근 가장 큰 문제가 되고 있는 공격으로는 피싱, 파밍 그리고 스파이웨어를 이용한 공격 등이 있다.

Ⅲ. 피싱(Phishing), 파밍(Pharming), 그리고 스파이웨어(Spyware)

최근에는 트로이 목마 프로그램에 대한 대응 기술이 개발되고, 각종 바이러스 차단 프로그램에 의해 차단되기 시작하면서, 일반 해커들이 해당 프로그램을 이용하여 개인정보를 유출시키기 어려워졌다. 또한, 트로이 목마 프로그램을 이용하여 해킹하기 위해서는 해당 프로그램을 해킹하고자 하는 시스템에 설치해야 하는데, 이는 쉽지 않은 작업이다.

이를 극복하기 위해서, 해커들은 사용자가 직접 중요 개인정보들을 입력하고 전송할 수 있게 하는 방법을 이용하기 시작하였는데, 이것이 피싱이다. 이후, 피싱에 대한 대응 기술이 개발되고, 사용자들의 정보보호 인식이 강화되면서, 피싱 기술이 과거만큼 효과적이지 못하게 되었고, 해커들은 이를 극복하기 위해 파밍 기술을 적용하기 시작하였다.

이에, 본 장에서는 개인정보 유출을 위해 최근 가장 널리 활용되고 있는 피싱과 파밍 그리고 스파이웨어에 대해 자세히 분석해 보도록 한다.

3.1 피싱(Phishing)

3.1.1 피싱의 정의

피싱은 사회공학적인 방법으로 해당 정보를 보유하고 있는 사람을 속여 중요한 정보들을 획득하기 위한 공격 행위를 의미한다.

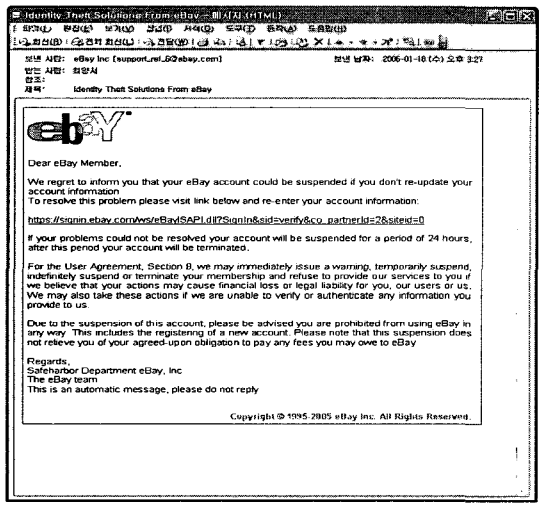
여기서 피싱(Phishing)이라는 단어는 "비밀을 탐지하다", "비밀을 찾아내다"라는 의미의 "fish"라는 단어와 전화 해킹을 의미하는 "Phreaking"이라는 단어가 통합되어 만들어진 단어로서, 해커들 사이에서는 이미 오래전부터 사용되던 단어이다.

이러한 피싱은 단순한 기술적인 요소를 이용한 해킹이 아니라, 사회공학적인 공격 방법을 활용하고 있다는 점에서 더 큰 위협이 되고 있다. 일반적으로 시스템 관리를 아무리 잘하더라도, 이러한 사회공학적인 방법을 통하면 해킹이 가능하기 때문에 이에 대한 대응책 개발이 매우 어렵기 때문이다.

3.1.2 피싱의 메시지 전달 방법

일반적으로 피싱 메시지는 전자우편(Email), 웹페이지, IRC 및 Instant Messaging, 그리고 트로이 목마 등을 이용하여 전달되게 된다.

(1) 전자우편



[그림 3] 전자우편을 통해 전달된 피싱 메시지

피싱 메시지를 전달하는 가장 일반적이고, 널리 활용되는 방법이 전자우편을 이용한 메시지 전달 방법이다. 추측컨대, 전자우편을 사용하는 거의 모든 사용자가 피싱 메일을 받아보았을 것이다. 실제로, 저자도 본 논문을 작성하던 도중 그림 3과 같은 피싱 메일을 받았다. 이는 특별한 것이 아니며, 이미 과거에도 이와 유사한 메일을 수차례 받은 적이 있었다.

