In recent articles, I’ve been looking briefly at some of the nasty ways that spammers are eluding search-string-based anti-spam filters. I mentioned that because many of these messages now put their text into images to avoid the scanners, we are forced to pay more attention to the domains mentioned in the body and in the e-mail headers.

The headers are problematic: the criminals who send spam think nothing of forging their headers to evade filters and to escape retribution (legal and illegal). Nonetheless, I have noticed a few major spam houses who have been using yet another trick in their attempts to infiltrate our in-boxes: they use domain names with constantly-changing server names. Thus, for example, I noticed that a particularly bad spam house (let’s call it, say, “badspammers.com”) is now sending out its useless ads for useless products using addresses ending in “@a.badspammers.com,” “@b.badspammers.com,” “@c.badspammers.com” and so on. Unfortunately, the anti-spam tool I’m currently using (maybe not for long) seems to be having trouble parsing these domain names; even though the rejection list includes “@badspammers.com,” it regularly allows the e-mail from a new variant to get through. Clearly, anti-spammer software has to be able to cope with this elementary technique when looking at the headers.

More important, though, is that any spam where the nasties expect to receive a response is going to have to have some reliable address in it – whether a real e-mail address (rare) or a Web URL. I think that these real contact points are a true vulnerability for the Bad Guys: by compiling shared lists of the contact addresses used by the people advertising via spam, it should be possible to spread the signature files widely to users and perhaps to all anti-spam providers.

The situation reminds me of the early days of the antivirus industry; when I was the first Secretary of the Anti-Virus Product Developers’ Consortium (AVPD) sponsored by the then-NCSA (later ICSA Labs and TruSecure) in the early 1990s, the idea of sharing virus signature strings among competing antivirus vendors struck some observers as ludicrous. However, I remember Bob Bales and Paul Gates arguing with the vendors that it was no stranger than having medical or biochemical information about diseases and toxic materials shared among competing pharmaceutical companies: the companies could compete on how well they fought the problems rather than concealing information about the problems. The industry agreed, and now antivirus companies routinely work with the AVPD and other organizations to share knowledge about new malicious software.

So I think that antispam software developers ought to be sharing knowledge of the spam recognition strings too. After all [I can hear the complaints already] domain thing is to fight the spam.

* * *

For further reading:
MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.