http://www.krcert.or.kr
cert@certcc.or.kr

IE 등 인터넷 탐색기의 각종 Spoofing 취약점

2004. 11.

인터넷침해사고대응지원센터 (KISC)

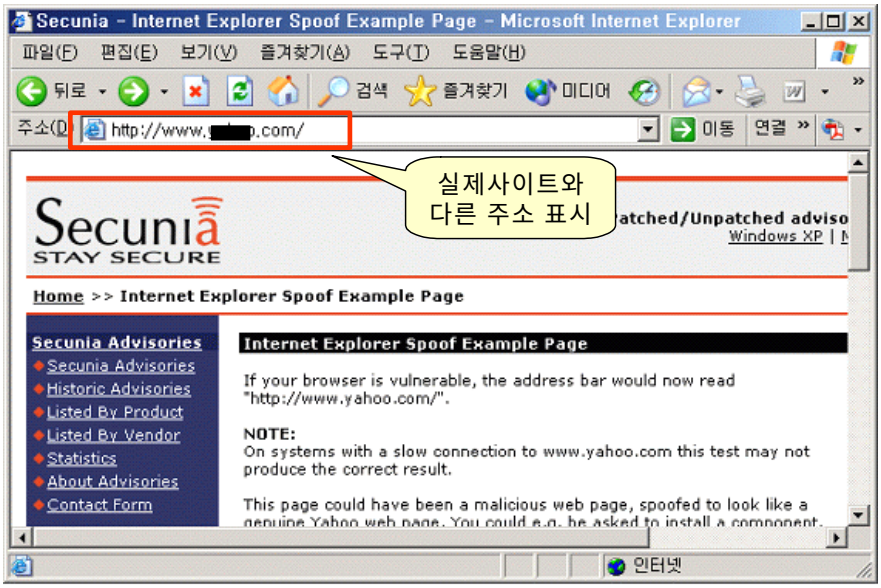
한국정보보호진흥원
Korea Information Security Agency

I. 개요

URL (Uniform Resource Location)이란 인터넷 상의 특정 정보를 지정하는데 사용하는 주소 표시 형식이다. (예. http://www.krcert.or.kr/index.html) 인터넷 익스플로러 등 인터넷 탐색기를 사용하여 정보를 검색할 때 이들 소프트웨어는 항상 인터넷 사용자가 어떤 사이트를 방문하고 있는지 주소창에 URL을 표시함으로써 알려 준다.

그러므로 인터넷 탐색기의 주소창은 항상 현재 방문하고 있는 사이트의 주소를 표시하고 있어야 하지만, 검색소프트웨어의 버그에 의하여 이 부분이 다른 주소로 표시되도록 할 수 있으며, 이를 URL Spoofing (URL 변조) 공격이라고 한다. 또한 주소 줄을 변경시키므로 address bar spoofing (주소줄 변조)라고도 한다.

다음의 (그림-1)은 URL 스푸핑이 성공한 경우의 인터넷 탐색기 화면이다. 이 그림에서 주소줄은 이 사이트가 www.OOO.com임을 나타내고 있지만, 실제로 탐색기 창에는 전혀 다른 사이트가 표시되고 있다.



(그림-1) URL 스푸핑 예제

이와 같은 URL spoofing 공격은 그 자체로써는 시스템의 운영이나 동작에 영향을 미치지 않는다. 그러나 최근 빈발하고 있는 피싱(Phishing)과 결합하였을 경우에는 공격 대상자가 자신이 속고 있다는 것을 알아채기 힘들기 때문에 자신도

모르는 사이에 피해자가 될 수 있다.

본 문서에서는 URL Spoofing으로 사용자를 속여 악용하는 기법들을 알아보고 그 방법들을 소개하여 스푸핑 및 피싱에 의한 피해를 최소화 하고자 한다.

