Contest finds workers at big firms handing data to hackers

Elinor Mills, CNET News.com on August 2nd, 2010

LAS VEGAS--Hackers competing in a social engineering contest at the Defcon conference here last Friday were able to trick random employees at 10 major U.S. tech, oil, and retail companies into giving them sensitive information over the phone that could be used in targeted computer attacks on the companies.

"Every single company, if it was a security audit, would have failed," Christopher Hadnagy, operations manager for Offensive Security, a training and penetration testing company, told ZDNet Asia's sister site CNET after the first day of the contest, which ended last Saturday and targeted BP, Shell, Google, PG&E, Microsoft, Apple, Cisco, Ford, Coke, and Pepsi.

"Not one company shut us down, although certain employees within the company did. But we (participants) were able to call right back and get another employee that was more willing to comply."

The organizers declined to offer specific comments about any one of the companies targeted by the contest or say which companies are faring better or worse than the others. But they said they'd release a report with aggregated information in a few weeks.

"The point isn't to shame anyone. It's to bring awareness to this attack vector, which is probably the easiest way to hack a corporation today," said Mati Aharoni, lead trainer at Offensive Security. "We really don't want to see anyone get harmed or get in trouble."

Social engineering is a hacking technique that involves simply tricking people into offering up sensitive information, rather than using technical means--such as breaking into computer systems--to get such data. The contest's organizers said companies put a lot of emphasis on buying security software and building technological defenses for their information, but they ignore their Achilles heel: the people who work for them.

"The human resources are the weakest and softest spot of the whole organization," Aharoni said. "The most used vector by hackers today is the easiest route, and that's usually the human element."

Each of the 10 contestants was assigned one of the target companies a week or so before the event and allowed to do "passive" Web research to gather intelligence on the target and figure out a plan of attack. They were not allowed to make social engineering calls or use phishing or other online methods to extract this information.

At Defcon the contestants have 25 minutes to make calls to try to get as many bits of information from a predetermined list as they can. The calls are broadcast over a sound system. The contestant with the most items at the end of the event wins.

Contestants are asked to get "innocuous information" about the corporations, such as what company provides dumpster service, whether it has a cafeteria, and what browser its employees use, contest organizers said.

None of the employees at the companies was asked for or gave out any financial information, credit card details, personal data, or other sensitive information barred from the contest, according to the contest organizers, whose Web site is dedicated to educating people about the dangers of the social engineering technique.

Only 3 people out of 50 or more employees who answered the phone calls, were skeptical and hung up without providing information, and all three were women, said Hadnagy.

"One woman said 'this question sounds fishy to me' and hung up within the first 20 seconds," Hadnagy said. "We all clapped."

In another case, one hacker got answers to nearly every question on the list of 30 to 40, plus information that wasn't part of the official list, according to Hadnagy.

"People went as far as opening up their e-mail clients, Adobe Reader, versions of Microsoft Word, and clicking on 'Help/About' and giving the exact version numbers of their software," said Aharoni. "For an attacker, the exact version number would provide a much higher level of success", allowing an attack to be tailored to exploit a vulnerability in that exact program.

The contest made ripples even before it officially began. After hearing about plans for the event, the FS-ISAC (Financial Services-Information Services Analysis Center) issued warnings to companies to be alert during Defcon. The contest organizers reached out to the agency and offered to work with it to educate and train people about recognizing and preventing social engineering attempts.

Meanwhile, several agencies in the U.S. federal government have expressed interest in the group's report when it's done, according to Hadnagy. He declined to identify the agencies.

"We will share information with law enforcement as they've asked of us," Aharoni said.

This article was first published as a blog post on CNET News.

URL:*http://www.zdnetasia.com/contest-finds-workers-at-big-firms-handing-data-to-hackers-62201764.htm*