Puzzle for November 20, 2006

This is from *SANS NewsBites* Vol. 8, Num. 15. What do you think of iDefense's idea?

> Microsoft has spoken out against iDefense's offer to pay US$10,000 to people who find and reveal to them critical vulnerabilities in Windows. According to a Microsoft spokesperson, the company “does not believe that offering compensation for vulnerability information is the best way [to] protect customers,” and instead prefers that “researchers” ensure a fix is available from vendors before disclosing the details of a vulnerability. iDefense says it believes their offer “promotes the concept of responsible disclosure.” iDefense Labs Michael Sutton said he finds it curious that Microsoft's Antivirus Reward Program offers US$250,000 for information leading to the arrest and conviction of malware writers, but is opposed to iDefense's program. Peter Mell, who manages the National Vulnerability Database (NVD) at the National Institute of Standards and Technology (NIST), says iDefense's program could skew bug hunters' attention to certain vendors rather than helping improve security in the industry.