

Technology Technology News

Hackers fool world's largest companies using smooth talk

August 02, 2010



Robert Baldi, right, makes calls to a company attempting to extract sensitive information during a social engineering exercise at the DefCon hacker conference in Las Vegas. Photo: AP

Hackers at an infamous **DefCon** gathering in Las Vegas are proving that old-fashioned smooth talk rivals slick software skills when it comes to pulling off attacks on the computer networks of some of the world's largest companies.

A first-ever "social engineering" contest at the conference challenges hackers to call workers at 10 companies including Google, Apple, Cisco, and Microsoft and get them to reveal too much information to strangers.

"Out of all the companies called today, not one company shut us down," said Offensive Security operations manager Christopher Hadnagy, part of the social-engineer.org team behind the competition that kicked off late last week.

The team kept hackers within the boundaries of the law, but had them coax out enough information to show that workers would have unintentionally made it easier to attack networks.

Workers that unknowingly ended up on calls with hackers ranged from a chief technical officer to IT support personnel and sales people.

One employee was conned into opening programs on a company computer to read off specifications regarding types of software being used, details that would let a hacker tailor viruses to launch at the system.

"You often have to crack through firewalls and burn the perimeter in order to get into the internal organisation," said Mati Aharoni of Offensive Security, a company that tests company computer defences.

"It is much easier to use social engineering techniques to get to the same place."

Other companies targeted were Pepsi, Coca Cola, Shell, BP, Ford, and Proctor & Gamble.

The contest, which continued Saturday at DefCon and promises the winner an Apple iPad tablet computer, is intended to show that hardened computer networks remain vulnerable if people using them are soft touches.

"We didn't want anyone fired or feeling bad at the end of the day," Aharoni said. "We wanted to show that social engineering is a legitimate attack vector."

A saying that long ago made it onto t-shirts at the annual DefCon event is "There is no patch for human stupidity."

"Companies don't think their people will fall for something as simple as someone calling and just asking a few questions," Hadnagy said.

"It doesn't require a very technical level of attacker," Aharoni added. "It requires someone with an ability to schmooze well."

One worker nearly foiled a hacker by insisting he send his questions in an email that would be reviewed and answered if appropriate.

The hacker convinced the worker to change his mind by claiming to be under pressure to finish a report for a boss by that evening.

"As humans, we naturally want to help other people," Hadgagy said. "I'm not advocating not helping people. Just think about what you say before you say it."

Companies that got word of the social engineering contest before DefCon called in the FBI, which was assured by the event organisers that nothing illegal was afoot.

Information about "exploiting human vulnerabilities" was available at the social-engineer.org website.

AFP

Most viewed

1. [It's a wipeout for Google Wave](#)
2. [Van man 1, Microsoft 0: now Aussie Ric's gunning for more tech giants](#)
3. [Wife learns of husband's second wedding on Facebook](#)
4. [Coalition to dump 'flawed' internet filter](#)
5. [Intel agrees to end chip war with rivals](#)

[Technology](#) [Technology News](#)

News

Biz-Tech

Security

Enterprise

Sci-Tech

Digital Life

[Top](#)

[More sites](#)

[Sections](#)

Copyright © 2010 Fairfax Digital

[Terms of use »](#)

[Standard site »](#)

[Feedback »](#)