※ 피싱 (Phishing) : Private Data와 Fishing의 합성어로, 사회공학적(social engineering) 기법을 이용한 온라인상의 정보 유출 사기 기법. 즉, 인터넷 뱅킹, 온라인 쇼핑몰 등을 사칭해 이용자를 현혹하는 이메일을 발송하여 계좌번호, 카드번호 등의 금융정보를 유출하고 이를 이용해 금융사기를 일으키는 신종 사기 수법

II. 스푸핑 기법

현재까지 공개된 스푸핑 기법은

- o 특수문자를 사용한 URL 변조
- o 스크립트를 이용한 변조
- o HTML 태그를 이용한 변조
- o 다이얼로그 박스를 이용한 스푸핑
- o 파일 다운로드 시 URI 및 확장자 변조
- o 컨텐츠 스푸핑
- o 인증서 스푸핑 기법

등 다양하다. 본 장에서는 각 기법에 따른 상세한 방법을 알아본다.

가. 특수문자를 사용하여 인터넷 주소 변조

URL Spoofing은 표시될 페이지의 위치 지정시 %00, %01, @ 등 특수 문자를 이용하여 URL 표시줄을 지우고 다시 표시할 수 있다. 이 취약점은 마이크로소프트의 IE에서 URL을 표준형태의 주소로 변환하기 위하여 사용하는 루틴의 버그에 의하여 발생한다.

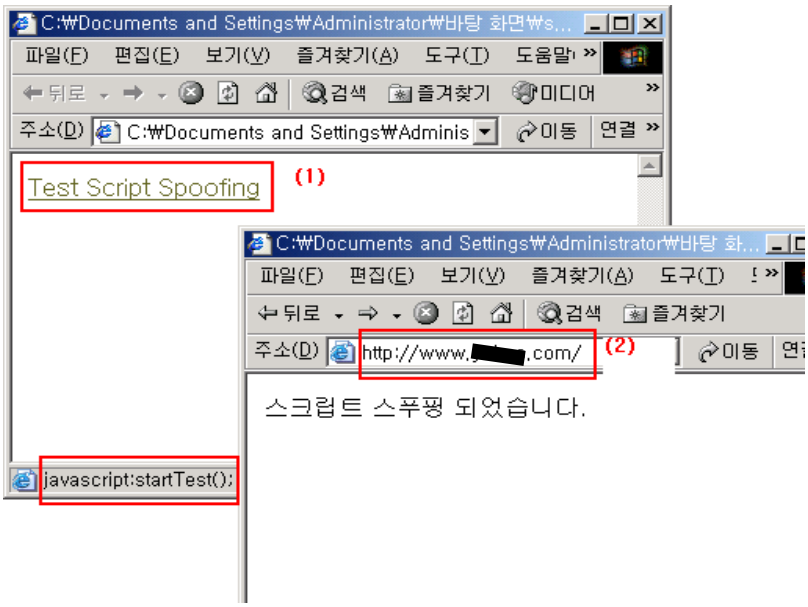
다음 예와 같은 주소는 실제로는 malicious_site.com에 접속되지만 인터넷 탐색기의 주소표시줄에는 http://www.trusted_site.com으로 표시된다.

```
http://www.trusted_site.com%01%00@malicious_site.com/malicious.html
```

나. 스크립트를 사용한 URL 변조

특정 버전의 인터넷 탐색기는 검색하는 페이지에 삽입된 스크립트에 의하여 주소표시줄에 공격자가 원하는 사이트로 표시되도록 할 수 있다. 이를 이용하여 악의적인 피셔는 믿을 수 있는 사이트의 URL을 보여주게 하여 중요 정보를 수집하고 금전적인 피해를 줄 수도 있다.

아래 (그림-2)는 스크립트를 이용하여 주소표시줄을 변조한 공격으로 (1)을 클릭하면 스크립트가 실행되는데 이 스크립트에 의해서 새로 만들어진 윈도우의 주소표시줄에는 (2)와 같이 http://www.OOO.com가 표시되나 실제 보여지는 사이트는 ./script result.html(실제 공격시는 악의적인 사이트)인 것을 알 수 있다.