그림 3과 같이 그림파일을 이용한 HTML형식의 메일이 도착되는 경우도 있으나, 일반 Text 형식으로 위장된 HTML형식의 메일이 도착되는 경우도 있다. 이는 메일 내부의 특정 URL을 속이기 위함이다. 즉, 메일 상에서는 정당한 URL인 것처럼 표시되나, 실제로 연결되는 사이트는 해커가 원하는 곳으로 지정하기 위한 것이다. 이를 위해 일반적으로 표 1과 같이 코딩되어 있다.

[표 1] URL 변경을 위한 HTML 코딩 방법

〈A HREF=https://signin.ebay.com〉 http://200.41.5.40:780/rock/e/〈/a〉

(2) 웹 페이지를 이용한 전달

전자우편을 이용한 전달방법 외에 가장 널리 사용되는 방법이 웹페이지를 이용한 전달방법이다. 이는 일반적으로 정당한 사이트의 각종 이미지 파일이나 내용을 활용하여 마치 실제 웹페이지인 것처럼 보이도록 작성되나, 실제로 특정 이미지 혹은 URL을 클릭하는 경우, 해커가 원하는 내용이 표시되거나, 특정 웹사이트를 접속하도록 작성된 경우가 대부분이다. 이를 위해 Cross Site Scripting[4]과 같은 공격 기법을 활용한다.

(3) IRC 및 Instant Messaging

최근에는 IRC 및 Instant Messaging 프로그램을 통해 피싱 메시지를 전달하는 방식이 이용되기도 한다. 이는 IRC 및 일반 Instant Messaging 프로그램이 사진이나, URL, 그리고 일반 멀티미디어 데이터를 직접 포함시킬 수 있는 기능을 가지고 있기 때문에 가능하다.

(4) 트로이 목마 프로그램

트로이 목마의 경우에는 직접 중요 정보들을 수집하여 전송하는 경우도 있지만, 사용자가 특정 웹사이트에 접근하고자 할 때, 해커에 의해 지정된 변조된 웹페이지를 보여주도록 하는 방식도 활용되고 있다.

3.1.3 피싱 공격을 위한 기술

현재 가장 널리 사용되는 피싱 공격은 일반적으로 사용자가 특정 웹페이지로 이동하여 해당 웹사이트의 접속을 위한 ID 및 비밀번호를 입력할 때 중요 정보

를 획득하는 방식을 택하고 있다. 본 절에서는 이때 주로 사용되는 공격 형태에 대해서 알아보도록 한다.

(1) Man-in-the-Middle 공격

피싱을 위해 널리 사용되는 공격이 Man-in-the-Middle 공격이다. 가장 일반적인 Man-in-the-Middle 공격으로는 허위 프락시 서버를 사용하는 것이다. 이는 일반 사용자가 특정 웹사이트에 접속하고자 할 때, 정당한 웹페이지를 직접 접속하지 않고, 해커가 운영하는 프락시 서버를 거쳐서 접속되도록 하는 방식을 의미한다. 이런 경우, 일반 사용자가 사용하는 모든 HTTP데이터를 확인할 수 있게 된다. 이 외에도 "DNS Cache Poisoning", "URL 속이기(Obfuscation)" 등의 공격 기술이 활용된다.

이와 같은 형태의 공격이 시도되는 경우에는 SSL과 같은 트래픽 보호 프로토콜을 사용하더라도 해당 트래픽의 모든 내용이 확인될 수도 있다.

(2) URL 속이기(Obfuscation) 공격

일반적으로 널리 사용되는 또 하나의 공격 방법이 바로 URL 속이기 방법이다. 이는 전자우편 등을 통해 전달된 메시지에 포함되어 있는 URL이 실제 보이는 것과는 다른 곳으로 연결되도록 만드는 공격 방식을 말한다. 이를 위해 일반적으로 "변조된 도메인명", "URL변조를 통한 호스트명 변경", "URL 숨기기" 등이 시도된다.

- 변조된 도메인명

변조된 도메인 명이란 표 2와 같이 정당한 도메인 이름과 유사한 도메인명을 이용하여 마치 정당한 사이트인 것처럼 보이게 하여 사용자를 속이는 방법이다.

〔표 2〕 변조된 도메인명

정당한 사이트 : http://secure.goodbank.com 변조된 도메인 명 - http://secure.goodbank.com.ch - http://goodbank.secure.com - http://secure.goodbanking.com

- URL변조를 통한 호스트명 변경

일반적으로 URL에 특정 사이트의 ID와 비밀번호 정보를 넣어 함께 사용하는 경우가 있는데, 이를 이용하여 전체 URL을 속이는 방법이 활용되기도 한다. 이는 표 3과 같은 방식이 적용된다.

