

[NT] Address Bar Spoofing Attacks Against Microsoft Internet Explorer 6

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-10/msg00071.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 28 Oct 2008 09:28:17 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Address Bar Spoofing Attacks Against Microsoft Internet Explorer 6

SUMMARY

IE6 is the second most popular web browser (after IE7), with market share of around 25% (according to recent surveys e.g. <http://marketshare.hitslink.com/report.aspx?qprid=2>).

This write-up presents two new phishing attack techniques, abusing an address bar issue (security vulnerability) with IE6 in combination with non-standard DNS domain names. The net result is that a phishing site may present itself via a link that when clicked in IE6 displays an almost indistinguishable URL from the one in used by the genuine site. The technique is new, i.e. it's different than the ASCII similar characters and IDN homographs attacks.

There are two techniques: the first technique presents an address bar which is very similar (visually) to the address bar expected for the genuine domain, by abusing the NBSP character. The second technique presents an address bar visually identical to the one expected for the genuine domain, using the fact that a non-DNSish characters are not displayed in the address bar in some cases. This technique requires

registration of a non-standard domain, hence it is probably theoretic only (although "site down" imitation is still possible).

The attacks were verified with Windows XP SP2 and Windows XP SP3.

DETAILS

Introduction:

URLs typically include host name, which tells the browser (after DNS resolution) where to fetch the resource from. While regular host names contain alphanumeric characters (a-z, A-Z and 0-9), dots, hyphens and (in Intranets only) underscores, it is possible to construct (at least syntactically) URLs whose host part contain any octet (as explained in RFC 1035 section 3.1). The interpretation of such characters when presented as links (when IDN is not supported by the browser, see below) by the browser and by the DNS infrastructure, as well as the way those characters are presented by the browser (in the address bar) are the subject of this write-up.

Non-DNS characters can be provided to the browser in several ways (assuming e.g. an anchor HTML tag context):

- * In raw form, i.e. as a byte (octet), e.g. \$
- * In HTML-encoded form, e.g. $
- * In URL-encoded form, e.g. %24

In raw form, the data is provided as-is. In HTML-encoded form, the data is considered Unicode, and may undergo encoding. In URL-encoded format, the data is (again) directly decodable into raw form. The difference is subtle, but important. The octet values 00-7F (corresponding to the ASCII characters) have a single interpretation across all systems. However, octet values 80-FF may have different interpretation depending on the code page and encoding system in use.

Address bar spoofing in IE6

Non-DNS characters

Within the ASCII range (00-7F), only the DNS subset of ASCII characters is allowed. As for higher values (e.g. A9 or %A9): IE6 uses DnsQuery_A to resolve the name. DnsQuery_A assumes that the characters are in the "current" Windows ANSI codepage (e.g. Windows-1252 or Windows-1255, see <http://www.microsoft.com/globaldev/reference/WinCP.msp#> <<http://www.microsoft.com/globaldev/reference/WinCP.msp#> for a list of Single Byte code pages). It translates the characters into UTF-8 representation and sends them this way. So %A9 is URL-decoded into the byte (\xA9) by IE6, then this raw byte is forwarded to DnsQuery_A, which interprets it according to the current codepage (e.g. Windows-1252 or Windows-1255) as COPYRIGHT_SIGN, moves to Unicode (U+00A9), and UTF-8 encodes this symbol (into the 2 byte sequence (\xC2) (\xA9)). The net result is that <http://www.foo%A9bar.com> goes out as a DNS query on [www.foo\(\xC2\)\(\xA9\)bar.com](http://www.foo(\xC2)(\xA9)bar.com).

As it happens, almost all single-byte character sets


```
sp: &n  
bsp: .  
_phish.site/">YourBankHere</a>
```

It should be noted that auto-complete does work for these URLs.

When the address bar box is not wide enough to show the whole URL, the picture is almost identical to that of the genuine URL (notice there's no slash after the host name, and the additional dots). When the address bar is at its full width, some users may still be fooled as the real domain is way off to the right, separated from the left part of the hostname by many white spaces. This shows up visually as (may wrap around in the text):

```
http://www.yourbankhere.com  
_phish.site/
```

The attack can be easily implemented using DNS wildcard mapping, assuming the attacker controls the phish.site domain. The attacker simply needs to add the following line for the phish.site zone configuration file (tested with BIND9):

```
*_phish.site. IN A ...IP address...
```

Note that the Host header will contain raw 0xA0 bytes. So by including the following PHP code in the index.php of the phishing server, the attacker can cater for multiple simultaneous phishing attacks:

```
<?php  
$match=array();  
preg_match("/^([a-zA-Z0-9 .-]+)\xA0/",  
$ SERVER['HTTP_HOST'],$match);  
echo "This is a phishing site for ".$match[1];  
?>
```

Attack #2 (theoretic): URL-encoded characters

It's possible to include URL-encoded characters in the address bar of IE6. IE6 URL-decodes them before querying the DNS, and internally this is how they are kept.

Now, here's where it gets interesting: high-bit characters will not be displayed in the address bar. So instead of showing visually as "http://www.foo%A9bar.com/ (or "http://www.foo(c)bar.com/") as one may expect, the address bar will show "http://www.foobar.com/.

Theoretically, this can be used for phishing. A phisher can register, say foo(\xC2)(\xA9)bar.com and use that in a phishing URL (http://www.foo%A9bar.com/). When clicked, the IE6 address bar will display the expected URL, http://www.foobar.com/. However, this vulnerability seems to be theoretic only, since (in the author's limited experience), it's not possible administratively to register such domain names.

[NT] Address Bar Spoofing Attacks Against Microsoft Internet Explorer 6

As for domain security, as far as IE6 is concerned, these are two different domains. Cookies are not shared, access across domains is denied, SSL certificate will not match, etc. Also, the Host header includes the value with the original raw character – i.e. the Host header is:

Host: www.foo(\xA9)bar.com

Even if no real domain can be registered, this can still be somewhat of an annoyance. For example, spam can offer a URL as evidence that a company's site is not available, or was hacked. So if an attacker wants to defame www.foobar.com, he may do so by sending spam with text such as "foobar inc. went chapter 11 – site is down. Check out http://www.foo%A9bar.com/. This will end up in DNS resolution failure.

Auto-completion applies to the address bar string (not the real URL), hence auto-completing, say, www.fo will result in www.foobar.com (the real domain name), and the browser will navigate to the genuine site.

Vendor status:

Microsoft (MSRC) was informed of the two issues on January 13th, 2008. MSRC acknowledged the two problems and assigned the first one the ticket MSRC7899, and the second one MSRC7900. However, Microsoft declined to fix the issues.

ADDITIONAL INFORMATION

The information has been provided by <mailto:amit.klein@xxxxxxxxxxxx> Amit Klein.

=====

This bulletin is sent to members of the SecuriTeam mailing list. To unsubscribe from the list, send mail with an empty subject line and body to: list-unsubscribe@xxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxx

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind. In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.