



## Monster.com Took 5 Days to Disclose Data Theft

August 24, 2007

By Jim Finkle, Reuters

BOSTON (Reuters) - Monster.com waited five days to tell its users about a security breach that resulted in the theft of confidential information from some 1.3 million job seekers, a company executive told Reuters on Thursday.

ADVERTISEMENT

Hackers broke into the U.S. online recruitment site's password-protected resume library using credentials that Monster Worldwide Inc said were stolen from its clients, in one of the biggest Internet security breaches in recent memory.

### RELATED LINKS

- [Monster.com Shuts Down Rogue Server](#)
- [Monster Invites Job Seekers to See How They Measure Up](#)
- [Monster.com Gobbles Privacy](#)

They launched the attack using two servers at a Web-hosting company in Ukraine and a group of personal computers that the hackers controlled after infecting them with a malicious software program known as Infostealer. Monstres, said Patrick Manzo, vice president of compliance and fraud prevention for Monster, in a phone interview.

The company first learned of the problem on August 17, when investigators with Internet security company Symantec Corp told Monster it was under attack, Manzo said.

"In terms of figuring out what the issue was, that was a relatively quick process," he said. "The other issue is you want to make sure exactly what you are dealing with."

His security team spent the weekend investigating, located the rogue servers, and got the Web-hosting

company to shut them down some time either late in the evening on August 20, or early in the morning of August 21, he said.

Manzo said that based on Monster's review, the information stolen was limited to names, addresses, phone numbers and email addresses, and no other details including bank account numbers were uploaded.

On August 21, Symantec published a report on its Web site that said it had found copies of scam e-mails that the engineers of the attack were using, with the aim of getting information that was more valuable than just the names and contact details of Monster.com users.

Pretending to be sent through Monster.com from job recruiters, the e-mails asked recipients to provide personal financial data, including bank account numbers. They also asked users to click on links that could infect their PCs with malicious software.

Their ultimate goal in taking the data from Monster.com was to gain enough personal information to lower the guards of target victims when they read the e-mails, said Patrick Martin, a senior product manager with Symantec's response team in Austin, Texas, which first identified the attack.

"It gives these spam e-mails just a little bit of credibility," Martin said. "These guys were trying to get financial information from people."

It wasn't until Wednesday, a day after Symantec issued the August 21 report, that Monster put a notice on its Web site, [www.monster.com](http://www.monster.com), warning users they might be the target of e-mail scams.

Monster then announced on Thursday that the details of some 1.3 million job seekers had been stolen. Fewer than 5,000 of those affected are based outside the United States, it said in a statement.

A company spokesman said Monster also posted letters to the 1.3 million affected users on Thursday in case the users were wary of opening e-mail from the company after the breach. He said Monster's database has about 73 million resumes.

The security breach comes at a rough time for the company, which in July reported lower-than-expected quarterly earnings.

Chief Executive Sal Iannuzzi, who took the company's helm in April, said on July 30 that he plans to cut 800 jobs, or 15 percent of Monster's full-time staff, in a bid to improve its financial performance.

[Copyright \(c\) 2007 Ziff Davis Media Inc. All Rights Reserved.](#)