(그림-2) 스크립트를 이용한 URL 변조

script.html

```
<html>
<body>
<a href="javascript:startTest();">Test Script Spoofing</a>

<SCRIPT>
function startTest()
{
  ...
  상세코드 생략
  ...

}

function openPage()
{
       mywindow = window.open("http://www.OOO.com/","newwindow");
       mywindow.blur();
       this.focus();
}

function test()
{
  ...
  상세코드 생략
  ...

}
</SCRIPT>

<A .............. HREF="./script result.html" ..............</A>

<html>
<body>
```

script result.html

```
<html>
<body>
<SCRIPT>
  ...
  상세코드 생략
  ...
</SCRIPT>
스크립트 스푸핑 되었습니다.
</html>
</body>
```

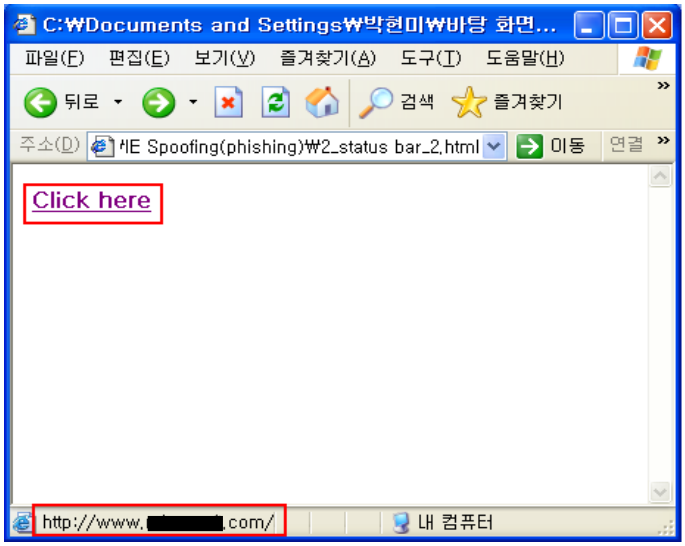
다. HTML 태그를 이용한 변조

(1) <IFRAME>이나 <TABLE> 태그를 이용하여 상태표시줄의 URL 변조

링크를 마우스로 가리켰을 경우 IE등 브라우저 하단의 상태표시줄에 클릭시 오픈되는 페이지의 URL가 표시된다. 이때 실제 연결되는 페이지와 다른 URL 즉, 신뢰할 수 있는 사이트의 URL를 보여주어 사용자가 연결하도록 유도한다.

<TABLE> 태그를 이용한 상태표시줄 스푸핑을 보여주는 아래 (그림-3)에서 상태

표시줄은 http://www.OOO.com이지만 실제로는 http://www.□□□.com 사이트로 링크된다.

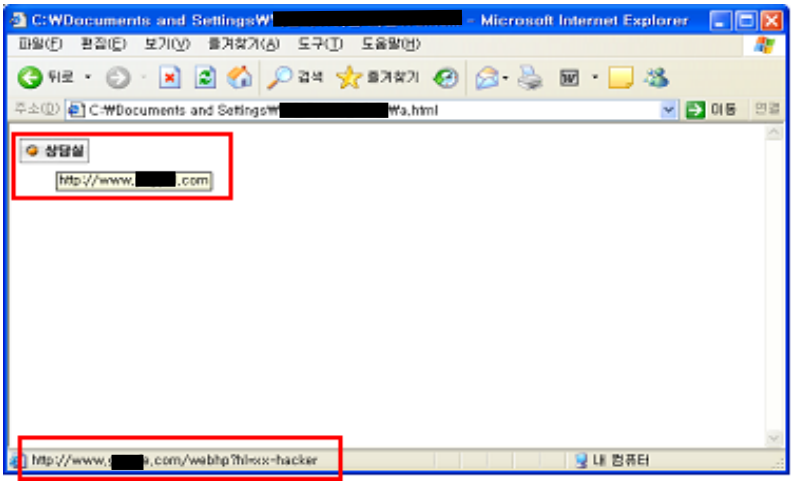


(그림-3) 상태표시바 Spoofing 공격

(2) 이미지 링크를 이용한 URL 변조

<A HREF> 태그를 이용하면 다른 페이지나 사이트로 이동할 수 있는 링크가 생성된다. 이 때, 이미지가 특정한 형식의 HREF 태그안에 포함되어 있는 경우 실제 URL의 내용을 숨길 수 있는 취약점이 있다. 즉, 이미지에 대한 설명은 신뢰할 수 있는 사이트의 URL이 표시되지만 실제 이미지를 클릭하면 악의적인 사이트로 연결된다. 사용자가 주의깊게 살피지 않아 신뢰할 수 있는 사이트라고 생각하는 경우 중요한 정보를 입력하여 피해를 입을 수 있다.

