Study: Hackers Attack Computers Every 39 Seconds

February 8 2007

Are hackers trying to get into your computer right now? And what are they up to? A study by the University of Maryland's A. James Clark School of Engineering is one of the first to quantify the near-constant rate of hacker attacks of computers with Internet access - every 39 seconds on average - and the non-secure usernames and passwords we use that give attackers more chance of success.

The study, conducted by Michel Cukier, Clark School assistant professor of mechanical engineering and affiliate of the Clark School's Center for Risk and Reliability and Institute for Systems Research, profiled the behavior of "brute force" hackers, who use simple software-aided techniques to randomly attack large numbers of computers. The researchers discovered which usernames and passwords are tried most

often, and what hackers do when they gain access to a computer.

On TV and in film, these kinds of hackers have been portrayed as people with grudges who target specific institutions and manually try to break into their computers. But in reality, Cukier says, "most of these attacks employ automated scripts that indiscriminately seek out thousands of computers at a time, looking for vulnerabilities."

"Our data provide quantifiable evidence that attacks are happening all the time to computers with Internet connections," Cukier notes. "The computers in our study were attacked, on average, 2,244 times a day."

Cukier and two of his graduate students, Daniel Ramsbrock and Robin Berthier, set up weak security on four Linux computers with Internet access, then recorded what happened as the individual machines were attacked. They discovered the vast majority of attacks came from relatively unsophisticated hackers using "dictionary scripts," a type of software that runs through lists of common usernames and passwords attempting to break into a computer.

"Root" was the top username guess by dictionary scripts - attempted 12 times as often than the second-place "admin." Successful 'root' access would open the entire computer to the hacker, while 'admin' would grant access to somewhat lesser administrative privileges. Other top usernames in the hackers' scripts were "test," "guest," "info," "adm," "mysql," "user," "administrator" and "oracle." All should be avoided as usernames, Cukier advises.

The researchers found the most common password-guessing ploy was to reenter or try variations of the username. Some 43 percent of all password-guessing attempts simply reentered the username. The username followed by "123" was the second most-tried choice. Other common passwords attempted included "123456," "password," "1234,"

"12345," "passwd," "123," "test," and "1." These findings support the warnings of security experts that a password should never be identical or even related to its associated username, Cukier says.

Once hackers gain access to a computer, they swiftly act to determine whether it could be of use to them. During the study, the hackers' most common sequence of actions was to check the accessed computer's software configuration, change the password, check the hardware and/or software configuration again, download a file, install the downloaded program, and then run it.

What are the hackers trying to accomplish? "The scripts return a list of 'most likely prospect' computers to the hacker, who then attempts to access and compromise as many as possible," Cukier says. "Often they set up 'back doors' - undetected entrances into the computer that they control - so they can create "botnets," for profit or disreputable purposes." A botnet is a collection of compromised computers that are controlled by autonomous software robots answering to a hacker who manipulates the computers remotely. Botnets can act to perpetrate fraud or identity theft, disrupt other networks, and damage computer files, among other things.

This study provides solid statistical evidence that supports widely held beliefs about username/password vulnerability and post-compromise attacking behavior. Computer users should avoid all of the usernames and passwords identified in the research and choose longer, more difficult and less obvious passwords with combinations of upper and lowercase letters and numbers that are not open to brute-force dictionary attacks.

Source: By Rebecca Copeland, University of Maryland