The Web: 'Bots' pushing poll results

By Gene J. Koprowski

United Press International

Published 10/13/2004 12:26 PM
CHICAGO, Oct. 13 (UPI) -- President George W. Bush and Sen. John F. Kerry will walk across the stage Wednesday night and greet each other at the beginning of the third and final presidential debate. Already, across the country, e-mail messages are arriving in newsroom inboxes declaring a winner.

A new form of spam is emerging this fall, called debate-spin spam, experts told UPI's The Web. The veracity of the e-mail messages being sent as letters to the editor is coming into question, as are the timing and content of many of the messages, because a significant percentage is being generated by bots, or intelligent software agents.

"In the world of politics, there are good bots and bad bots," said Christopher Faulkner, chief executive officer of C I Host, an online hosting service in Bedford, Texas. "There are hundreds of bots available for spamming or political use."

For example, BotSpot.com makes available a bot known as "Mr. Smith E-Mails Washington," which occupies a high-profile in the computing community, because it is intended for consumers to use to e-mail members of Congress. Bots also can be customized quite easily, too, and can send out millions of messages in minutes.

"For these political-action groups, many of them probably set up their own in-house servers," Faulkner told The Web. "All it takes is a little know how and a little bandwidth."

During the first presidential debate, OpinionJournal.com, published by The Wall Street Journal, reported its letters editor received about 3,500 e-mails. The Washington Post wrote an editorial about the influx of e-mail it received, some declaring a winner to the debate before it had even commenced. Other news organizations, including UPI, also received suspect letters, including three versions of the same letter, purportedly from different accounts.

"When they're doing a mass mailer, they don't log into Google and get Gmail and send them out one by one," Dan Forootan, founder and president of EZ Publishing Inc., an Internet hosting company in Davis, Calif., told The Web.

The messages may come from public Internet addresses, such as Google or Yahoo, but experts said it is surprisingly easy to forge the header of a reputable firm and send e-mail from its address.

"This is a sophisticated version of spin," said John McIntyre, founder of RealClearPolitics.com, a political site in Chicago.

During the debate Sept. 30, UPI received a number of e-mails from Gmail accounts -- accounts whose owners cannot be verified.

"Bush keeps trying to tell us that Iraq is part of the war on terror," said one of the messages.

Another e-mail, hewed to a similar theme, said "President Bush's message seems to be more along the lines of 'we won't give up, we will not pull out, the world is safer under my watch.'"

Yet another e-mail that evening, received before the debate had concluded, claimed that the writer could "hardly believe it when President Bush said he invaded Iraq because the enemy attacked us. Iraq didn't attack us. Osama bin Laden did -- and George W. Bush gave the terrorist leader exactly what he wanted."

McIntyre said such e-mails are similar to the telephone calls he received when he was on WGN-AM radio in Chicago, giving analysis on The Milt Rosenberg Show the night of the debate.

"We received a couple of calls that were highly suspect," he told The Web. "I was skeptical as to whether they were legitimate calls. They were so scripted. They were what a campaign would want the caller to say: 'I was for Bush in 2000. I was undecided. Now I am for Kerry.' It sounds too perfect."

There are ways to determine if incoming e-mail is political spam, experts said.

"You can check the header and body of the message," explained Tom Buoniello, vice president of product management at Sybari Software Inc., an anti-spam software developer in East Northport,

N.Y. "You have to set this up at the server level, not at the client (individual PC) level, but you can determine if the system has seen a similar message before."

Anti-spam software examines the route that a message took, and then uses recurrent-pattern detection techniques to see if others took the same route over the Internet, or originated from the same server, he explained.

"You can classify the e-mail in one of four ways," Buoniello told The Web: "It's not spam and is probably real. It is 100 percent spam, and you've seen it several times in one day. It's probably spam, but you are not 100-percent certain. Or, it might be spam -- hold it at the gateway and don't deliver it for a few minutes."

The reason anti-spam software can intercept suspect messages at the gateway is that spammers send out messages en masse. The software watches to see if messages arrive within a few minutes of one another containing similar text, or routing patterns or headers. If so, they can be snagged, he said.

The capability to write mass e-mail messages -- and have computers write the content -- has been around for years for sophisticated users of Unix systems, Mark Gruensfelder, manager of solutions engineering at Infocom Systems Inc. in Iselin, N.J., told The Web. "The program itself can generate the content."

Sales departments at many major companies use automated programs to send messages to prospects and customers all the time -- with reply to a third-party address, such as the sales manager, inserted on the header, for the recipient to see.

Bots now make it even easier to do, experts said. They even can participate in online polls, or generate news stories based on poll results, rather than reflect actual public sentiment.

Some political supporters of a particular candidate may grant permission to the campaign to use their e-mail addresses to send out letters, experts said.

"But it becomes quite nefarious when someone is spoofing someone else's legitimate e-mail address," Mark Pruner, an attorney and vice president of marketing at RD Legal Funding LLC in Englewood, N.J., told The Web.

With the rise of political spam, the effectiveness of it is likely to decrease.

"There is a real proliferation of this kind of software," Amy Showalter, president of the Showalter Group Inc., a political consulting firm in Cincinnati, told The Web. "But when everyone uses the same tactic, people question whether it is really authentic. We find that (whenever) the software that allows 'robo letters to the editor' is used in full force, its PQ -- or persuasion quotient -- has yet to be determined."

--

The Web is a weekly series by UPI examining the global telecommunications phenomenon known as the World Wide Web. E-mail sciencemail@upi.com