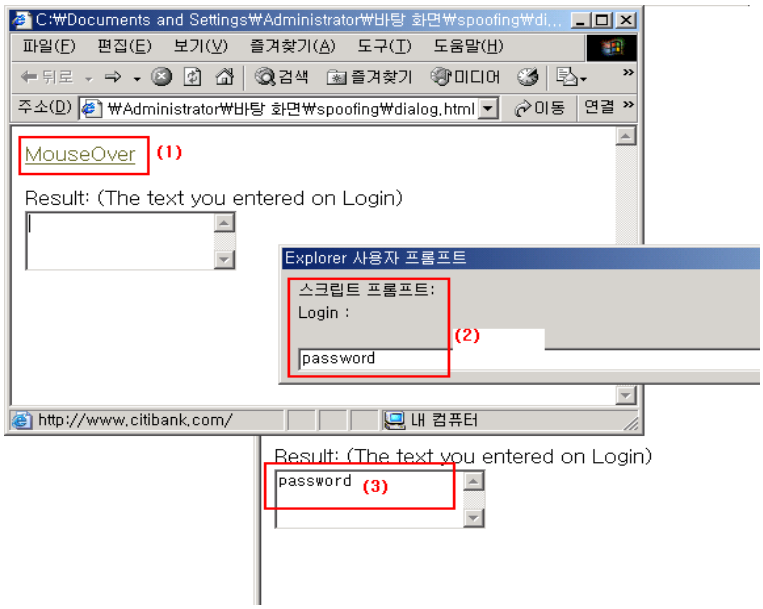
인터넷 창에서 마우스로 변조된 링크가 걸려진 그림을 가리키면 연결하고자 하는 사이트의 URL이 상태표시줄에 표시되며, 실제 연결되는 사이트의 URL이 표시되는 것을 확인할 수 있다. 그러나 이를 미처 알아채지 못한 일반 사용자는 이미지를 클릭하여 조작된 악의적인 사이트에 접속하게 된다.



(그림-4) 이미지 URL Spoofing 취약점 공격

라. 다이얼로그 스푸핑

다이얼로그 창을 위조하여 사용자의 입력을 유도하고 사용자의 입력을 가로챌 수 있다. 이는 어떤 탭이 다이얼로그 박스를 실행시켰는지 브라우저가 알지 못하여 생기는 문제로 악의적인 웹사이트에 정보를 노출시키거나 프로그램을 다운로드 받을 수 있게 한다.



(그림-5) 다이얼로그 스푸핑

```
<html>
<body>

<SCRIPT>
  ...
 상세코드 생략
 ...
    document.myform1.userinput.value = prompt("Login:");

 상세코드 생략
 ...
</SCRIPT>

<form name="myform">
Result: (The text you entered on Login)<br>
<textarea name="userinput" rows="3"></textarea></form>
</html>
</body>
```

(1)마우스로 해당 링크를 클릭하면 (2)스크립트에 의해 다이얼로그 박스가 표시되고 (3)다이얼로그 박스에 임의의 문자를 입력하면 웹페이지에 입력한 문자열이 보여진다. 여기서 다이얼로그 박스를 신뢰할 수 있는 사이트에서 보낸 것으로 생각하여 중요한 정보(“password")를 입력하면 (3)의 악의적인 웹페이지로 전달된다.

