Subject: Database restored
Posted by xptek on Thu, 02 Jun 2005 00:49:00 GMT

CrimsonBecause part of the attack today was carried out by distributed code to bots. It's clever, of course, because it makes it difficult to pin down one attacker by IP. There also seems to be some sort of relationship to a soon-to-be-shut-down website that was hosting a password stealing script that many of you may have fallen victim to.

Blazer and I are still going through all the data: but a few things are clear.

1) The person who did this has a modicum of talent (not "smart" but smarter than most script kiddies)
2) The attack's effects were NOT worth the effort obviously put into the attack considering I was able to fix everything within a few minutes of actual work.

We are pretty sure several passwords were stolen, but they are MD5 hashes which will hace to be bruteforced to see in plain text, but can currently be used to log in as any user whose password was stolen. In fact, the attacker (who I'm 99.9% sure is Spoony or was ordered by him) is possibly already posting under other people's accounts.

Try again.