threatpost
The Kaspersky Lab Security News Service

Published on *threatpost* (http://threatpost.com)

Former Employees a Rich Target in Social Engineering Contest

By *Paul Roberts*
Created *09/03/2010 - 5:40pm*

The results of a hacking contest at the DEFCON conference shows that the largest U.S. corporations have a lot to learn. "If any of these targets had hired us to do a social engineering audit, we would have failed them," an organizer said.

Its a truism in the computer security world that people, rather than machines, are the easiest targets for would be criminals and hackers. Now the results of a recent contest at the annual DEFCON hacking conference in Las Vegas bear that out and suggest that former - not current - employees may be an fatter target for those who wish your company harm.

The organizers of the "Capture the Flag" style contest, dubbed "How Strong is Your Schmooze," say that they have met with federal law enforcement personnel, who requested a first look at the data, and are readying a report presenting the findings from the various social engineering hacks that took place during the two day event in August. Among the findings: former employees - as much as current ones - can be a rich source of information about the inner workings and security defenses used by their employers.

In all, the results of the contest were not encouraging, said Chris Hadnagy, co-founder of Social-Engineer.org and a principal at [1]Offensive Security [1].

"If any of these targets had hired us to do a social engineering audit, we would have failed them," he said. "There wasn't one company that successfully demonstrated security awareness." That was surprising, given that the companies targeted by contest participants were some of the largest and richest in the U.S., including Cisco Systems, Microsoft, Google, Ford Motor, Pepsi and Coca Cola.

Contest participants spent time researching their targets and came to the contest with dossiers of names, titles, positions, e-mail and phone numbers. While some of the individuals targeted in the contest performed admirably, no company exhibited across the board success against social engineering hacks, Hadnagy said.

"We had people who shot us down real quick and said some things that made us know that they

were aware of security, but within the same company, we could call and get someone who, within minutes, would give us any information we want."

To avoid breaking the law, contest organizers kept that information to a minimum: the kind and version of operating system or Web browser they were using, the kind of document reader their company used or what kind of beer the person liked. In other cases, employees were asked to point their browser to a predetermined, but benign Web page. Still, many of the information "flags" that were collected could be used in a targeted attack, organizers say.

What little security awareness there was within organizations tended to concentrate at the senior levels of the organization, he said.

"Call centers were probably the weakest trained areas in our opinion," Hadnagy said. "When we called management, they seemed aware of trapping questions and malicious solicitations. But call centers and tech support didn't seem to have any training at all about security awareness." Even companies that claimed to do employee training around social engineering, like Cisco, fell short when actually tested, he said.

The tournament raised alarm within leading corporations and among law enforcement after it was announced. Contest organizers issued assurances and worked with both the FBI and Electronic Frontier Foundation prior to the event to ensure that no laws were broken in during the event. Law enforcement also requested a first look at any report stemming from the contest. That meeting took place this week, with the public release of the report due in a week or so, Hadnagy said.

Employers need to do a better job of training employees to spot social engineering attacks, he said. They also need to stay on top of software updates.

"It was shocking -- 55% of the companies were still using Internet Explorer 6 as their Web browser," said Hadnagy of Microsoft's much maligned and insecure browser. (http://threatpost.com/en_us/blogs/old-and-insecure-ie6-still-popular-enterprise-081810)

But one big vulnerability for firms may be utterly outside of their control: former employees, Hadnagy said.

"We had a contestant who used job search Web sites to scrape resumes of people who used to work for the company he was targeting. He'd call, pretend to be a headhunter and ask you questions about the technology you used in that past position," he said.

Companies have to help employees develop a better sense of how social engineering attacks work and what kinds of information it is and isn't appropriate to ask for, he said.

Organizers haven't yet been asked back to DEFCON for a repeat contest, but Hadnagy feels confident they will be.

"I'm just happy that we accomplished what we set out to and kept the contest above the legal and moral line," he said.

//

Source URL: http://threatpost.com/en_us/blogs/former-employees-rich-target-social-engineering-contest-090310

Links:
[1] http://www.offensive-security.com
[2] http://www.twitter.com/home?status=Former Employees a Rich Target in Social Engineering Contest http://threatpost.com/en_us/c5K