Aplura, LLC
4036 Wildwood Way
Ellicott City, MD 21042
301-523-2110 (w)
410-864-8386 (f)

Focused Information Security
www.aplura.com

Social Networking, A threat to business?

Essay By: Sean Wilkerson

February 18, 2009

Many office workers have an account on at least one of the big SocNets (Social Networking sites) such as LinkedIn, Facebook, Twitter, MySpace, or Orkut. However, are they logging into these sites from work?

During Aplura's log-centralization projects, there is usually a request to generate a report on the most heavily visited Internet websites by internal users. This can be a touchy issue, because inevitably the top 10 sites, by usage, are not remotely related to work. However, the recent trends show that instead of just news, retail and blog sites, office-workers spend a copious amount of their working-hours reading (and updating) SocNets. Most users also accept the default configuration for their account and never think to tweak their settings to help preserve privacy or security such as this article recommends for Facebook users.

There are a few expected threats of SocNets which include things such as: Phishing expeditions, user mis-direction or beguilement, or lack of control over posted information.

These security concerns (and many others) were well-illustrated by "Nathan Hamiel and Shawn Moyer" in their "Fail 2.0" talk on Feb. 7th 2009 during ShmooCon (Annual Hacker Conference in DC).

Although a well-executed social engineering attack spawned from a SocNet could cause chaos to an individual's life, the rest of this article will focus on two other threats which face the business network. Both threats are a result of intentional user action and beguile.

First threat: Loaded Content (html and the bait-and-switch)

Most Internet users follow the old (and broken) paradigm that the Internet has both good and bad neighborhoods, and that you can eliminate risk by browsing only to the “good ones.” Generally speaking, most users believe their favorite websites are benign; however, there attributes of the popular social network sites that increases their threat potential. Below are two illustrations of how websites (specifically SocNets) can infect systems.

A frequent component to Social Networking websites is a way for page-visitors to leave comments. Some of the sites allow visitors to place comments using HTML which the site then renders when the page is viewed. An attacker could simply leave an HTML comment on a user's page that issues a redirect to tell the user's browser to download and install malware. There are few protections from this, and an increasing number of ways to craftily deliver this attack. One method might be for an attacker to leverage the **just announced** Microsoft's MS09-002 vulnerability which exposes a flaw in their Internet Explorer browser.

The next security concern relating to user's pages, is the add-on module bait-and-switch. The Mozilla and Firefox browsers made add-on's popular, and this is now an expected feature of many applications, including SocNets. They also allow user-created content in the form of add-on modules which other users can attach to their profile or page. These add-ons extend the user-experience by providing a helpful or entertaining enhancement to either the user's page or the way the user relates to others. Unfortunately, there is virtually no control by the SocNet maintainers over these add-ons. Sites like Facebook, allow users to add “apps” to their pages once they have accepted the warning that the apps require additional data access. Most of these apps operate via java-script run on the end-user's browser.

Why is this bad?

Imagine if an attacker created a useful application on a large SocNet. They then share this app out with as many people as possible. Within a week, a few hundred thousand people use the app by adding it to their page/profile. When the attacker is ready, they change the code to have the app perform a malicious action such as download command and control software. If used from work, the system could become infected

and/or under attacker-control. If these numbers seem unrealistic, consider Facebook's recent “25 Things About Me” craze, and the millions of users who had used it within a few days.

Second threat: Intentional Sensitive Data Extrusion

For most of the history of Information Security, the goal was to keep the bad guys out. That's the whole point of Firewalls. However, this trend drastically shifted a few years ago and now a chief information assurance concern is to inspect the data that leaves the network. Many organizations have added visibility to their network egress points so they can inspect this traffic.

The concept becomes muddied though, when a SocNet which exists to share information with the public, contains information that is sensitive. Such an event occurred recently when member of the House Intelligence Committee, Rep. Peter Hoekstra (R-Mich) sent a series of Tweets to his Twitter page containing his agenda and whereabouts during a s**ecret** trip to Baghdad by a contingent of congressman. Then just a few days later, news came out that State Senators in Virgina had telegraphed an unintended message to their opponents via Twitter.

Moving Onward

The ease of use of sites like Twitter has dramatically lowered the threshold (and bar) to publish data to the public Internet. Many cell phones incorporate features which allow users to frequently update their online status. Companies that have staff who handle sensitive information should seriously consider their organization's public disclosure policy since blogging, micro-blogging, and other SocNets have fuzzed the line between PR policy and security policy. Additionally, since work-life and home-life continues to fuse, organizations should consider computer awareness training programs which educate their users on current online threats even if they don't appear to apply to the work place. Such a program could save your user's unnecessary stress at home at a minimum and ultimately could protect your enterprise network.