Evaluating the Security Risks of Freedom on Social Networking Websites

Rutgers University Technical Report DCS-TR646, January 2009.

Blase E. Ur
Rutgers University
blaseur@rci.rutgers.edu

Crystal Maung
Rutgers University
kyithar@cs.rutgers.edu

Vinod Ganapathy
Rutgers University
vinodg@cs.rutgers.edu

ABSTRACT

Many Web 2.0-based social networking sites permit their users to post comments containing a variety of HTML tags on other users' profiles. In this paper, we show that allowing arbitrary users to post multimedia HTML content on other users' social network profiles is an attack vector. Specifically, we demonstrate three attacks—the Social-DDoS attack, the Social-C&C attack, and the Browser-choking attack—each of which allows an *arbitrary* Web user to jeopardize the security of other Web users.

Using the Social-DDoS attack, a malicious Web user can launch a distributed denial of service attack against a Web server; the Social-C&C attack allows a botmaster to covertly and efficiently deliver commands to bot-infected machines; and the Browser-choking attack cripples Web browsers by increasing their memory consumption and prevents users from viewing targeted social network profiles. We present an experimental evaluation of these attacks on two popular social networking Web sites, Myspace and Flickr. Our results show that the attacks can be highly effective when launched using popular social network profiles. In the context of our results, we discuss the security risks of allowing social network users to post media files on other users' pages, and we conclude with a discussion of possible approaches to mitigate these risks.

.