BLADE software eliminates 'drive-by downloads' from malicious websites (w/ Video)

October 6 2010

Insecure Web browsers and the growing number of complex applets and browser plug-in applications are allowing malicious software to spread faster than ever on the Internet. Some websites are installing malicious code, such as spyware, on computers without the user's knowledge or consent.

These so-called "drive-by downloads" signal a shift away from using spam and malicious e-mail attachments to infect computers. Approximately 560,000 websites -- and 5.5 million Web pages on those sites -- were infected with malware during the fourth quarter of 2009.

A new tool that eliminates drive-by download threats has been developed by researchers at the Georgia Institute of Technology and California-based SRI International. BLADE -- short for Block All Drive-By Download Exploits -- is browser-independent and designed to eliminate all drive-by malware installation threats. Details about BLADE will be presented today at the Association for Computing Machinery's Conference on Computer and Communications Security.

"By simply visiting a website, malware can be silently installed on a computer to steal a user's identity and other personal information, launch denial-of-service attacks, or participate in botnet activity," said Wenke Lee, a professor in the School of Computer Science in Georgia Tech's College of Computing. "BLADE is an effective countermeasure against

all forms of drive-by download malware installs because it is vulnerability and exploit agnostic."

The BLADE development team includes Lee, Georgia Tech graduate student Long Lu, and Vinod Yegneswaran and Phillip Porras from SRI International. Funding for the BLADE tool was provided by the National Science Foundation, U.S. Army Research Office and U.S. Office of Naval Research.

The researchers evaluated the tool on multiple versions and configurations of Internet Explorer and Firefox. BLADE successfully blocked all drive-by malware installation attempts from the more than 1,900 malicious websites tested. The software produced no false positives and required minimal resources from the computer. Major antivirus software programs caught less than 30 percent of the more than 7,000 drive-by download attempts from the same websites.

"BLADE monitors and analyzes everything that is downloaded to a user's hard drive to cross-check whether the user authorized the computer to open, run or store the file on the hard drive. If the answer is no to these questions, BLADE stops the program from installing or running and removes it from the hard drive," explained Lu.

Because drive-by downloads bypass the prompts users typically receive when a browser is downloading an unsupported file type, BLADE tracks how users interact with their browsers to distinguish downloads that received user authorization from those that do not. To do this, the tool captures on-screen consent-to-download dialog boxes and tracks the user's physical interactions with these windows. In addition, all downloads are saved to a secure zone on a user's hard drive so that BLADE can assess the content and prevent any malicious software from executing.

"Other research groups have tried to stop drive-by downloads, but they typically build a system that defends against a subset of the threats," explained Lee. "We identified the one point that all drive-by downloads have to pass through -- downloading and executing a file on the computer -- and we decided to use that as our chokepoint to prevent the installs."

The BLADE testing showed that the applications most frequently targeted by drive-by download exploits included Adobe Reader, Sun Java and Adobe Flash -- with Adobe Reader attracting almost three times as many attempts as the other programs. Computers using Microsoft's Internet Explorer 6 became infected by more drive-by-downloads than those using versions 7 or 8, while Firefox 3 had a lower browser infection rate than all versions of Internet Explorer. Among the more than 1,900 active malicious websites tested, the Ukraine, United Kingdom and United States were the top three countries serving active drive-by download exploits.

Legitimate Web addresses that should be allowed to download content to a user's computer without explicit permission, such as a browser or plug-in auto-updates, can be easily white-listed by the user so that their functionality is not affected by BLADE.

The researchers have also developed countermeasures so that malware publishers cannot circumvent BLADE by installing the malware outside the secure zone or executing it while it is being quarantined.

While BLADE is highly successful in thwarting drive-by download attempts, the development team admits that BLADE will not prevent social engineering attacks. Internet users are still the weakest link in the security chain, they note.

"BLADE requires a user's browser to be configured to require explicit

consent before executable files are downloaded, so if this option is disabled by the user, then BLADE will not be able to protect that user's Web surfing activities," added Lee.

Provided by Georgia Institute of Technology