〔표 3〕 URL 변조 방법

일반적 인증: http://id:pw@hostname/path 변조된 도메인 명 - http://goodbank.com:ebanking@evilsite/phishing/path

표 3의 변조된 도메인명과 같이 사용되는 경우, 실제 시스템에서는 goodbank.com이라는 ID와 ebanking이라는 비밀번호를 이용하여 evilsite에 접속하는 것으로 해석되게 된다.

-URL 숨기기

웹서버는 다양한 언어를 지원하기 위해서 다양한 인코딩 방식을 지원한다. 해커는 이러한 인코딩 방식을 이용하여 특정 문자열을 숨기기도 한다. 이러한 인코딩 방식에는 "Escape Encoding", "Unicode Encoding", "Inappropriate UTF-8 Encoding", "Multiple Encoding" 등이 있다. 실제로 그림 3의 피싱 메시지에 의해 유도되는 URL에 해당되는 웹페이지에도 특정 공격 코드를 숨기기 위해 "Escape Encoding"방식이 이용되고 있었다.

〔표 4〕 Escape Encoding 방식으로 변경된 Text

Encoded Text
%66%75%6E%63%74%69%6F%6E%20%69%28
%79%29%7B%76%61 . . . %3D%22%22%7D
 	
Decoded Text
function i(y){var f='',z,q,w,v;for(z=0;z<y.length;
z++) {q=y.charAt(z);w=h.indexOf(q);if(w)-1){v=
((w+1)%x-1);if(v<=0){v+=x}f+=h.charAt(v-1)}else{
f+=q}}c+=f};functionjjj(){document.write(c);g=''}

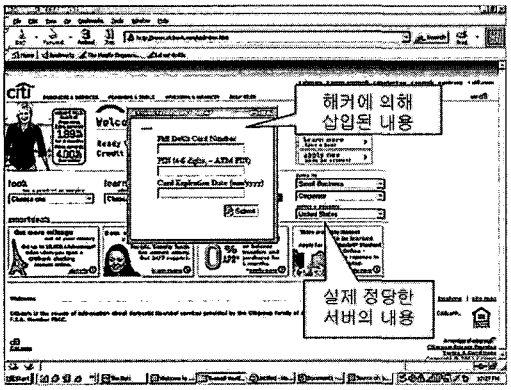
(3) Cross-site Scripting 공격

Cross-site Scripting 공격이란 해당 취약점을 가지고 있는 웹페이지에 해커가 조작한 웹 문서를 끼워 넣어 전체 웹 문서를 변경시키는 공격 기법을 의미한다. 이와 같은 경우, 웹 브라우저에서는 정당한 도메인에 접속한 것으로 판단되나, 실제로는 조작된 웹페이지가 표시되며 이를 통해 중요 정보들이 해커에게 전송되게 된다.

〔표 5〕 Cross-site Scripting 공격의 일반적인 URL 형태

http://goodbank.com/ebanking?URL=http://evilsite.com/phishing/fakepage.htm

실제로 Cross-site Scripting 취약점을 가지고 있는 사이트에서는 그림 4와 같이 특정 페이지를 삽입하여 실제 정당한 사이트인 것처럼 보일 수 있게 된다. 이는 일반적으로 다음 표 5와 같은 URL을 이용하게 된다.

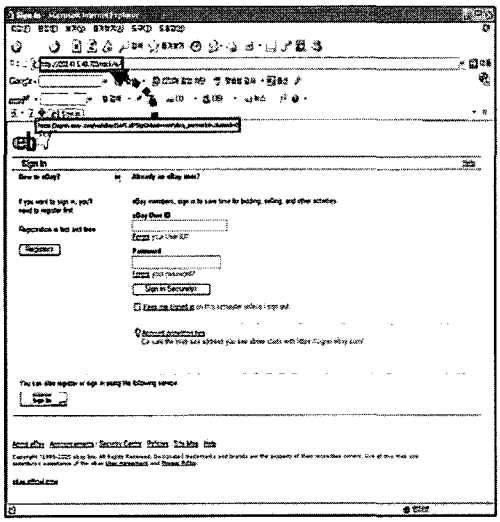


〔그림 4〕 Cross-site Scripting을 이용한 웹페이지 삽입

(4) Hidden Attack

최근에는 실제 공격을 수행하는 코드들과, 해당 웹 페이지가 잘못된 내용이라는 것을 알 수 있게 하는 내용을 사용자들이 보지 못하게 함으로써, 안전한 웹 페이지로 인식되게 하기 위한 노력이 시도되고 있다. 이는 "Hidden Frame"이나 "Graphical Substitution" 등을 이용하여 수행된다.

