Technology Review
PUBLISHED BY MIT

Monday, September 15, 2008

Turning Social Networks Against Users

Applications built on social networks may be the ideal way to distribute malicious code.

By Erica Naone

Ever since Facebook (http://www.facebook.com/) opened its doors to third-party applications a year and a half ago, millions of users have employed miniature applications to play games, share movie and song recommendations, and even "zombie-bite" their friends. But as the popularity of third-party applications has grown, computer-security researchers have also begun worrying about ways that social-networking applications could be misused. The same thing that makes social networking such an effective way to distribute applications--deep access to a user's networks of friends and acquaintances--could perhaps make it an ideal way to distribute malicious code.

A number of research projects have demonstrated growing unease. At the Information Security Conference (http://isc08.twisc.org/) in Taiwan this week, researchers from the Foundation for Research and Technology Hellas (http://www.forth.gr/) (FORTH) in Greece will present details of an experiment that involved enlisting Facebook users in a potentially devastating kind of Internet attack. The researchers created an application that displays photographs from *National Geographic* on a user's profile page. However, invisible to the user, the app also requests large image files from a target server--in this case, a test machine hosted at FORTH. Provided that enough people add the application to their page, the resulting flood of requests can shut down the server or render it inaccessible to legitimate users.

Elias Athanasopoulos (http://www.ics.forth.gr/~elathan/) , a research assistant at FORTH who is involved in the project, says that the researchers made no effort to promote their application but found that around 1,000 Facebook users installed it within a few days. The resulting attack was not particularly severe, but Athanasopoulos says that it could disrupt a small website, and he suggests that the onslaught could be made more intense with minor adjustments to the application. The attack relies on open access to Facebook. "It's very difficult to provide a platform that will not [allow developers to] interfere in malicious ways with the rest of the Web," he says.

A more detailed analysis covering several different social-networking sites suggests that the potential for mischief may actually run much deeper. Two computer-security consultants--Nathan Hamiel of Hexagon Security Group (http://www.hexsec.com/) and Shawn Moyer of Agura Digital Security (http://www.agurasec.com/) --recently built examples of malicious applications on top of OpenSocial (http://code.google.com/apis/opensocial) , an open application platform used by MySpace (http://www.myspace.com/) , hi5 (http://www.hi5.com/) , Orkut (http://www.orkut.com/) , and several other social networks. One of their demo applications, called DoSer, logs out users who view a compromised profile page for seven seconds. Another, called CSRFer, sends unauthorized friend requests from a target user. But Hamiel says that there are plenty more ways to attack social networks and that little can be done to defend them. "[An application] hooks into the social net about as deep as it can go," he says.

A key problem is that it is so difficult for users to know what a social-networking application is actually doing. "You cannot really check what an application is doing, being a user," says Roel Schouwenberg, a senior antivirus researcher at Kaspersky Lab (http://www.kaspersky.com/) , in Belgium. "As a security professional, that doesn't give me nice feelings."

Social factors also play an important role, Hamiel says, because social networks foster an atmosphere of trust that is easy to exploit. For example, a malicious program recently spread via Facebook in the form of a fake update for Flash that was forwarded from one friend to another. "It was the social aspect that drove them to do something technically stupid," Hamiel says.

The companies behind social-networking sites are just starting to wake up to the issue of security. Facebook, for example, recently created a security page (http://www.facebook.com/security) to educate users about potential risks that they could face. The company adds that its security team "is dedicated to investigating and auditing our own code for holes, as well as reaching out to people in an extended community to let us know if we've missed anything."

Hamiel warns that it may be nearly impossible to eliminate all malicious programs, and he notes that an attacker could build a legitimate application, wait until a large number of users have installed it, then make the application "go bad" by updating it with malicious code.

Limiting all applications' capabilities does not provide a solution because it would destroy what makes them so attractive to users. "You're in a tough position because the goal of a social network is to facilitate creativity and communication," he says. "If you start being too restrictive, you're basically restricting what the social network is all about. You have a functionality arms race."

A more effective solution, according to Athanasopoulos, would be to hire programmers to audit the code being used by external applications. But he acknowledges that the expense of this could make it unattractive for most companies.

As social networks become increasingly popular, Hamiel expects to see many more attacks. "People don't have the same respect for software running in their browser as they do for something they would download and install," he says. In the future, he adds, that may have to change.