

By: ~~April 2008~~ Popa, Security and Search Engines Editor

Colorado Students at Risk Due to Major Security Breach

University of Colorado at Boulder hit by security breach

We've seen it so many times, we see it again and we'll probably see it in the future: computers hosting important information get compromised, mostly due to weak security measures set up by the administrators. This time, there are "only" 9,000 affected students and about 500 instructors according to a report by NetworkWorld. A computer of the University of Colorado at Boulder got compromised a few days ago and, due to its suspicious behavior, the administrators found malicious code installed on it. I wonder what could have happened if the installed malware had not modified the computer activity...However, according to the same source, the computers were automatically restarted every once in a while, a fact that attracted the administrators' attention who started an investigation. Moreover, "the university has called in Applied Trust Engineering to help with a forensics investigation," NetworkWorld [adds](#). "The computer started misbehaving. People saw suspicious behavior, like the re-booting," Greg Stauffer, IT services communications manager, commented. The university will start sending letters to the ones affected in order to inform them about the security breach. And now, some juicy details regarding the information stored on the compromised computer: the system hosted all kinds of details including here names, addresses, Social Security Numbers and grades. As mentioned, there were no less than 9,000 affected students and 500 instructors. As I've said, there were lots of cases in the past and even if they could be an important example for security administrators out there, such breaches occur every once in a while. Obviously, the most important data loss that comes in our minds is the HMRC issue when no less than 25 million people were put at risk due to 2 unencrypted discs sent from a department to another. Moreover, there were several data breaches reported, most of them being possible especially because of the weak security measures or no security tools at all...