InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Fannie Mae Contractor Indicted For Logic Bomb

Had the malicious script designed to wipe Fannie Mae's 4,000 servers not been discovered, the company could have lost millions of dollars and a week's worth of uptime.

By Thomas Claburn, InformationWeek
Jan. 29, 2009
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=212903521

It was mere chance that a senior Unix engineer with Fannie Mae discovered a logic bomb.

The logic bomb, a malicious script designed to wipe Fannie Mae's 4,000 servers, was allegedly placed by Rajendrasinh Makwana, an IT contractor who worked in Fannie Mae's Urbana, Md., facility. It was set to execute on Jan. 31. Had it done so, Fannie Mae engineers expect it would have caused millions of dollars in damage and possibly shut down the government-sponsored mortgage lender for a week.

Makwana, 35, was indicted for unauthorized computer access Tuesday in a Maryland District Court. Court documents indicate that he is a citizen of India who resides in the United States under a work visa.

According to the affidavit of FBI special agent Jessica Nye, the Unix engineer who found the malicious script, identified only as SK, did so by accident. "The malicious script was at the bottom of the legitimate script, separated by approximately one page of blank lines, apparently in an effort to hide the malicious script within the legitimate script," the affidavit states.

The discovery occurred on Oct. 29. Makwana had been terminated as a Fannie Mae contractor on Oct. 24, around 1 or 1:30 p.m., the affidavit says, but his network access was not terminated until late that evening. Makwana was fired for allegedly creating a computer script earlier that month that changed server settings without the permission of his supervisor.

Makwana was not required to turn in his badge or Fannie Mae-supplied laptop until the end of the day on Oct. 24. According to Nye's affidavit, it was during that afternoon that Makwana is alleged to have planted the malicious script.

"On October 24, 2008, at 2:53 pm, a successful SSH (secure shell) login from IP address 172.17.38.29, with user ID s9urbm, assigned to Makwana, gained root access to dsysadmin01, the development server," the affidavit states. "... IP address 172.17.38.29 was last assigned to the computer named rs12h-Lap22, which was [a Fannie Mae] laptop assigned to Makwana. ... The laptop and Unix workstation where Makwana was able to gain root access and create the malicious script were located in his

cubicle."

Makwana is currently free on $100,000 bail pending trial. He has had to surrender his passport.

Christopher C. Nieto, the public defender representing Makwana, said his client will enter a plea of not guilty on Friday, but could not comment further at this time.

Graham Cluley, senior technology consultant at Sophos, sees the risk of similar incidents as companies downsize in response to the troubled economy.

"As belts tighten and the credit crunch continues to hit around the world, more and more companies will be making the decision to make staff and contractors redundant," he said in an online post. "...[A] disaffected employee could create havoc inside your organization so make sure that appropriate security is in place."

An *InformationWeek* report, "Efficiently Isolating Contractors From Sensitive Data: The Many Advantages Of Software-Based Contractor Isolation," examines contractor security trends and offers recommendations for decreasing contractor-related security risks. Download the report here (registration required).