실제로 그림 5는 그림 3의 메시지에서 지정하는 웹 페이지로, 이 웹 페이지에서는 웹 브라우저에서 URL



〔그림 5〕 URL 표시 변경이 시도된 웹페이지

부분을 강제적으로 교체하도록 하는 방법이 활용되고 있었다. 그런데, 그림 5에서는 저자가 사용하는 웹브라우저에 다수의 툴바(Toolbar)가 설치되어 실제 URL이 표시되는 위치와는 달리 보다 아래쪽에 해커가 의도한 URL이 표시됨을 볼 수 있었다.

물론 그림 5에서 사용된 모든 이미지 및 기타 내용은 실제 ebay사이트에 존재하는 내용이었다.

(5) 웹브라우저 취약점을 이용한 공격

앞서 언급된 방식 외에도 사용자 웹 브라우저의 취약점을 이용한 공격 방법이 있다. 이는 MS Explorer의 취약점을 이용하여 특정 문자를 숨기거나, MS Explorer와 Media Player의 취약점을 함께 사용하여 공격 하는 방법 등이 활용된다[3].

3.2 파밍(Pharming)

3.2.1 파밍의 정의

파밍은 피싱이 사용자에 의해 쉽게 탐지될 수 있는 점을 극복할 수 있는 공격 기법이다. 파밍은 다양한 방법을 통해 정당한 사용자가 특정 도메인명에 대한 IP 주소 확인 요구 시, 해커가 장악하고 있는 악의적인 웹 사이트의 주소를 제공하도록 하여 해당 사이트로 접속되도록 유도하는 공격 기법을 의미한다.

기존의 피싱은 사용자의 잘못된 판단에 의해 사용자 스스로가 중요 정보를 유출하도록 하는 사회공학적인 방법을 이용했으나, 파밍은 순수 기술적인 공격 방법을 이용하여, 사용자가 해당 웹사이트가 정당한 것인지를 또는 악의적인 것인지를 파악할 수 없도록 하는 기법을 이용하는 것이다. 파밍은 주로 웹 트래픽의 전달방향 변경(redirection)을 통해 시도된다.

3.2.2 파밍 공격 방법

파밍을 위한 공격 방법은 매우 다양하다. DNS 자체를 공격하여 DNS의 내용을 변경하기도 하고, 해당 사용자의 PC 또는 시스템을 공격하기도 하며, Man-in-The-Middle 공격 등을 이용하기도 한다.

(1) Local Host의 네트워크 설정 변경

일반적으로 각 운영체제들은 자체 Domain Name 항목을 가지고 IP 주소 확인이 가능하도록 특정 파일들을 제공하고 있다.

예를 들면 LINUX의 경우 "/etc/hosts" 파일을 들 수 있으며, 윈도우의 경우에는"C:\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTS" 파일을 들

수 있다.

상기 파일들은 해당 시스템이 DNS query를 생성하기 이전에 먼저 IP 주소를 찾기 위해 접근하는 파일이다. 따라서, 본 파일들이 변경되게 되면, DNS의 내용과는 상관없이 해당 IP 주소로 트래픽을 전송하게 된다. 해커들은 이와 같은 점을 이용하여, "HOSTS" 파일의 내용을 변경함으로써 파밍을 시도하곤 한다.

또한, 해커들은 "HOSTS"파일 변경 외에도 DNS 설정을 변경하여 해커가 관리하고 있는 DNS서버로 DNS query를 전송하게 만들기도 한다. 이는 직접 해당 시스템의 DNS 설정을 변경하는 경우도 있으나, rogue DHCP 서버 등을 운영하여 해당 설정을 변경하도록 유도하는 경우도 있다. 이는 DHCP 서비스를 이용하는 시스템의 경우, 네트워크 관련 모든 설정들을 DHCP 서버로부터 획득하도록 되어 있는 점을 악용하는 것이다.

