The Register®
Biting the hand that feeds IT

Original URL: http://www.theregister.co.uk/2010/07/31/hacking_human_gullibility/

Social-engineering contest reveals secret BP info

Hacking human gullibility at Defcon

By **Dan Goodin in Las Vegas**

Posted in Enterprise Security, 31st July 2010 02:29 GMT

Defcon A hacker competition that challenges contestants to trick employees of large companies into divulging potentially sensitive information aims to show how human gullibility is the biggest security vulnerability of all. During its first day at the Defcon hacker conference in Las Vegas, it had clearly achieved its goal.

With just two phone calls, entrant Josh Michaels managed to dupe a computer support employee at BP into spilling details that could have proved crucial in launching a network attack against the global oil company. The information included what model laptops BP used and the specific operating system, browser, anti-virus and virtual private network software the company used.

Michaels was also able to trick the employee into visiting Social-Engineer.org [1], a feat that won the contestant extra points.

“That was scary,” said Michaels, shortly after ending the call, in which he posed as a Louisiana-based employee handling claims stemming from BP's massive oil spill in the Gulf of Mexico. “You never know what you're going to get. There's an adrenalin rush that comes with social engineering.”

Under the rules [2] of the the Social Engineering Capture the Flag contest, entrants had 25 minutes to call a company chosen in advance by the organizers. The contestants were permitted to make as many calls as they wanted using a variety of ploys. Points awarded varied depending on the kinds of “flags” collected, which included the version of Adobe Reader the company used, the garbage collector that hauled its trash, or success in getting the target to visit a website of the caller's choosing.

“We assumed that if we can make a person open up their browser, tell us the version of their browser they had, and then visit a website, in essence if we were malicious, terrible hackers, we could have driven them to a site that had some kind of malicious file on it and that most likely the person would have downloaded it and accepted the malicious file,” said Chris Hadnagy, operations manger for a firm called Offensive-Security.com and a contest organizer.

Callers sat in a soundproof glass booth while about 80 people crammed into a conference room listened on, often chuckling and applauding as targets naively volunteered potentially sensitive information. Companies that were called during day one of the two-day competition included BP, Shell, Apple, Google, Microsoft, Cisco Systems, Proctor and Gamble, Pepsi, Coca-Cola, and Ford. Of the dozens of calls made to the 10 companies, only three of the targets refused to cooperate.

“They would have given pictures of their family if they had been asked,” Hadnagy said during a press conference. “It was just so smooth and easy.”

Organizers said they went to considerable lengths to make sure the contest didn't cross any legal or ethical lines. The rules expressly bar the solicitation of any confidential information such as credit card numbers or passwords, and the ruses can't include claims that someone's account has been compromised, or other scenarios that might lead targets to believe they are at risk.

Despite the guidelines, which were posted for weeks in advance, the contest attracted the attention of members of the FBI's cyber-hacking division, one of whom called and said he had been contacted by multiple US companies who were concerned their confidential information would be targeted in the competition.

“I thought it was a prank,” Hadnagy said. “I thought: 'This guy is ripping me one.' I wan't very nice to him.”

Hadnagy arranged to call the person back and when Hadnagy was connected to FBI headquarters, he decided the person was for real.

Hadnagy's reaction is one of the better countermeasures that targets of social engineering attacks can take. But as security professionals have long pointed out [3], it runs against the grain of human evolution, which has largely rewarded the species for banding together in trusted groups.

It was something Michaels, the contestant who socially engineered the BP support employee, witnessed first hand.

“You have to come off as you don't know a lot,” Michaels told *The Reg*. The employee “wanted to do whatever he could to help me.” ®

Links

1. http://www.social-engineer.org/
2. http://www.social-engineer.org/blog/defcon-social-engineering-contest/
3. http://www.theregister.co.uk/2010/03/04/social_penetration/

Related stories

Fake Firefox update used to sling scareware (30 July 2010)
http://www.theregister.co.uk/2010/07/30/firefox_update_scareware_ruse/

Fake *Toy Story 3* scams creates malign buzz (20 July 2010)
http://www.theregister.co.uk/2010/07/20/toy_story_3_scams/

Blizzard exposes real names on WoW forums (7 July 2010)
http://www.reghardware.com/2010/07/07/wow_forums/

Broken-hearted email servers mark LoveBug anniversary (4 May 2010)
http://www.theregister.co.uk/2010/05/04/love_bug_anniversary/

Cybercrooks befuddled by Icelandic volcano name (21 April 2010)
http://www.theregister.co.uk/2010/04/21/icelandic_volcano_scareware_confusion/

Zeus spyware pretends to be Royal Mail PDF (16 April 2010)
http://www.theregister.co.uk/2010/04/16/zeus_pdf_spyware/

DNS Trojan poses as iPhone unlocking utility (15 April 2010)
http://www.theregister.co.uk/2010/04/15/iphone_unlocking_trojan_scam/

Trojan poses as Adobe update utility (29 March 2010)
http://www.theregister.co.uk/2010/03/29/software_update_trojan/

Hacking human gullibility with social penetration (4 March 2010)
http://www.theregister.co.uk/2010/03/04/social_penetration/

© Copyright 1998–2010