Password hash leaks at LinkedIn, EHarmony, and Last.fm

The Week of Leaks

LinkedIn

- ~6.5 million SHA-1 password hashes were posted for public view (of ~150 million users?)
- Passwords were hashed one time and were unsalted
- Usernames were not posted with the password hashes (but it should be assumed they were also compromised)

EHarmony

- ~1.5 million MD5 password hashes were posted for public view (of ~20 million users?)
- The hackers asked for assistance cracking this list and 1.22 million were cracked and posted in a matter of hours.
- Passwords were hashed one time and were unsalted
- Usernames were again not included with the hashes.

Last.fm

- Password hashes were posted publicly relating to this breach and has been said to be in the millions. Last.fm did confirm that they were hacked.
- A person that worked for Last.fm states that hashes they used were MD5 and were unsalted.
- Suspicions that they were attacked were raised in May 2012, but did not find evidence of a breach. This was related to users get spammed at their Last.fm specific email addresses.

Take Aways

- All of these breaches came to light within a few days of each other making security researchers wonder how connected they are.
- Could there be a zero day exploit in the wild that allowed the hackers to get these hashes? Or were the companies involved lacking in their security and using unpatched software?

References

- http://techcrunch.com/2012/06/06/6-5-million-linkedin-passwords-reportedly-leaked-linkedin-is-looking-into-it/
- http://arstechnica.com/security/2012/06/8-million-leaked-passwords-connected-to-linkedin/
- http://gigaom.com/europe/last-fm-suspected-password-breach-weeks-ago/