(2) Domain Hijacking

여기서 의미하는 Domain Hijacking은 기술적인 공격 방법이 아니라, 도메인 관리의 문제를 이용하는 공격 방법이다. 일반적으로 도메인 명은 영구적으로 사용할 수 있는 것이 아니다. 따라서, 일정 기간이 지나면 재등록을 해야 하는데, 관리적인 실수로 재등록을 하지 않고 등록기한을 넘기는 경우가 있다. 이때, 악의적인 해커가 해당 도메인 명을 타 IP주소로 등록하는 경우, 과거와는 달리 전혀 다른 시스템으로 웹 트래픽이 전송되게 된다.

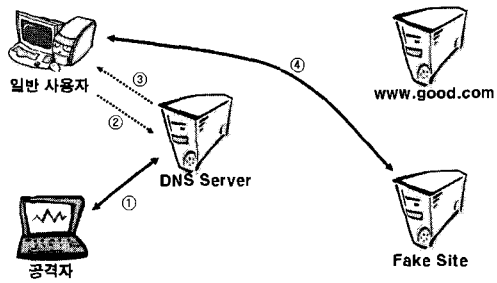
실제로 2005년 1월에는 미국 뉴욕의 ISP업체인 Panix.com의 도메인 명이 타 사용자에 의해 가로채어져서 전혀 다른 사이트로 연결되었던 적이 있다[11].

이와 유사하게, III장의 1.3절에서 설명한 바와 같이 비록 같은 도메인 명은 아니지만, 유사한 도메인 명을 등록하여 사용자들의 실수를 통해 악의적인 사이트로 접속되도록 유도하는 경우가 있다.

(3) DNS 공격

파밍을 위해 시도되는 공격 중에는 DNS 자체의 취약점을 이용하여 공격이 시도되는 경우가 있다. 특히, DNS 설정의 취약점을 이용하거나, DNS 시스템 자체의 취약점을 이용하는 경우가 있다.

즉, 그림 6과 같이, ①해커는 DNS의 다양한 취약점을 이용하여 DNS 시스템 내부의 항목 자체를 변경시키고, ②정당한 사용자가 특정 웹사이트로 접근하고자 할 때, ③해커가 지정한 웹 사이트에 대한 IP 주소를 제공하여, ④실제 접속이 "Fake Site"로 접속되도록 유도하는 공격 방법이다.

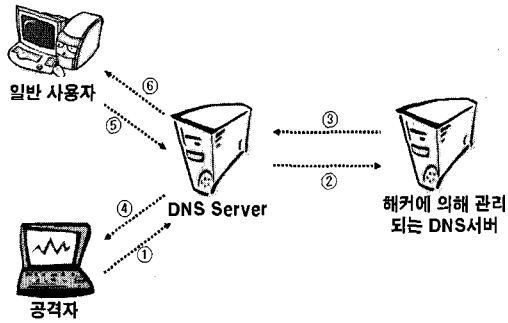


〔그림 6〕 DNS 내용 변경을 통한 Fake Site접속 유도

이와 같은 형태의 공격을 위해 사용되는 공격 방법에는 "DNS Cache Poisoning", "DNS ID Spoofing[4]", "The Birthday Attack[4]" 등과 같은 것들이 존재한다. 본고에서는 "DNS Cache Poisoning"에 대해 알아보도록 한다.

DNS Cache Poisoning이란 DNS의 Cache 메커니즘의 취약점을 이용하여 의해 임의의 IP주소 항목이 특정 DNS의 Cache에 존재하도록 하고, 이에 따라 정상적이지 못한 사이트로 접속되도록 유도하는 공격을 의미한다. DNS Cache Poisoning은 그림 7과 같은 절차를 통해 시도된다.

① 먼저, 해커는 특정 도메인(.hack.com)을 관장하는 DNS서버를 구성한다. ②그리고, 해커는 해당 도메인에 속하는 특정 시스템(ex. www.hack.com)에 대한 IP주소 확인 작업을 지속적으로 수행한다. ③그러면, 정상적인 DNS는 해당 도메인을 관리하는 DNS서버로 해당 도메인명에 대한 IP주소를 요청하게 된다. ④이때, 해커가 관장하는 DNS는 해당 도메인명에 대한 IP주소뿐만 아니라, 타 도메인 명



〔그림 7〕 DNS Cache Poisoning 절차

(www.good.com)에 대한 변조된 IP주소도 알려준다. 이렇게 되면 정상적인 DNS의 Cache에 추가적으로 알려진 도메인 명에 대한 IP주소가 저장되게 된다. ⑤이때, 정상적인 사용자가 해당 사이트(www.good.com)에 접속하기 위해 IP주소 확인을 시도하게 되면, ⑥Cache에 존재하는 잘못된 IP주소를 알려주게 되는 것이다. 현재, 최신의 DNS 서버들에서는 이와 같은 취약점이 제거되었다.

