

New weapons needed for the war on junk email

Today's spam filters are highly effective, but they may be no match for spammers seeking new ways to fool people into visiting commercial websites or downloading rogue software carrying viruses, worms, spyware, or other dangerous applications, says John Aycock, an assistant professor of computer science at the University of Calgary.

Aycock and his student Nathan Friess conducted new research that shows it is possible to create a new type of spam, or bulk email, that would likely bypass even the best spam filters and trick experienced computer users who would normally delete suspicious email messages.

"Two things typically distinguish today's spam," says Aycock, who monitors potential computer hazards in an effort to block harmful effects. "It comes from an unknown source and contains content that is easily recognizable as spam because of obvious advertising, outrageous wording or gibberish." The next generation of spam, however, could be sent from your friends' and colleagues' email addresses – and even mimic patterns that mark their messages as their own (such as common abbreviations, misspellings, capitalization, and personal signatures) – making you more likely to click on a web link or open an attachment that could harm your computer, spy into your hard drive, or steal your personal information.

Aycock and Friess will present these findings--and some new solutions--on April 30 at the 15th annual conference of the European Institute for Computer Anti-Virus Research, being held in Hamburg, Germany. The aim of the research is to raise awareness of the potential threat so that anti-spam software can be written that anticipates spammers' next moves and protects business and personal computers.

"We want to look at potential threats and see what we can do about them right now, as opposed to getting to the point where we're forced to react," says Aycock.

In the past, spammers have tried to increase their effectiveness by sending huge volumes of email, in the hopes that a few messages would inevitably sneak past automated spam filters. Spammers' ultimate success, however, depends upon their ability to trick people into clicking on links or downloading attachments.

Most spam is now sent from so-called zombie computers – vast networks of remote computers that have been infected by rogue software, called "malware," which can be used to automatically send bulk email messages. Based on the new research, Aycock thinks that spammers could soon use zombie computers in a totally new way. Instead of housing only spam generating software, infected zombie computers could also house programs that spy into a person's email, mine it for information, and generate realistic-looking replies.

Such a specific, targeted approach has previously been viewed as too complex to be worth spammers' efforts. But Aycock and Friess tested one part of this hypothetical new approach, showing that it is not only possible but relatively easy to automatically generate this new type of spam. They used two pools of email – one which they generated manually and another that came from publicly available Enron databases that were released after the company's collapse.

A computer program mined the data in both email pools, finding statistically significant patterns of abbreviation, capitalization and signatures. A second program used these patterns to automatically transform a standard, one-line spam message into convincing, individualized replies.

The new approach hasn't been used by spammers yet, but Aycock says it's only a matter of time before they

begin to exploit resources already at their fingertips.

"All the pieces are in place right now," he says. "Spammers are using zombie networks, spammers have access to email accounts, spammers know that spam filters are catching most of their messages. They're looking for ways around those defences. Also, data mining has been used for a long time by lots of people. And what we're talking about is very simple data mining. At some point, the other shoe has to drop."

If the weapons are within reach, so are some solutions (see background). "The new solutions are not difficult," Aycock says. "They're all within technical reach right now. They're just not packaged nicely like some other anti-spam solutions."

Aycock hopes that companies that make anti-spam software and email programs will take advantage of the new information and quickly integrate some of his suggested solutions into existing software suites. He also recommends that business and personal computer users remain vigilant and keep their existing defences up to date in order to prevent their computers from becoming infected "zombies."

"Existing spam software is nearly 99 percent effective against current spam techniques, and anti-virus software is still the best defence against malicious software," he says. "It's generally a good practice to have multiple defences on your computer, so if one thing fails, another exists to catch the threat," Aycock says.

Source: University of Calgary

This document is subject to copyright. Apart from any fair dealing for the purpose of private study, research, no part may be reproduced without the written permission. The content is provided for information purposes only.