Theft at Monster alarms experts

Scope of scam reveals new level of danger

By Hiawatha Bray, Globe Staff  |  August 31, 2007

Security specialists say that the alleged theft of information of millions of users of the Monster.com job-hunting website shows how cunning and dangerous e-mail scammers have become.

The attack on Monster Worldwide Inc., a New York company with its operations center in Maynard, apparently was intended to acquire millions of e-mail addresses of Monster users. These could then be targeted by phony "phishing" messages appearing to come from Monster. Because the recipients already had dealings with Monster, they would be more likely to follow the instructions in the messages.

It's called "spear-phishing," the careful targeting of phishing messages to those most likely to be fooled by them. The practice is nothing new, but Richard Wang, research manager at the Burlington laboratory of computer security firm Sophos Inc., said the Monster scam suggests a new level of sophistication. "I haven't heard of it on the sort of scale we saw at Monster," Wang said. "That may simply be because it hasn't been done on this sort of scale before."

On Wednesday, Monster chief executive Sal Iannuzzi told the Reuters news service that the amount of personal data stolen might be much bigger than the company believed when it acknowledged the breach this month. "We're assuming it is a large number," Iannuzzi said. "It could easily be in the millions."

Yesterday, Reuters reported that among those whose data was stolen were users of a website operated by the US government. Contact information for 146,000 of some 2 million users of USAjobs.gov was stolen, according to Peter Graves, a spokesman for the US Office of Personnel Management. Monster runs that site.
The scam was first reported by researchers at computer security firm Symantec Inc. The company discovered a new "Trojan horse" program infecting hundreds of computers on the Internet. Machines infected with the program would log on to Monster, using legitimate passwords belonging to companies that use Monster to hire new workers. Investigators don't yet know how the data thieves obtained those passwords. But the Trojan program would use them to collect personal data from resumes at the site, and forward the data to a computer in Russia belonging to a Ukrainian firm.

Most of the stolen data - names, addresses, phone numbers - was easily available elsewhere and posed little risk. But the e-mail addresses were valuable to phishers because the addresses gave them a mailing list of Monster subscribers. They could use the list to launch precise spear-phishing attacks with a likelihood of success.

"The phisher will look for any affinity between an institution or situation and a human being," said Peter Cassidy, secretary-general of the Anti-Phishing Working Group in Cambridge. "They'll find any relationship and mine it."

That's because people are more likely to trust mail messages that appear to come from a person or organization they know. A 2005 study at Indiana University found that 72 percent of students obeyed the instructions in phishing messages when they appeared to come from a trusted source, while the compliance rate for untrusted messages was just 16 percent.

Phishers have used a variety of methods to create the illusion of affinity. Millions of people have gotten messages purporting to come from the IRS that state the recipient is entitled to a tax refund. "Who doesn't have a relationship with the Internal Revenue Service?" Cassidy said.

Some phishers go further by visiting the Internet sites of various institutions and collecting any e-mail addresses they find there - a cumbersome but perfectly legal process. They then send the victims fake messages from the institution. Cassidy cited a 2005 case in which phishers bombarded faculty and staff at the University of Kentucky with scam messages apparently from the school's credit union.

The Monster attack carries affinity ripoffs to the next level, Cassidy said. The attackers stole the e-mail data, not for immediate profit but for use in their real scam. Victims received messages purporting to have come from Monster, with embedded links that would install malicious software on the users' computers. One such program captured the users' passwords to online bank accounts; another locked vital files on the computer and demanded money in exchange for the key. In other cases, victims received e-mail messages seeking to recruit them to launder money generated in other Internet scams.

Because the Monster site exists to provide employers with information about millions of job seekers, it may be impossible to prevent future security breaches. A single compromised employer password would expose vast amounts of information. "There is no guaranteed fix," Iannuzzi said.

But consumers can protect themselves from scams with software that sits on top of e-mail programs and Web browsers and identifies phony mail and addresses. In addition, Wang of Sophos Labs said...
that subscribers to Monster and other job-hunting sites should avoid putting sensitive information like Social Security numbers in their resumes.

The New York Times Co., parent company of The Boston Globe, has an alliance with Monster to sell help-wanted advertising.

Hiawatha Bray can be reached at bray@globe.com.

© Copyright 2007 Globe Newspaper Company.