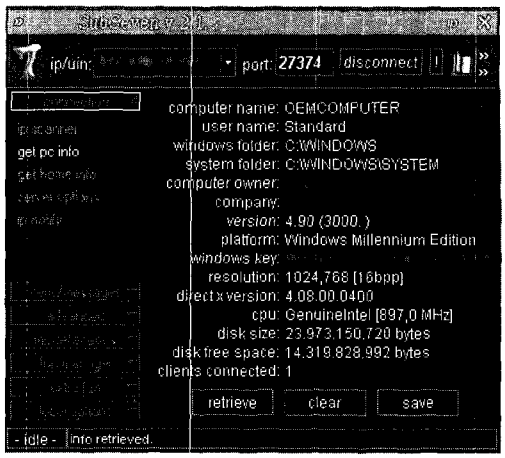
(4) Page Rank Escalation

일반적으로 사용자들이 특정 사이트에 접속하고자 할 때, 해당 사이트의 도메인 명을 완전히 기억하지 못하는 경우가 대부분이다. 따라서, 대부분 일반 포털 사이트나, 서치 엔진(ex. Google, Yahoo, etc.)에서 해당 사이트를 찾게 된다. 그런데, 일반 서치 사이트의 특정 링크들은 사용 요금을 지불하고, 타 링크보다 앞선 위치에 표시되도록 할 수 있다. 이런 경우, 악의적인 해커는 유사한 사이트 명을 이용하여 악의적인 링크를 가장 앞쪽에 위치시킬 수 있다. 이를 통해 해커는 일반 사용자들을 해커가 원하는 사이트에 접속하도록 유도할 수 있다. 물론, 이와 같은 공격이 아직까지 발생하지는 않았으나, 충분히 가능성이 있다고 판단된다.

3.3 스파이웨어(Spyware)

스파이웨어란 다양한 해킹방법을 이용하여 임의 시스템에 침입하여 해당 사용자에 관한 정보를 수집하고 이를 전송하는 악성 프로그램을 의미한다. 즉, 1990년대 말과 2000년대 초반 크게 유행했던 각종 트로이목마(Trojan) 프로그램이 일종의 스파이웨어라고 할 수 있다. 대표적인 트로이목마 프로그램으로 백오리피스2K, 서브세븐 등이 있으며, 이와 같은 악성프로그램이 특정 시스템에 설치되면, 해당 시스템의 모든 정보를 획득할 수 있을 뿐만 아니라, 해당 시스템 전체를 제어할 수 있었다. 그 기능을 간단히 살펴보면, 실시간 화면 캡처, 키 로깅(Key logging), 시스템 종료 및 재부팅, 파일 전송, 프로그램 실행, 화면 바꾸기(flipping), 메시징 등 매우 다양하다.

최근에는 이와 같은 다양한 기능을 갖는 악성 프로그램보다 특정 목적을 가지고 해당 기능만을 수행하는 악성 프로그램들이 주류를 이루고 있다. 특히, 중국 해커들에 의한 특정 온라인 게임의 계정 및 비밀번호 수집 프로그램 등이 이에 해당한다.



[그림 8] SubSeven V.2.1.3 메인화면

Ⅳ. 대응 방안

4.1 피싱 대응방안

피싱 대응 방안에 대해서는 크게 사용자 측면과, 서버 측면으로 나누어 볼 수 있다.

4.1.1 사용자 측면의 피싱 대응 방안

일반 사용자 측면에서 보았을 때, 피싱 공격에 대한 대응은 사회공학적인 공격을 어떻게 대응할 것인가에 초점이 맞춰질 수 있다.

가장 중요한 것은 어떠한 형태로든 수신된 메시지에 대해 세심한 관찰을 통하여 피싱 공격 여부를 확인하는 것이다. 특히, 그 내용이 중요 정보를 요구하는 경우는 더욱 그러하다.

