Aplura, LLC
4036 Wildwood Way
Ellicott City, MD 21042
301-523-2110 (w)
410-864-8386 (f)

Focused Information Security
www.aplura.com

Password Reuse

Essay By: Sean Wilkerson and Daniel Deighton

October 22, 2009

Attackers recently targeted Microsoft Hotmail users and were able to compromise in excess of **30,000** accounts. Gmail and Yahoo webmail users also had their account-credentials appropriated, but not nearly at the volume of Hotmail. If you have accounts on any of these e-mail systems, take the time to change your password immediately.

Complexity requirement is most often the major problem with passwords and although it is a real threat, that topic deserves its own (future) essay. The critical issue of the day is a rapidly-growing trend that attackers may gain access to your personal (including financial) information if you use the same password between multiple accounts. If you share passwords between accounts, then a compromise of one could provide an attacker with the keys to your entire online life. For example, the bad guys first knock over a less-secure site and harvest the user accounts (e.g. passwords). Then they reference the stolen accounts to see if they exist on other entities such as retail or banking sites. Although this reconnaissance sounds time-intensive, there are many resources which automate this task and allow anyone to check the existence of a username across hundreds of sites within a few seconds.

A few months ago, a large number of well-known security professionals were hit with this same attack. Many of them had accounts on the frequented Hak5 website used for collaboration. When Hak5 got ... hacked ... the bad guys were able to collect the user-data. They then successfully used the stolen credentials on the personal servers and e-mail accounts of the victims. Many well-known security professionals had accounts on Hak5 and therefore the attackers now had their information in the palm of their hands. This was a black eye to many of the elite in the security community, but the moral of the story is that even the pros don't always do it right.

It is best practice to use a unique password for each account. However, this isn't easy since it requires one to track dozens of different passwords to minimize the effect of a single compromise.

There are a few shortcuts which might help to mitigate the risk of account compromise through password reuse, though all carry some additional risk.

The user might memorize a short password of 6-8 characters then apply small adaptations to that password depending on where it is used. For instance, the user's password might be *i4T8u^* which when used at AmaZon.com an *A* and *Z* could be integrated into the password creating *Ai4T8u^Z.* The resulting password is complex but easy to remember. The downside is if the attacker learns the pattern then they might easily guess any other account by the same owner.

The user might memorize a small handful of passwords each to be used with only a certain *class* of account. The class distinction could be: Major online e-tailers, financial institutions, news organizations, lower-grade e-tailers, and maybe reserve one for random small sites. This practice is not as strong as using fully-diverse passwords for each account, but it is better than sharing one for all.

An alternative to memorizing every unique password is to use Password Management software. This software typically stores your account information (including passwords) in an encrypted database. You only have to remember one, really strong, password to gain access to all of your different credentials. When needed, it is simply a matter of copying the username and password into the login form from your password management software application. Although this is simple, it also has some risks associated with it which should be considered before use.

As we shift our lives further online we face many challenges in maintaining the integrity of our accounts. Managing unique passwords may be cumbersome, but puts one extra hurdle between the bad guys and you.

References

Definitions and Research:

- String Reuse: http://websitehelpers.com/general/passwords.html
- Password Management Software: http://en.wikipedia.org/wiki/Password_manager
- Password Strength: http://en.wikipedia.org/wiki/Password_strength

News Items:

- Hotmail Attack Announcement: http://windowslivewire.spaces.live.com/blog/cns!2F7EB29B42641D59!41528.entry?wa=wsignin1.0&sa=363915619
- Hotmail Incident Response: http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=220301340
- Hotmail/Password Reuse: http://www.itbusinessedge.com/cm/blogs/mah/phishing-attacks-underscore-importance-of-protecting-e-mail-passwords/?cs=36775
- Hotmail Attack Shows Weak Passwords: http://blogs.zdnet.com/security/?p=4538
- Google users attacked too: http://news.bbc.co.uk/2/hi/technology/8292928.stm
- Security Gurus Fall Prey: http://news.softpedia.com/news/Security-Gurus-0wned-by-Black-Hats-117934.shtml
- Hak5: http://www.hak5.org/
- Hak5 Attack: http://forums.remote-exploit.org/general-discussion/24848-hak5-hacked.html
- Password Reuse: http://www.telegraph.co.uk/technology/news/6125081/Security-risk-as-people-use-same-password-on-all-websites.html

Tools:

- Account Reconnaissance across 128 sites: http://namechk.com/
- Account Reconnaissance across 150 sites: http://friendscall.me/
- Account Reconnaissance across 340 sites: http://knowem.com/