



Previous: [Black Hat 2008 Wrap Up](#)

Next: [BGP in the News](#)

## The Phish That Bites Back

August 25, 2008 by Joe Stewart

Filed under [General](#), [Phishing](#) category.

We all get phishing emails. Some of us more than others, so it's no surprise that sometimes people take out their frustrations on the phishing form, letting the phisher know just what they think of him or her.

Please fill in the confirmation form. All fields of the confirmation form are required.

|                         |                             |
|-------------------------|-----------------------------|
| <b>Organization ID:</b> | Phish this!                 |
| <b>User ID:</b>         | I got yer phish right here! |
| <b>Password:</b>        | ●●●●●●●●                    |

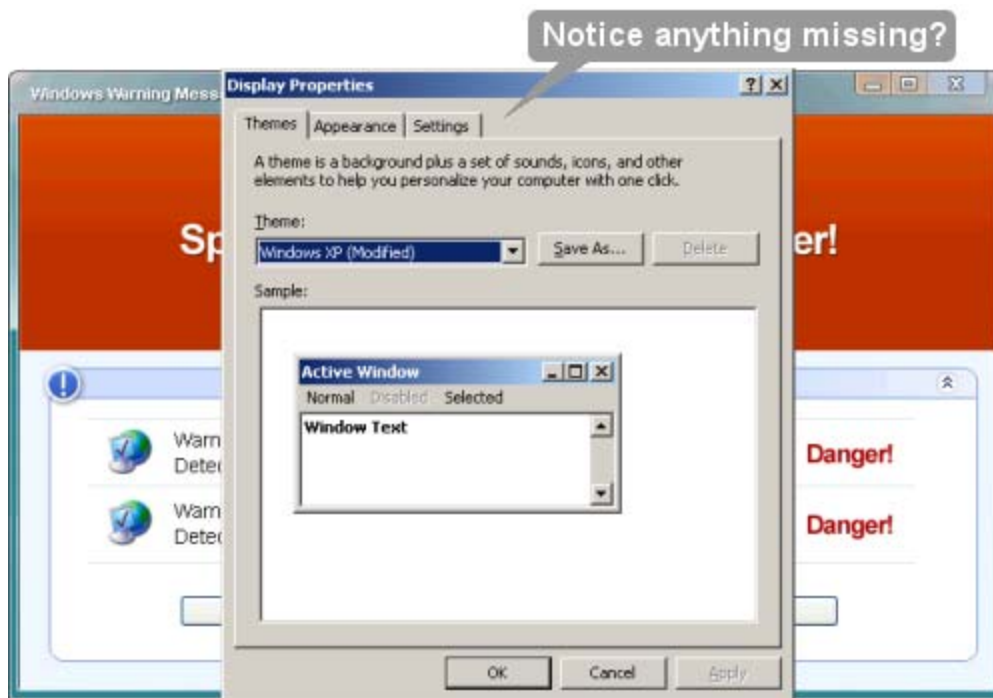
**Confirm & Exit**

While it might make you feel better, it isn't always a good idea. For instance, if you were to do this on a phishing page hosted by the [Asprox botnet](#), you might get more than you bargained for. The Asprox phishing form backend has a bit of extra logic added to it. If the form looks like it has been filled out with legitimate data, you get redirected to the main page of the bank website.

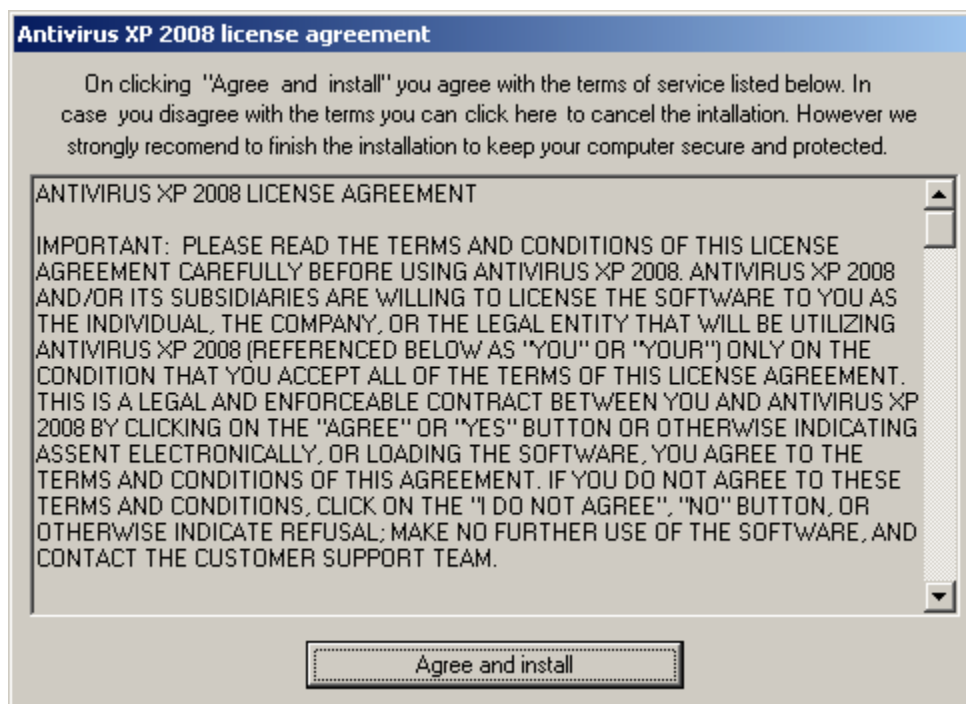
However, fill it out incompletely or use certain words like "phish" or NSFWUYAS (Not Safe For Work Unless You're a Sailor) language, and your browser will be subjected to a number of exploits. If you are running Windows and haven't recently installed your security updates and patched all your browser plugins/ActiveX controls, you might find yourself infected with your very own copy of Asprox.

