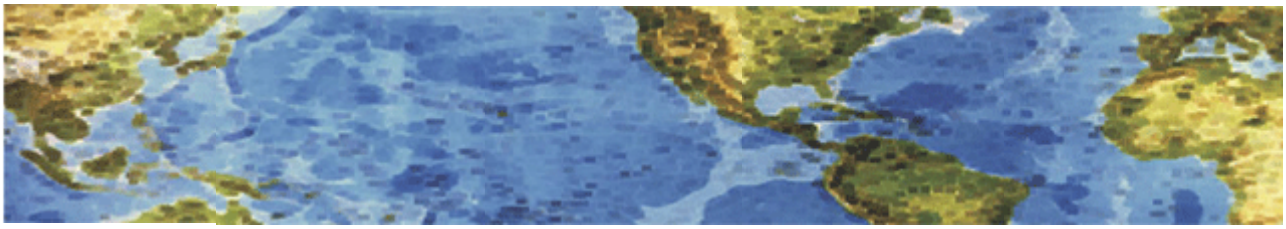
HALL ASSOCIATES



Risk-Based Decision Making Commentary
27 September 2013 Newsletter

Mobile Browsing - Is Your Company at Risk?

This infographic gives a quick visual representation of some of the key findings of a recent Webroot research report on web security in the US and UK. As cybercriminals increasingly exploit vulnerabilities in mobile browsers and apps, companies with mobile workforces (or those that allow employees to use their own mobile devices to access the company network) face new challenges in protecting users and customers data. And the impacts of failing to protect against mobile browsing threats can be severe.

Among the key points:

50% of companies in the US estimate that web-borne attacks cost from $25,000 to $1 million in 2012

90% of respondents agree that managing the security of remote users is challenging

50% of firms with remote workers had a website compromised

Mobile Threats Experienced in 2013 by Companies

9% lost data

24% got Malware

45% lost devices

Mobile Threat Impacts

53% reported business activities were significantly disrupted

61% required additional resources to manage mobile security

56% had reduced employee productivity

What can you do to minimize these kind of impacts if your employees use their own mobile devices?

1. Establish and enforce device control policies.
2. Require YOUR device level security to be used by any personal mobile device
3. Provide mandatory mobile workforce security training.

HALL ASSOCIATES

Social Engineering Example – Spear Phishing

These phishing emails are typically targeted to individuals at companies that are high ranking officials, possibly CXOs. The contents of the email will usually include personally identifiable information of the victim to build confidence in the email. This might include full name, telephone number, position, etc. This is possibly one of the best examples of a targeted spear phishing attack.

Thousands of high-ranking executives across the country have been receiving e-mail messages this week that appear to be official subpoenas from the United States District Court in San Diego. **Each message includes the executive's name, company and phone number, and commands the recipient to appear before a grand jury in a civil case**. A link embedded in the message purports to offer a copy of the entire subpoena. But a recipient who tries to view the document unwittingly downloads and installs software that secretly records keystrokes and sends the data to a remote computer over the Internet. This lets the criminals capture passwords and other personal or corporate information. Another piece of the software allows the computer to be controlled remotely. According to researchers who have analyzed the downloaded file, less than 40 percent of commercial antivirus programs were able to recognize and intercept the attack. An example image (courtesy of the New York Times blog by John Markoff) of the article is show below:

From: United States District Court [subpoena@uscourts.com]
To: Steve Kirsch
Cc:
Subject: Subpoena in case #28-755-YCH

AO 88(Rev.11/94) Subpoena in a Civil Case

Issued by the
UNITED STATES DISTRICT COURT

Issued to: Steve Kirsch
Propel Software Corporation
408-571-6300

SUBPOENA IN A CIVIL CASE

Case number: 28-755-YCH
United States District Court

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

Place: United States Courthouse
880 Front Street
San Diego, California 92101

Date and Time: May 7,2008
9:00 a.m. PST

Room: Grand Jury Room

So how can someone avoid responding to this type of e-mail phishing? **Obviously, the number one thing is user awareness**. Unfortunately, the security community has been pushing user awareness for a decade, and the attackers just get less blatant and obvious about their attacks, making it more difficult for users to avoid this type of attack. There are two things to drum into potential targets of these type of attacks:

One – No Government agency would send this type of alert via e-mail. There are phishing e-mails supposedly from the Justice Dept, the FTC, the FBI, the IRS and numerous other agencies.

Two – ***Never*** click on a link in an e-mail without checking on it first. I recommend calling the agency and asking if they sent this.

http://www.zdnet.com/blog/security/targeted-spear-phishing-attacks/1032