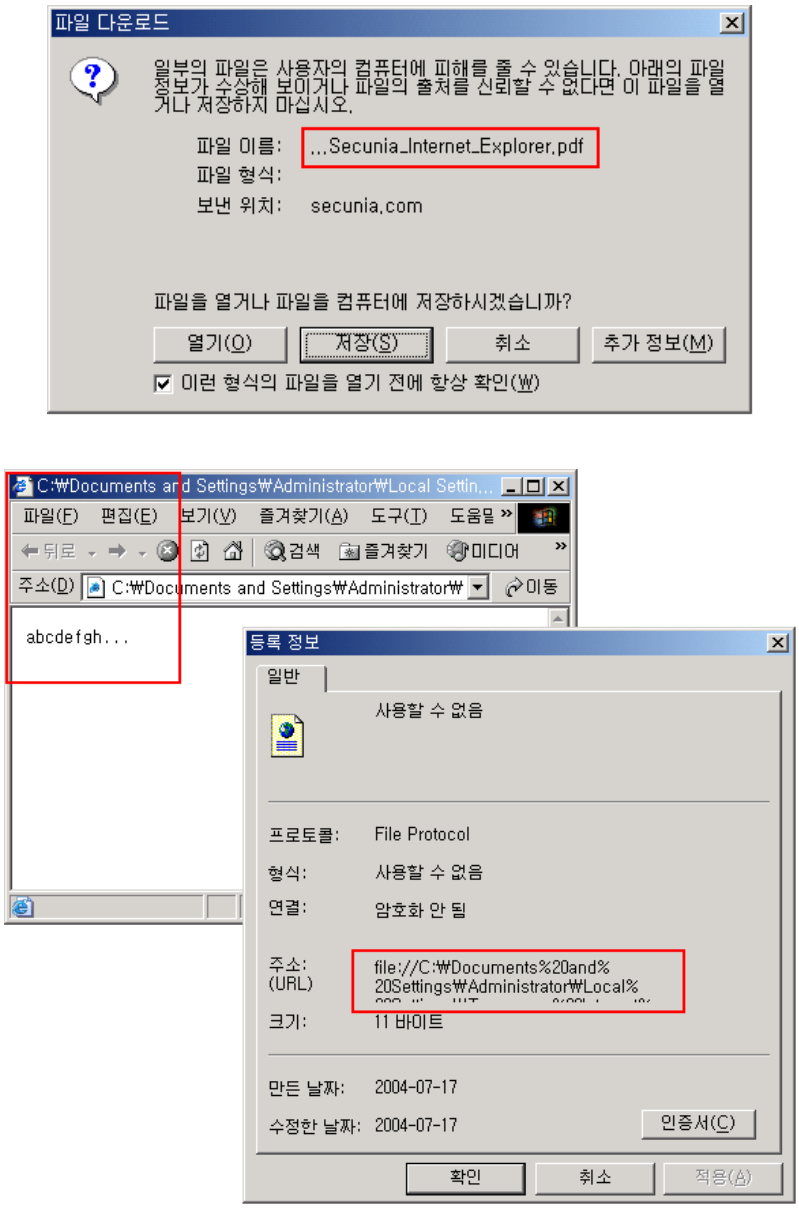
사용자는 다이얼로그가 은행과 같은 신뢰할 수 있는 사이트에서 생성된 것으로 착각하여 중요한 정보를 입력하거나 프로그램을 다운로드 받는 것에 대해 의심을 하지 않을 수 있다.

마. 파일 다운로드 시 URL 및 확장자 변조

다이얼로그 박스에서 파일의 경로를 잘못 보여지게 함으로서 사용자를 속일 수 있는 취약점이 있다. 즉, 실제 파일은 악의적인 사이트에 있는 파일이지만 다이얼로그 박스의 경로는 신뢰할 수 있는 경로로 보여서 사용자가 아무런 의심없이 파일을 다운로드하여 실행할 수 있다. 다운로드 파일이 악의적인 목적의 파일인 경우 피해를 입을 수 있다.

또한, IE에서는 다운로드 할 파일의 확장자를 변조할 수 있는 http-equiv 취약점이 있어서 원하는 파일 대신 악성행위를 하는 HTML 파일을 내려받을 수도 있다. 이 취약점은 파일이름에 포함된 CLSID를 이용한 것으로, 사용자는 대상을 pdf 파일 등으로 생각하여 다운로드 받았으나 실제로는 html 파일로 IE가 실행되어 안에 포함되어 있었던 악성스크립트 등이 실행될 수 있다.

