Still more creative uses for CAPTCHA

devblogs.microsoft.com/oldnewthing/20040316-00

March 16, 2004

Raymond Chen

I want to say up front that I think CAPTCHA is a stupid name. CAPTCHA stands for "Computer-Aided Process for Testing…" something something. Why do people feel the urge the create some strained cutesy acronym for their little invention? Anyway, it has already been noted how spammers are getting around these tests by harvesting a practically-free resource on the Internet: the desire to see pornography.

> Someone designed a software robot that would fill out a registration form and, when confronted with an image processing test, would post it on a free porn site. Visitors to the porn site would be asked to complete the test before they could view more pornography, and the software robot would use their answer to complete the e-mail registration.

Ah, remember the days when you had to whisper the word "pornography"? Anyway, it looks like the virus-writers have also taken the two-edged sword and pointed it in the other direction. (Ah, another one of Raymond's tortured mixed metaphors.) As you may be aware, the latest trend in virus-detection-avoidance is to attach an encrypted ZIP file, since virus-checkers don't know how to decrypt them. To get the sucker to activate the payload, you put the password in the message body. Well, virus checkers figured this out rather quickly and scanned the message body to see if there's a password in the text. Now the virus-writers have upped the ante. The Bagle-N virus attaches an encrypted ZIP file and provides the password as an image, using the same trick as the anti-robot people. Fortunately, the image generator they use is pretty easy to do OCR on, since they don't make any attempt to fuzz the images. I predict the next step will be that the virus-writers send **two** messages to each victim. The first contains the payload, and the second contains the password. That way the virus-scanning software is completely helpless since the password to decrypt the ZIP file isn't even in the message being scanned! Once again, just goes to show that social engineering can beat out pretty much any technological security mechanism.

(I think virus scanners are now starting to block any password-protected ZIP. But that won't stop the viruses for long. They'll just have a link to a ZIP file or something.)

Raymond Chen

Follow