Comcast tries pop-up alerts to warn of infections

October 10 2009, By DEBORAH YAO , AP Business Writer

(AP) -- Comcast Corp. wants to enlist its customers in a fight against a huge problem for Internet providers - the armies of infected personal computers, known as "botnets," that suck up bandwidth by sending spam and facilitating cybercrime.

The country's largest provider of high-speed Internet to homes started testing a service this week in Denver in which Comcast sends customers a pop-up message in their Web browsers if their computers seem to have been co-opted by a botnet. One botnet can have tens of thousands or even millions of PCs.

The message points to a Comcast site with tips for cleaning infected computers. It reads: "Comcast has detected that there may be a virus on your computer(s). For information on how to clean your computer(s), please visit the Comcast Anti-Virus Center."

Comcast said users can close the warning banners if they wish, but they cannot opt out of receiving them. A reminder will return every seven days while a computer appears to be infected.

The program, which Comcast hopes to roll out nationally, is one of the most aggressive moves yet by a major Internet provider to curb what's become a scourge on the Internet.

Botnets are a part of most serious cybercrime. They're used to steal credit card numbers, carry out so-called "denial-of-service" attacks that

bring down Web sites and send spam by hijacking e-mail accounts and Internet connections.

A computer can fall into the sway of a botnet when it is infected with malicious software that puts the machine under the control of criminals, who use the anonymity provided by having so many zombie machines at their disposal to cover their tracks.

Comcast's service is meant to block that step, by alerting customers to PC infections they likely didn't know about because anti-virus software updates can't keep up fast enough.

Comcast will try to detect a PC's role in a botnet by studying how much data the machine is downloading and receiving.

"These cyber criminals have become so fast, a bot can be instructed to send out millions of spams in a matter of minutes," said Jay Opperman, Comcast's senior director of security and privacy. "The faster that we can detect these things are operating on our network, the better."

He said Comcast can tell the difference between a customer legitimately downloading a lot of video or other data and the malicious deeds of a bot-induced PC. One way is that the company checks the source of downloads, Opperman said, to compare them to a list of suspect sites that are known for spamming and other attacks. Opperman said Comcast will not look inside the content of the traffic, a controversial process called deep packet inspection.

Even so, the move could be risky, especially if Comcast's program gets people to trust and respond to pop-up ads - which are often a vehicle for delivering the viruses that land an infected computer in a botnet. These phony ads often claim that a computer is infected and should be cleaned up with a click.

Comcast says its program contains an important secondary confirmation that the message is from the company and not a scammer: Comcast will send an e-mail to the customer's primary e-mail account.

However, Phil Lin, marketing director at network security firm FireEye Inc., said hackers could mimic Comcast's pop-up banner or the confirmation ads. And unsuspecting customers wouldn't know they should expect to see a confirmation from Comcast in the first place.