파일을 다운로드 받고자 할때 활성화되는 파일 다운로드 다이얼로그 박스에서 아래 그림과 같이 파일이름이 보여진다. 파일 이름에는 파일의 확장자가 .pdf 이라서 사용자는 아무런 의심없이 파일을 열어 확인하고자 한다. (그림-6)에서처럼 파일은 IE에서 열리는데, 등록정보에서 실제 파일의 URL을 확인하면 아래와 같이 스페이스가 포함되어 있는 긴 파일이름을 가진 악성파일임을 알 수 있다.



(그림-6) 다운로드 파일의 확장자 변조

```
file://C:\Documents%20and%20Settings\Administrator\Local%20Settings\Temporary%20Internet%20Files\Content.IE5\4XARG9ER\Secunia[1].pdf%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20.{3050f4d8-98B5-11CF-BB82-00AA00BDCE0B}Secunia_Internet_Explorer.pdf
```

바. 컨텐츠 스푸핑 취약점

인터넷과 내부 네트워크 사이에서 인터넷 게이트웨이 역할을 수행하는 ISA 서버는 Reverse Lookup 결과를 캐쉬에 저장하는데, 저장시 결함으로 위조된 인터넷 웹사이트를 진짜 인터넷 컨텐츠로 인식하게 함으로써 사용자의 중요 정보를 유출할 수 있는 취약점이 있다.

Reverse Lookup(IP로 웹사이트 확인)이 발생하도록 만들어진 웹 사이트를 열 경우 공격자는 위조된 도메인 이름을 가진 Reverse Lookup 응답 메시지를 보내어 ISA 서버의 웹 캐쉬에 저장되도록 한다. 이후에 이 사이트에 접속하는 사용자는 캐시에 저장된 위조된 웹 사이트에 연결된다.

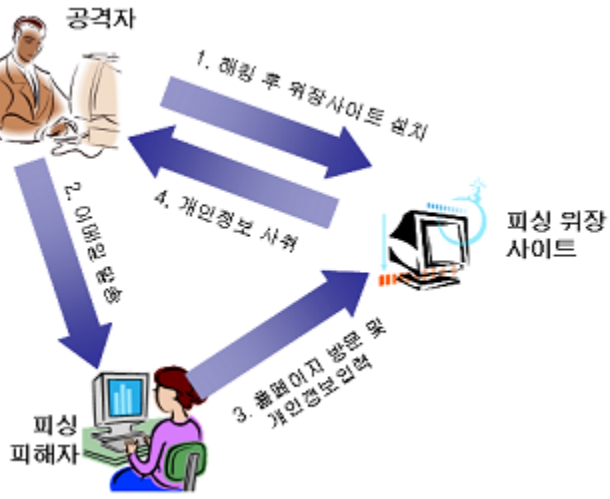
이러한 공격에 대응하기 위해서 DNS 캐쉬 크기를 0으로 설정하여 DNS 캐싱을 불가능하게 하거나(단, 이 방법은 DNS 성능이 저하되는 문제가 있음) 웹 캐쉬에 저장된 컨텐츠를 삭제시키도록 한다.

사. 인증서를 우회한 취약점

조작된 “onunload" 이벤트를 사용하여 신뢰하는 웹사이트에서 유효한 인증서를 다운로드 받아서 악의적인 사이트를 보는 동안에도 오른쪽 하단의 ”secure padlock (화면 우측 하단에 표시되는 자물쇠 표시)"을 보여주도록 할 수 있다. “secure padlock" 이 보이기 때문에 사용자는 안전한 사이트라고 생각하여 아무런 의심없이 중요 정보를 입력할 우려가 있다.

III. 스푸핑 기법을 이용한 피싱(Phishing) 공격방법

URL 스푸핑 등은 시스템의 파일이나 자원을 파괴하는 공격이 아니고, 사용자에게 잘못된 정보를 보여주는 공격이다. 이 공격은 주로 Phishing과 같은 사용자를 기만하는 사회공학적 공격의 일부로 사용된다.



