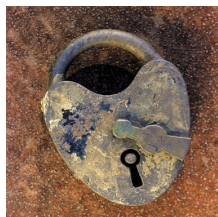


14 July 2008

By: George Craciun, Security News Editor



SSH attacks target servers  
Silicon Republic

## [Security Software Fails to Report SSH Attacks](#)

### *How hackers manage to go undetected*

Servers with open SSH ports have recently begun to come under hacker attack, which seems to be coordinated, although it is not automatically reported because the hackers employ a brute force attack from more than one machine. Nazar Aziz, IT consultant and developer, has been vigilant enough to detect the attack, which started at the beginning of this month. Here is how the whole thing goes: if a hacker tries to gain access to a machine, the security software detects the attack and auto-reports it. The attacker's IP is banned, and the brute force attack is halted; this is what happens when the hacker uses just one machine and one IP to route the attack. There is a more efficient way of avoiding detection: using several hosts with different IPs. Brute force SSH attacks are easily detected by security solutions, but not when the attacker tries to guess the password three times and then switches to another IP. Instead of using the same IP and running an endless amount of queries, he/she uses several ones and runs three queries from each. "This attack is different in that there appears to be a single list of usernames/passwords and a list of SSH servers to attack. Bots pick a user name and only attempt a brute force attack three times before the same server is passed along to the next bot. Since the attack is relayed to the next bot (with a different IP address) the attack in effect is continued without being detected by this method," says Nazar Aziz as cited by [The Register](#). According to Aziz, this form of attack started earlier this month. He manages a small bank of Linux servers, and when the attacks commenced he was vigilant enough to detect them. A closer inspection of the system logs revealed that the servers were indeed under a coordinated attack. How was Nazar Aziz able to pick up on this when other surely would have missed it? It all has to do with the fact that a couple of months back he fell victim to a hacker attack, which determined him to be more cautious than the usual server admin.