일단, 잘 알지 못하는 사용자로부터 도착된 전자 우편은 일단 모두 피싱일 가능이 있다고 의심할 필요가 있고, 첨부된 파일은 바이러스 혹은 악성 스파이웨어라고 의심할 필요가 있다. 그리고, HTML 형태로 도착된 전자우편 상의 URL이 실제로 해당 URL과 연계되어 있는지를 유심히 살펴보아야 한다. 이는 도착된 HTML 메시지에 대한 소스보기 등을 이용하면 쉽게 파악할 수 있게 된다.

실제로 본 저자에게 도착된 그림 3의 메시지의 경우 표 6과 같은 소스코드를 가지고 있었다.

즉, 메시지에 나타나는 URL(ebay 사이트)과는 달리 전혀 다른 사이트로 접속을 시도하게 되어있는 것이다.

사회공학적인 공격기법에 대한 대응 외에도 추가적인 대응방안이 필요하다. 먼저, 사용하는 시스템에 대

〔표 6〕 피싱 메일의 소스코드

```
<html>
<p><font face="Arial">
<A HREF="https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0">
<map name="qnlc"><area coords="0, 0, 646, 569" shape="rect"href="http://200.41.5.40:780/rock/e/"></map>
<img SRC="cid:part1.04060203.01060905@identdep_op769490451123@ebay.com" border="0" usemap="#qnlc"></A></a></font></p>
<p><font color="#FFFFFD">?? ??? in 1827 I'll call back! I wish I advise you </font></p>
</html>
```

한 지속적인 보안 패치와, 다양한 바이러스 차단 프로그램, 스파이웨어 차단 프로그램 등을 이용하여 해당 시스템에 악의적인 프로그램이 설치되지 않도록 노력해야 한다.

또한, 사용하는 웹 브라우저의 기능들 중 사용하지 않는 기능에 대해서는 그 기능을 중지 시켜야 하며, 윈도우 팝업 차단, Active X차단, Multi-media 자동 실행 차단, 자동 내려 받기 기능 차단 등이 적용되어야 한다. 최근에는 피싱 차단을 위한 플러그인이 제공되는데, 이를 이용하는 것도 좋은 방법이다.

또한 특정 웹사이트를 방문할 때, 해당 웹사이트가 정당한 것인지를 확인하도록 노력해야 할 것이다.

4.1.2 서버 운영 측면의 피싱 대응 방안

서버 측면에서의 피싱 대응 방안은 해당 서버를 접속하는 경우, 특정 기능을 통해 접근한 서버가 정당한 서버임을 알려줄 수 있는 방안을 강구하는 것을 의미한다. 이는 일반적으로 사용자에 대한 교육을 통해 이루어질 수 있으며, 강력한 인증 메커니즘을 도입함으로써 수행될 수도 있다.

4.2 파밍 대응방안

파밍에 대한 대응 방안 중 사용자들이 할 수 있는 것은 피싱에 대한 대응 방안이 대부분이다. 실제로, 일반 사용자들이 그 외의 대응책을 수행하기는 쉽지 않다.

서버 관리 측면에서 본다면, DNS 관리자들은 해당 DNS에 알려진 취약점이 존재하지 않도록 관리해야 할 것이다. 이를 위해 해당 DNS에 대한 시스템 패치, 설정 업그레이드 등을 수행해야 하며, 가능하다면 인증된 안전한 사이트로부터 호스트 명에 대한 IP 주소가 정확한지를 확인하는 작업 등을 수행하여야 한다.

4.3 스파이웨어 대응방안

스파이웨어는 다양한 형태를 통해 사용자에게 전달된다. 일반 바이러스처럼 유용한 프로그램이나, 재미있는 그림 등으로 위장되어 전달되는 경우가 대부분이다. 또한, 인터넷 상에서 무료로 제공되는 각종 파일에는 이와 같은 스파이웨어가 포함되어 있을 확률이 매우 높다. 따라서, 특정 프로그램을 내려 받는 경우에는 항상 해당 파일에 문제가 없는지를 확인해야 한다. 또한, 백신 프로그램이나, 스파이웨어 또는 Ad-ware 방지 프로그램을 이용하여 악의적인 프로그램을 차단할 수 있도록 해야 한다.

Ⅳ. 결 론

인터넷 사용자의 급증과 함께, 다양한 서비스가 인터넷을 통해 제공되기 시작하였다. 이러한 서비스에는 단순한 정보 전달을 위한 서비스뿐만 아니라, 경제적 활동의 중심이 되는 은행업무나 신용카드관련 서비스, 그리고, 다양한 물품의 구매 서비스 등이 포함되었다. 이와 더불어 개인의 중요 정보들 역시 인터넷으로 송/수신되기 시작하였다.

