Hooks hijacked? New research shows how to block stealthy malware attacks

November 3 2009

The spread of malicious software, also known as malware or computer viruses, is a growing problem that can lead to crashed computer systems, stolen personal information, and billions of dollars in lost productivity every year. One of the most insidious types of malware is a "rootkit," which can effectively hide the presence of other spyware or viruses from the user - allowing third parties to steal information from your computer without your knowledge. But now researchers from North Carolina State University have devised a new way to block rootkits and prevent them from taking over your computer systems.

To give some idea of the scale of the computer malware problem, a recent Internet security threat report showed a 1,000 percent increase in the number of new malware signatures extracted from the in-the-wild malware programs found from 2006 to 2008. Of these malware programs, "rootkits are one of the stealthiest," says Dr. Xuxian Jiang, assistant professor of computer science at NC State and a co-author of the research. "Hackers can use rootkits to install and hide spyware or other programs. When you start your machine, everything seems normal but, unfortunately, you've been compromised."

Rootkits typically work by hijacking a number of "hooks," or control data, in a computer's operating system. "By taking control of these hooks, the rootkit can intercept and manipulate the computer system's data at will," Jiang says, "essentially letting the user see only what it wants the user to see." As a result, the rootkit can make itself invisible to the computer user and any antivirus software. Furthermore, the rootkit can install additional malware, such as programs designed to steal personal information, and make them invisible as well.

In order to prevent a rootkit from insinuating itself into an operating system, Jiang and the other researchers determined that all of an operating system's hooks need to be protected. "The challenging part is that an operating system may have tens of thousands of hooks - any of which could potentially be exploited for a rootkit's purposes," Jiang says, "Worse, those hooks might be spread throughout a system. Our research leads to a new way that can protect all the hooks in an efficient way, by moving them to a centralized place and thus making them easier to manage and harder to subvert."

Jiang explains that by placing all of the hooks in one place, researchers were able to simply leverage hardware-based memory protection, which is now commonplace, to prevent hooks from being hijacked. Essentially, they were able to put hardware in place to ensure that a rootkit cannot modify any hooks without approval from the user.

The research, "Countering Kernel Rootkits with Lightweight Hook Protection," will be presented at the 16th ACM Conference on Computer and Communications Security in Chicago, Nov. 12.

Source: North Carolina State University (news : web)

Citation: Hooks hijacked? New research shows how to block stealthy malware attacks (2009, November 3) retrieved 27 April 2024 from https://phys.org/news/2009-11-hijacked-block-stealthy-malware.html