스푸핑 기법을 이용한 자주 사용되는 피싱 공격 과정은 다음과 같다.

(1) 공격자는 보안이 허술한 특정 사이트를 해킹하여 위장사이트를 설치한다. 이때 설치하는 페이지에 URL이 위장할 원래 사이트의 주소로 표시되도록 프로그램을 삽입한다.

(2) 공격자는 임의의 인터넷 사용자에게 이메일에 거래하는 금융기관 등의 개인정보를 수정하라는 내용을 수록하여 송신하고, 특정 링크를 클릭하도록 유도하여 (1)에서 확보한 위장사이트로 접속하게 한다.

(3) 메일을 수신한 피싱 피해자는 공격자가 유도한 위장사이트에 접속하여 주소표시줄이 자신이 거래하는 금융기관임을 확인하고, 사이트가 지시하는 대로 개인정보를 입력한다.

(4) 공격자는 피해자가 입력한 개인정보를 사용하여 금융기관으로부터 경제적 이득을 취한다.

이와 같은 피싱 공격 중 (3)과 같이 피해자가 자신이 거래하는 금융기관의 인터넷

사이트임을 확인하였지만, 실제로는 공격자의 위장사이트이다.

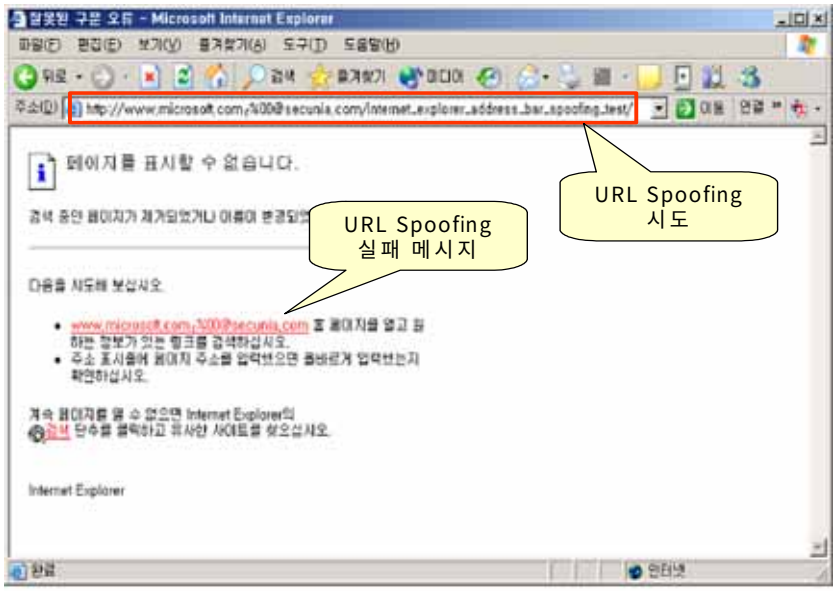
IV. 대응방법

o 최신 패치의 적용

URL Spoofing 등 스푸핑을 방지하기 위해서는 사용하고 있는 인터넷 탐색기의 최근의 패치를 확인하고 적용하여야 한다. 마이크로소프트 IE의 경우, 윈도우즈 XP/SP2 버전이 아니라면 IE 5.0, 5.5, 6.0등 모든 버전에서 이러한 공격에 노출되어 있다. 그러므로 SP2를 설치하거나 최신 보안 패치를 모두 설치하여야한다.

※ IE의 경우, Windows XP의 SP1에서 최신 패치를 모두 적용한 경우에도 (2004. 10.19 현재) 일부 취약

윈도우 XP/SP2는 현재 알려져 있는 URL Spoofing 등 공격에서 안전하고 알려져 있지만 주의하여야 한다. 이 밖에, 마이크로소프트 IE가 아닌 오페라, 모질라 등 공개 인터넷 탐색기도 유사한 취약점이 공개되었으므로 최신 패치를 설치하여야 한다.