Not only do you then get the opportunity to unknowingly send phishing emails on behalf of the botnet, you will likely get some extra goodies, since Asprox is also a downloader trojan. You won't notice it running, but you might notice some of the things it downloads and installs.

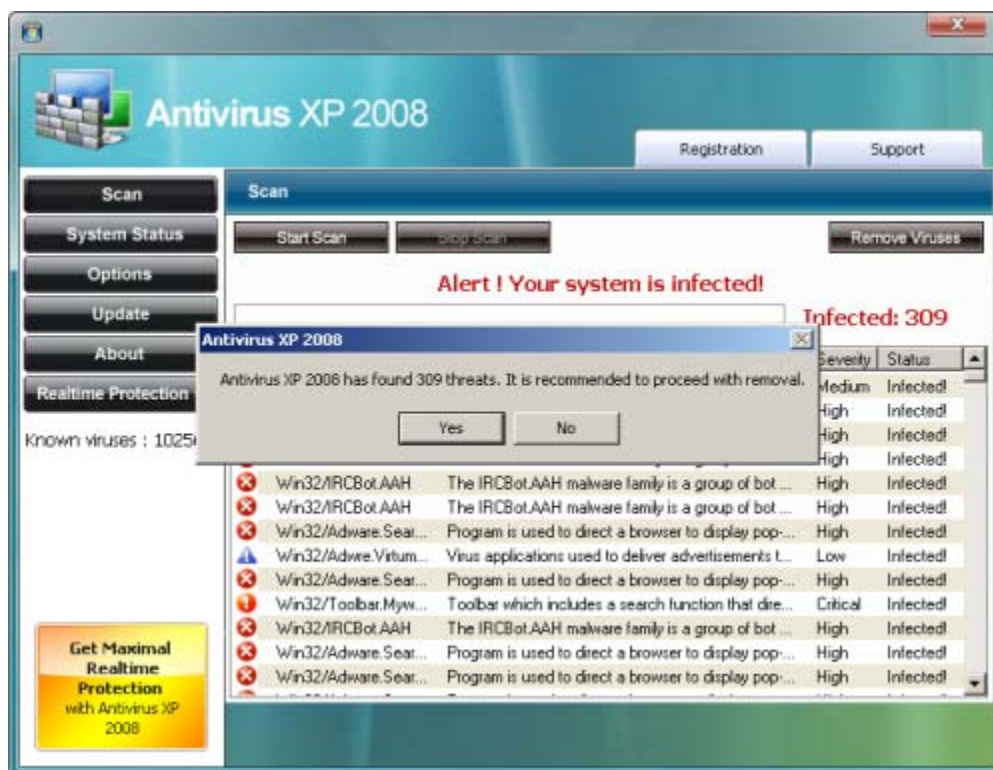
For instance, you might find your desktop wallpaper changed to a "spyware alert" type of message, and now all your screensaver shows is scary blue-screens-of-death. Of course, if you're familiar with the Windows desktop properties dialog, you can change all that back, right?



Oops. the rogue antivirus program has removed that functionality for you. But hey, at least it gives you a chance to look over the license agreement, right?



Except you'll notice the lack of a "I disagree" or even a "close window" button at the top of the dialog (which can't be minimized, and stays on top of all your other windows). So there's no easy way to continue using your computer without clicking on the "Agree and install" button. But don't worry, Antivirus XP 08 has already installed itself, whether you click through the license agreement or not. Eventually you will see this:



Of course, you're not infected with everything this program says you are - it's scareware, designed to get you to fork over \$50 or \$100 in order to clean your system of all these nasty threats. But it doesn't actually detect or clean anything, especially not the Asprox bot you're hosting now.

And at any time, Asprox might deliver another malicious payload and install it for you - and it could be much worse: we've seen the Zbot banking trojan installed by Asprox in the past. So instead of a dealing with a nuisance program, you might be silently sending your banking and credit card information to the botnet owners. Something to think about before venting your frustrations on the bad guys. Sometimes phish bite back.

This entry was posted on Monday, August 25th, 2008 at 12:52 pm.

Share This Information | [The Phish That Bites Back](#)



#### Other SecureWorks Blog Categories:

- [General](#) (25)
- [Links](#) (7)
- [Phishing](#) (3)
- [Research](#) (68)
- [Spam](#) (1)
- [Trojans](#) (4)

Printed from <http://www.secureworks.com>

For more information, please call (877) 905-6661 or email [info@secureworks.com](mailto:info@secureworks.com).