SECURITY darkREADING
Protect The Business Enable Access

Social Engineers Successfully Gather Info

The Defcon18 contest worked well -- too well -- its organizers say

By Kelly Jackson Higgins, DarkReading
Aug. 5, 2010
URL:http://www.darkreading.com/story/showArticle.jhtml?articleID=226600101

The one glimmer of hope during last week's social-engineering contest at Defcon18 was when two different employees at a major retailer separately shut down a contestant trying to smooth-talk his way into gathering sensitive information on their company.

"One of them said the questions [asked of her] sounded 'fishy'" and that she couldn't answer the questions for security reasons, says Chris Hadnagy, founder of social-engineer.org, which sponsored the Social Engineering Capture The Flag contest in Las Vegas last week. "We all clapped -- we thought that [reaction] was great. Unfortunately, the contestant [then] got a different lady at a different location of the company and was successful."

Success was the overwhelmingly disturbing trend in the contest, where around 17 people had 25 minutes to social-engineer by phone information out of a specific company they were assigned to. Each contestant had been assigned a "target" company in advance of the contest, and were allowed to gather as much information as they could passively (no phone calls, email, or direct contact) before the big showdown in Vegas.

They scored points based on the predesignated "flags" they were able to capture -- everything from finding out who supplies the company's in-house cafý food to the type of browser and version they use, their antivirus program, and who handles the trash dumpsters. The flag that brought home the highest number of points was getting the employee to visit a URL, and each of the target company's employees that were given the URL visited it.

All of the contestants were able to social-engineer information out of their targeted companies, some posing as journalists, IT survey-takers, and businessmen, for instance. The list of companies targeted in the contest included Google, BP, McAfee, Symantec, Shell, Microsoft, Oracle, Cisco, Apple, and Walmart. The contest organizers won't reveal which company's employees gave up what information, but the bottom line is that it worked better than the organizers had anticipated.

"I didn't expect it to go as well as it did. In this day and age, I thought more companies would be a lot more security-conscious and not give out such detailed information," says Hagnagy, who is also operations manager for Offensive-Security.com. "From a security professional's standpoint, it was discouraging that this is a massive subset of corporate America -- oil, retail, manufacturing, phone, and security companies. It's a little scary."

Hagnagy says in all cases but one, where the contestant was unable to get a person on the phone at all, the social engineering exploits worked. The contestants each came up with their own pretext for the call, using their own styles and personas. "Every company where we were able to contact a human, they were successful at social-engineering them," he says.

He says the fact that some of the employees visited a URL at the urging of the social engineering caller raises