이와 같이 중요 정보들이 인터넷을 통해 전달되기 시작하면서, 해커들은 과거 자신의 명성을 알리기 위해 해킹을 시도하는 데서 벗어나, 경제적인 이득을 위해 해킹을 시도하기 시작하였고, 이중 불법적인 개인정보의 획득을 통한 이익 창출이 매우 널리 시도되기 시작하였다.

특히, 인터넷을 통해 특정 사이트에 접근하고자 할 때 사용되는 ID와 패스워드와 같은 중요정보를 획득하고자 하는 시도가 크게 증가하기 시작하였다.

이를 위해 해커들은 사회공학적인 공격 기법을 가미한 피싱 공격을 시도하기 시작하였으며, 피싱에 대한 대응이 시작되면서, 해커들은 파밍 공격을 시도하기 시작하였다. 실제로, 각종 통계자료를 보면 2004년에 비해 2005년에 피싱 공격이 무려 4배나 증가한 것으로 나타나고 있다.

이에, 본고에서는 피싱과 파밍 공격이 무엇이며, 어떠한 절차를 통해 이루어지는지를 확인하였으며, 그에 대한 대응 방안에 대해 논의하였다.

보안 전문가들은 2006년에도 지속적으로 피싱 및 파밍 공격이 증가할 것으로 예상하고 있다. 앞으로 증가되는 피싱 및 파밍 공격에 피해를 받지 않도록 주의

해야 할 것이다. 본고가 피싱 및 파밍 공격 방어에 도움이 되었기를 바란다.

참 고 문 헌

[1] 한국정보호호진흥원, "인터넷 침해사고 동향 및 분석 월보 2005년 12월", 2005.1.
[2] terms, http://www.terms.co.kr/spyware.htm
[3] NISR, "The Phishing Guide", NGS Software Ltd., 2004.
[4] NISR. "The Pharming Guide". NGS Software Ltd., 2005.
[5] Danny Allan, "Identity Theft, Phishing and harming: Accountability & Responsibilities", OWASP AppSec, Oct. 2005.
[6] "Proposed Solutions to Address the Threat of Email Spoofing Scams", The Anti-Phishing Working Group, Dec. 2003.
[7] "Anti-Phishing: Best Practices for Institutions and Consumers", McAfee, March 2004.
[8] Gunter Ollmann, "URL Encoded Attacks", 2002
[9] Gunter Ollmann, "Security Best Practice: Host Naming and URL Conventions", 2005
[10] Joe Stewart, "DNS Cache Poisoning - The Next Generation", 2003
[11] Steven Musil, "ISP Panix over domain hijack", CNET News.com, Jan 17, 2005.
[12] 인터넷침해사고대응지원센터, "SPAM BOT을 이용한 Phishing SPAM 발송 시스템 분석 보고서", KISA, 2005.
[13] 인터넷침해사고대응지원센터, "피싱 사이트 악용 서버 분석 사례", KISA, 2005.
[14] APWG, "Phishing Activity Trends Report", Nov. 2005.
[15] The Open Web Application Security Project(OWASP) Foundation, http://www.owasp.org/
[16] Anti-Phishing Working Group, http://www.antiphishing.org/
[17] NORAD(The North American Aerospace Defense Command), http://www.norad.mil

〈著 者 紹 介〉

최 양 서 (Yang-Seo Choi)

1996년 2월 : 강원대학교 전자계산학과 이학사
2000년 8월 : 서강대학교 검퓨터공학과 공학석사
2000~현재 : ETRI 정보보호연구단 선임연구원
〈관심분야〉 정보보호, 포렌식, 침입분석, 네트워크 보안, 보안장비 시험

서 동 일(Dong-Il Seo)

1994년 2월 : 포항공과대학교 정보통신학과 공학석사
2004년 8월 : 충북대학교 전산학과 이학박사
1989년 1월 ~ 1992년 2월 : 삼성전자 종합연구소
1994년 3월 ~ 현재 : 한국전자통신연구원, 네트워크보안구조연구팀장
2002년 1월 ~ 현재 : ASTAP Forum IS-EG 의장
2003년 1월 ~ 현재 : 정통부지정 IT국제표준화전문가
2004년 1월 ~ 현재 : TTA TC1 부의장
〈관심분야〉 네트워크보안, 해킹, 인터넷정보보호, 보안장비 시험