

## Re: Outlook hijacked

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2004-02/0479.html>

---

**From:** Billy O'Connor ([billyoc\\_at\\_gnuyork.org](mailto:billyoc_at_gnuyork.org))

**Date:** 02/21/04

Date: Sat, 21 Feb 2004 03:21:33 GMT

zrep@ngoc.com (R Pierce) writes:

> *I have XP Pro on a DSL connection, with XP Firewall enabled. Despite  
> all the flack it gets, all of the online "testers" of firewall  
> security never find any holes in my system.....  
>  
> Today, while my wife was typing an email, someone started typing on  
> the email with her. They mimicked words that she or her prior  
> correspondents had used in older emails (as if they had been read  
> previously. My wife typed who is this?...reply was "This is  
> -----".....She then typed "Where are you?"...the reply was "in your  
> house..."*

Get that hulk off the network, \*now\*.

> *Clearly somebody was online with her real-time. After this short  
> exchange, all kinds of odd word combinations were typed on this email,  
> things like, "man at 10 o'clock, man and a half, man and woman,  
> etc..over and over and over.  
>  
> I cannot see that any of my personal files were opened, as judged by  
> modification dates.*

Did you check all of your hidden/cookie files and the registry?

Well, it doesn't really matter, you're compromised.

>  
> *Is it possible for a hacker to look into unopened emails? One of the*

Yes, the attacker has full control of that machine now, if they can  
"type" into an email you're composing.

> *parts of the email was actually a reference to a new email my wife had  
> yet to read.  
>  
> How is this accomplished? It is as if someone had a remote assistance  
> request from us somehow, which was not the case here. Besides*

comp.security.misc: Re: Outlook hijacked

Yes, that probably *\*was\** the case, you could be compromised simply by visiting a malicious web site.

> *unhooking the PC from DSL or turning it off is there anything else I*  
> *can do? Another firewall program? Any ways to find out who this was?*

Unplug that computer from the network *\*right now\**. Format the drive and reinstall an operating system.