Bogus e-mails from FDIC link computer users to viruses, says computer forensics expert

October 27 2009

Gary Warner is the UAB Director of Research in Computer Forensics. Credit: UAB

Cyber criminals are using fake messages claiming to be from the Federal Deposit Insurance Corporation (FDIC) to deliver a virus capable of stealing unsuspecting victims' bank passwords and other sensitive personal information, says Gary Warner, the director of research in computer forensics at the University of Alabama at Birmingham (UAB).

Warner says the spam is being delivered with one of two subject lines:

- FDIC has officially named your bank a failed bank

- You need to check your Bank Deposit Insurance Coverage

Warner says that once the message is opened the spam asks users to visit a specific Web site, a link to which is included in the message. Those that follow the link are taken to a page that asks them to click and download a copy of "your personal FDIC insurance file."

"Unfortunately, anyone who clicks that download link will be downloading a version of the Zeus Bot virus, which has the capacity to steal bank passwords and other financial and personal information," Warner says.

Warner and his research team in the UAB Spam Data Mine have been tracking the new spam for a number of days and report its delivery volume to be very high.

The spam claims to be from the e-mail address consumeralerts@fdic.gov, which is a real e-mail address used by the FDIC, but has obviously been forged by the malware distributors in this situation, Warner says.

"The cyber criminals behind this spam have gone to great lengths to mimic the logos and look of FDIC communications, including going so far as to forge an official FDIC e-mail address in an effort to confuse consumers into following links and downloading harmful programs," Warner says.

"As is the case with any agency or company e-mail, do not follow links or click downloads embedded in the messages. Instead, visit the site in question through your Web browser and log in as you normally would," he says. "If an entity has an important message for you, you'll be able to find it on its Web page.

"Legitimate companies will never ask you to download programs or enter your personal information via an e-mail."

Source: University of Alabama at Birmingham (news : web)