<< Back to Article

AIM Hack Shows AOL Hasn't Patched Critical Security Hole

By Ryan Singel 12.05.07 | 12:00 AM

Virginia-based AOL quietly issued a security fix to its AIM instant messaging system this week, after a security researcher demonstrated for Wired News that the company had failed to properly close a September security hole allowing hackers to gain complete control of any PC running the latest version of AIM.

"It could take over 60,000 computers in two days, but I don't want to," says 31-year-old programmer Michael Evanchik, who developed the new attack. "It's a pretty big hole. You don't even have to click anything."

The hack highlights a key difficulty for AOL as it attempts to compete with sites like Facebook and MySpace that feature their own instant messaging systems. AOL has responded by turning its popular AIM client into a multimedia portal, adding extra features that make it easier for hackers to attack the downloadable software.

In October, the company released AIM 6.5 partially to fix a critical vulnerability in how the software handles HTML code. But security experts criticized AOL at the time for rushing out a half-baked solution, and relying heavily on server-side filtering to try and prevent malicious code from traveling through AOL's network. Securing the client from this class of attack could require sacrificing some multimedia functionality.

Monday night's silent server-level patch demonstrates that those experts were right: The AIM 6.5 client remains vulnerable to the same fundamental weakness, potentially allowing malicious hackers to create a worm that infects thousands of users in a matter of hours.

"Instead of locking down the AIM client, they add filters in the server," says Aviv Raff, the security researcher who reported the original remote exploit in September, and who analyzed the newest attack for Wired News. "Filtering in the server will never be enough. It's like a cat and mouse game."

Raff said that as soon as AOL told him they fixed his September exploit, he quickly developed functioning variants himself -- an easy process since the company was essentially filtering by keywords.

AOL spokeswoman Erin Gifford , however, says all is well.

"We have taken steps to protect users from this known and reported issue," said Gifford, after Wired News reported the issue.

Evanchik said he was moved to develop the attack after an anonymous MySpace user began harassing his sister. He planned to use it to deliver a homemade key logger to the user's machine, though he says he hasn't done so.

His attack was a single line of JavaScript that performed two functions. First, it set up an error handler that would download and run a malicious file from the internet. Then it directed the AIM client to try and display a non-existent image from the web. Because the image link was broken, AIM 6.5 followed the error instructions and turned over the victim's computer to the attack.

AOL's response was to add Evanchik's specific attack string to the company's server-side filtering software. AOL says that's good enough, and it doesn't expect to see any more exploits.

"We feel confident we have gotten all the problem issues resolved," Gifford said.