Research on browser weaknesses triggers attacks

July 30 2008

IBM's X-Force says cyber-criminals are using public research on Web browser weaknesses to launch attacks before most users are even aware of their vulnerability. The mid-year report from the security group indicates that organized criminals are adopting new automated techniques and strategies that allow them to exploit vulnerabilities much faster than ever before.

According to the X-Force report, 94 percent of all browser-related online exploits occurred within 24 hours of a vulnerability being officially disclosed. These attacks, known-as "zero-day" exploits, are on the Internet before people even know they have a vulnerability that needs to be patched in their systems.

Many security researchers have routinely posted the code needed to exploit a weakness as part of a security advisory. According to the X-Force report, these disclosed vulnerabilities are twice as likely to trigger zero-day exploits.

"The two major themes in the first half of 2008 were acceleration and proliferation," said X-Force Operations Manager Kris Lamb. "We see a considerable acceleration in the time a vulnerability is disclosed to when it is exploited, with an accompanying proliferation of vulnerabilities overall. Without a unified process for disclosing vulnerabilities, the research industry runs the risk of actually fueling online criminal activity. There's a reason why X-Force doesn't publish exploit code for the vulnerabilities we have found, and perhaps it is time for others in our

field to reconsider this practice."

The latest X-Force report also found that browser plug-ins are the newest target-of-choice. In the first six months of 2008, roughly 78 percent of web browser exploits targeted browser plug-ins.

For more security trends and predictions from IBM, including graphical representations of security statistics, please access the full report at: www.ibm.com/services/us/iss/xforce/midyearreport

Provided by IBM