DontBlockTheBat

Don't Block "The Bat!"

A lot of spam claims (in the User-Agent or X-Mailer header) to come from a program called "The Bat!", and it may appear attractive to block this. However, this is a bad idea.

The Bat! is a legitimate email client which, like Outlook and Eudora, is often falsely impersonated by spamware. It is generally advisable for spammers to fake this header to look like a real mail client, as best they can, because it makes spam detection harder. So they do.

Spamassassin will tag and score messages that claim to be from the Bat that it can tell isn't really (just as is does for obviously false Outlook X-Mailer headers). In fact, The Bat's development team have been very helpful in this regard, providing lots of good tips on ways to tell *real* Bat mail from the fake stuff.

as MattKettler put it:

'In reality nearly all spam is generated by custom software that runs in the background on infected PCs in botnets.

Think about it, the mail viruses that infected the PC in the first place can generate emails to spread themselves.. Spamming activity is simply good reuse of the same code.

So, your spam was probably generated by a fragment of code from the Storm worm, mydoom, bagel, etc, possibly glued together with some other code for the differing payload needs.

But no spammer is going to be foolish enough to put:

User-Agent: Storm Worm Botnet v 3.12.0

But we can all dream... 🙂'