Researchers flag phony domains in e-mail security study

September 11 2011, by Nancy Owano

(PhysOrg.com) -- A paper released this week shows how an e-mail scoffing technique picks up personal employee information, company secrets and passwords almost effortlessly with just the setting up of domain and e-mail server. The researchers discovered business invoices, employee personal identifying information, network diagrams, user names, passwords, and trade secrets were part of the treasure trove of e-mail information that was captured by phony domains set up for the experiment.

The paper is titled "Doppelganger Domains," and as its title suggests the technique involves an e-mail address that at first glance looks identical to the real address but is missing a dot between subdomain and domain. While "typo-squatting" is nothing new, doppelganger domains are a troublesome variant. They are troublesome because the involved error is

so easy to make and so easy not to instantly recognize. A no-dot omission instead of a misspelling can do considerable damage. As The Register phrased it, it is a case where "executive butterfingers get slurped by honeypots" just because of the sender missing the dot between host/subdomain and domain. An attacker's "uscompany.com" versus the "correct" us.company.com is an example. Attackers could configure their email server to vacuum up email addressed to that real domain. Corporate giants are easy targets, with their heavy usage of email, accompanied by the likelihood of mis-sent e-mails.

The study's authors, Peter Kim and Garrett Gee from the Godai Group, a security firm, found that 30 percent (151) of the Fortune 500 companies profiled were potentially vulnerable in a six-month waiting period, where they had set up doppelganger domains to see what they would get. What they did get were 120,000 e-mails that innocent people had mistakenly sent to the phony missing-dot domains.

Types of Fortune 500 industries listed as susceptible to doppelganger domains in the test included telecom, technology, aerospace and defense, banks, food and consumer products. While the test was an experiment, the researchers say real-world doppelganger domains exist, as they found no-dot domains of this nature in China. Some of those domains are already known for phishing.

Kim and Gee recommend ways to avoid the interception of e-mails through doppelganger domains. Their recommendations, among others, include (1) finding out if a doppelganger domain is already in use and if so then filing a dispute known as a Uniform Domain Dispute Resolution Policy (2) configuring the mail server not to allow outbound e-mails to doppelganger domains. While another recommendation might appear too obvious to mention, it is of practical value: Tell others to be careful. "Communicate the attack vector to your internal users, customers, and business partners."

More information: Press release