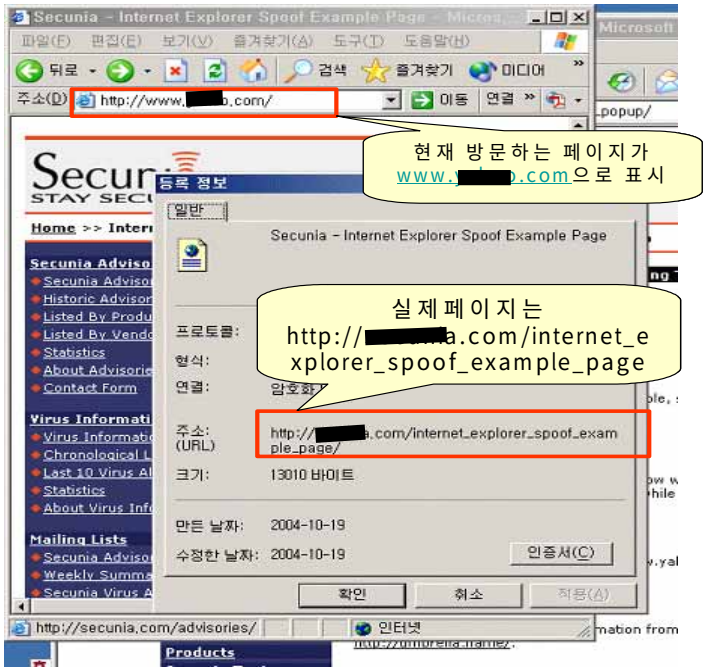


(그림-7) 패치시 URL 스푸핑 공격 실패

o 방문하고 있는 페이지의 주소 확인

방문하고 있는 페이지의 주소가 위조되어 있는지 아닌지 확인하는 방법은 해당

페이지의 속성을 확인하면 된다. 페이지의 속성은 IE의 "파일" 메뉴에서 "속성"을 선택하면 된다. 속성을 표시하면 현재 탐색기에 표시된 페이지의 원래 URL이 표시되므로 주소가 변조되었는지 확인할 수 있다.



(그림-7) 실제 URL 확인방법

※ 위 그림에서 IE 위도우의 주소창은 http://www.OOO.com이지만, 표시된 페이지의 실제 URL은 http://□□□.com/internet_explorer_spoof_example_page임

V. 결론

KrCERT의 해킹바이러스 통계 보고서에 따르면 피싱사고는 계속적으로 증가하고 있다. (10월말 현재 총 144건이나 7, 8, 9, 10월은 113건으로 78%를 차지함) 아직까지 국내에서는 피싱에 의한 금전적인 피해가 보고되지는 않았지만 미국의 경우 그 피해액수는 5억달러에 달한다고 보고되었다.

특히 주목할만한 점은 기존의 피싱은 사회공학적인 방법으로 사용자를 조작된 사이트로 유도하였으나 요즘에는 IE 등의 스푸핑 기법과 조합하여 더 교묘하고 적극적인 방법을 피싱에 이용하고 있다는 것이다.

이에 대응하기 위해 사용자는 최신 보안패치 및 서비스 팩으로 업데이트하고, 개인정보를 요구하는 이메일은 바로 삭제하고, URL 위조 등 출처가 의심스러운 사이트는 URL 주소를 직접 입력하거나 필히 재확인 하여 피해를 당하지 않도록 한다.

이와 같은 스푸핑 등에 의한 피싱 등 사고 예방을 위해서는 중요한 홈페이지를 운영하는 운영자들이 홈페이지 인증서 등을 사용하는 적극적인 방법으로 자신의 홈페이지가 정상적인 페이지임을 인증하는 방법들을 사용할 수 있다. 그러나 현재 홈페이지를 인증하는 서비스는 일반적으로 사용되지 않고 있으므로 피싱 등에 의한 피해를 방지하기 위하여는 이와 같은 공격방법들을 이해하고 항상 확인하는 방법이 최선이다.

□ 참고사이트

1. http://secunia.com/
2. http://www.securityfocus.com/
3. http://www.microsoft.com/
4. http://www.krcert.or.kr/