Free Tool Hacks Banking, Webmail, and Social Networking Sessions

Man-in-the-middle attack tool automates hacks for non-Web security experts

OCTOBER 6, 2008 | 5:55 PM

By Kelly Jackson Higgins
Senior Editor, *Dark Reading*

A researcher will demonstrate a free, plug-and-play hacking tool this week that automatically generates man-in-the middle attacks on online banking, Gmail, Facebook , LiveJournal, and LinkedIn sessions -- even though they secure the login process.

Jay Beale, who recently released the so-called “Middler” open-source tool, will show it off at the SecTor conference in Toronto. Aside from the unnerving capability of hacking into sites that perform secure logins and then use clear-text HTTP, Middler is also designed for use by an attacker with no Web-hacking skills or experience. “The Middler allows an attacker with no Web application-hacking experience to launch attacks that previously required substantial time and skill,” according to Beale.

The Middler basically clones the victim’s online session by using the same cookies and HTML form parameters as the victim. Then the attacker can inject malicious JavaScript onto the Web pages, redirect the user to another page, or log the victim’s session.

Beale’s tool can override a secure banking session by rewriting the URLs on the page to remove the Secure Sockets Layer (SSL) protection.

Beale, who is co-founder of security consultancy InGuardians Inc., formerly Intelguardians LLC , says many organizations don’t realize that only encrypting the password form leaves users vulnerable to man-in-the-middle attacks. LinkedIn, for example, first has users sign in at its HTTPS address. But after you’re in, you get sent back to the regular HTTP address, http://www.linkedin.com/home.

Then the attacker can access the LinkedIn user’s contact information and inbox, and even add himself to the victim’s “network,” or add the victim to his network.

The researcher also plans to demonstrate at SecTor how to use Middler for injecting JavaScript into browser sessions, which the tool uses to infect the user's browser with the Browser Exploitation Framework, which is considered a browser-level botnet tool.

Beale says Middler can also detect vulnerabilities in a browser and then use Metasploit to exploit them. It can also launch its own cross-site request forgery (CSRF) attacks, he says. And the Python-based tool can be set up to “fire and forget” so the attacks can execute automatically.

Beale also plans to show how Middler can meddle with software installations and updates and inject Trojans, both in computers and on the iPhone.

Have a comment on this story? Please click "Discuss" below. If you'd like to contact Dark Reading*'s editors directly, send us a message.*