Bad Apples!

For the first time, Apple Macintosh users are being targeted with MalWare.

There has been a certain amount of smugness and a sanctimonious attitude from elements of the Mac community towards the long suffering Windows users. This has been in respect of the blight of MalWare in the forms of Viruses, Worms, SpyWare, AdWare etc that affect Windows users every time they connect to the Internet.

However, as the “Halo” effect of the iPod drags the rest of Apple’s product range into the main stream, then the community of malicious code authors are also going to sit up and take notice.

The MalWare authors, to use the oft repeated marketing slang, go after the “low hanging fruit” first. That is to say, the more versions of a platform such as Windows on the Internet with the potential of a successfully crafted piece of MalWare infection, the more notoriety or cash they will generate for themselves. Let’s not fool ourselves here on the motivation for the MalWare authors either. There is fortune to be made by the MalWare author. This is either through the renting of compromised “zombies” on the Internet for Denial of Service attacks or the mass distribution of billions of SPAM emails.

As the number of Mac owners increase, then this platform becomes a viable target for expending research effort for crafting new MalWare.

A lot of this attraction to the Mac OS X platform has been facilitated by the migration of Apple a number of years ago towards a BSD based Unix base for the Tiger Operating System and Leopard of the future. Many students would have come across BSD variants in the past and be more familiar with the structure of the Operating System, and where to target their efforts than the previous Mac Operating System.

In the last weeks, there have been a number of proofs of concept pieces of MalWare released to the Internet to attack the Mac OS X platform. Admittedly, these are not spreading with the speed of the usual Windows based MalWare, but it does signal a sea-change for the Apple user community.

It is no longer acceptable for Mac users to expect that because of either a level of obscurity or architectural superiority of the Mac OS X that they are immune to the vile tide of MalWare that attempts to break down the defences that attempt to breach our computer on a daily basis.

As with all Windows based PC users, the Apple Mac community are now going to have to start “wearing their seatbelts” if they want to continue to use the Internet in a MalWare free way.

Updates are, and have been, available for the recent vulnerabilities that have been identified. The same principles that apply to Windows users apply to the Mac experience;

- Have a reliable and up to date anti-virus software package installed
- Keep your Operating System and application patches up to date

- Have your network firewall enabled and properly configured
- Do not open attachments that you are not expecting!

The types of issues discovered in the last weeks have included using the Safari web-browser to visit a malicious site and run exploit code on the target Mac, including install a root-kit. Installation of a root-kit on any computer is a holy grail of the MalWare author.

This increased attention on the Mac platform over the last weeks is a symptom of Apple becoming a victim of their own success.

The MalWare released to date has been largely ineffective in spreading. However, it is only a matter of time before a virulent piece of MalWare arrives that will catch the complacent Mac user napping, and if it is anything like some of the recent, destructive, PC based MalWare, it could be devastating.