Published on *InfoWorld* (http://www.infoworld.com)

Stealing corporate secrets proves to be all too easy

By InfoWorld Tech Watch
Created *2010-08-02 04:00AM*

Organizers of a contest to highlight the dangers of social engineering said that employees of some of the top U.S. corporations were eager to cough up private data to contestants, exposing a serious lack of investment in user education about the dangers of scams and other human-focused attacks.

The contest, held Friday and Saturday at the annual Defcon hacking conference in Las Vegas, was organized by social-engineer.org [1], a nonprofit founded to raise awareness about the dangers of soft attacks that use phone calls, email, and in-person persuasion to target individuals and employees of corporations.

[Master your security with InfoWorld's interactive Security iGuide [2]. | Stay up to date on the latest security developments with InfoWorld's Security Central newsletter [3]. **]**

The capture-the-flag-style event allowed contestants to research a list of high-profile target companies, including Microsoft, Cisco, Apple, BP, Shell, Google, Proctor & Gamble, Pepsi, Coke, and Ford. The contestants were then given the assignment to retrieve specific "flags" -- pieces of nonsensitive information, such as the version of a particular operating system or the contractor responsible for picking up the firm's garbage.

The results were not encouraging, said Chris Hadnagy, operations manager at consulting firm Offensive Security and a contest organizer. Contestants were able to extract information from every one of the ten U.S. firms targeted, and only a tiny minority of employees contacted by contestants hung up or refused to give up information the contestants were looking for.

In order to get employees to cough up information, contestants posed as journalists reporting a story, researchers conducting a poll, technical support specialists, potential customers, or merely needy strangers. The employees were often surprisingly trusting -- even pointing their Web browsers to the social-engineer.org website at the suggestion of the stranger on the phone.

"Most people are trusting and really want to help," said Hadnagy. And he said that contestants would have likely had more success in person than over the phone. "It would be even easier in person, because you can use body language and facial expressions to help you gain trust," he

said.

The contest, which InfoWorld's Tech Watch first reported on in June [4], got the attention of the FBI, who expressed concern and called conference organizers to Washington, D.C., to explain the rules (ultimately, no attempt was made to prevent the contest from happening). Hadnagy said that around 20 participants took part on Friday, but that many others who had registered to participate dropped out, with some citing pressure from employers to forego the exercise, including threats of termination.

Mati Aharoni, of Offensive Security and social-engineer.org, said that the point was not to embarrass companies that fell victim to the social engineering hacks, but mainly to raise awareness about the need for better user education -- especially for lower-level employees not considered "important" by management, but who may be sources of important information for potential attackers.

A report on the results of the contest is forthcoming, although specifics about which information was obtained from which companies will not be released. The winner received the rare and coveted "black badge," granting the holder lifetime admission to the Defcon conference.

This article, "Social engineering contest proves to be all too easy [5]" was originally published at InfoWorld.com [6]. Get the first word on what the important tech news really means with the InfoWorld Tech Watch blog [7].

Security Central Hacking Social Engineering

Links:
[1] http://social-engineer.org/
[2] http://www.infoworld.com/d/security-central/infoworld-iguide-security-threats-and-countermeasures-480?source=ifwprm_secigd&idglg=ifwsite_secigd_fssr
[3] http://www.infoworld.com/newsletters/subscribe?showlist=infoworld_sec_rpt&source=fssr
[4] http://www.infoworld.com/t/hacking/new-defcon-contest-tests-hackers-social-engineering-skills-236
[5] http://www.infoworld.com/t/hacking/social-engineering-contest-proves-be-all-too-easy-420
[6] http://www.infoworld.com/?source=footer
[7] http://www.infoworld.com/blogs/infoworld-tech-watch?source=footer