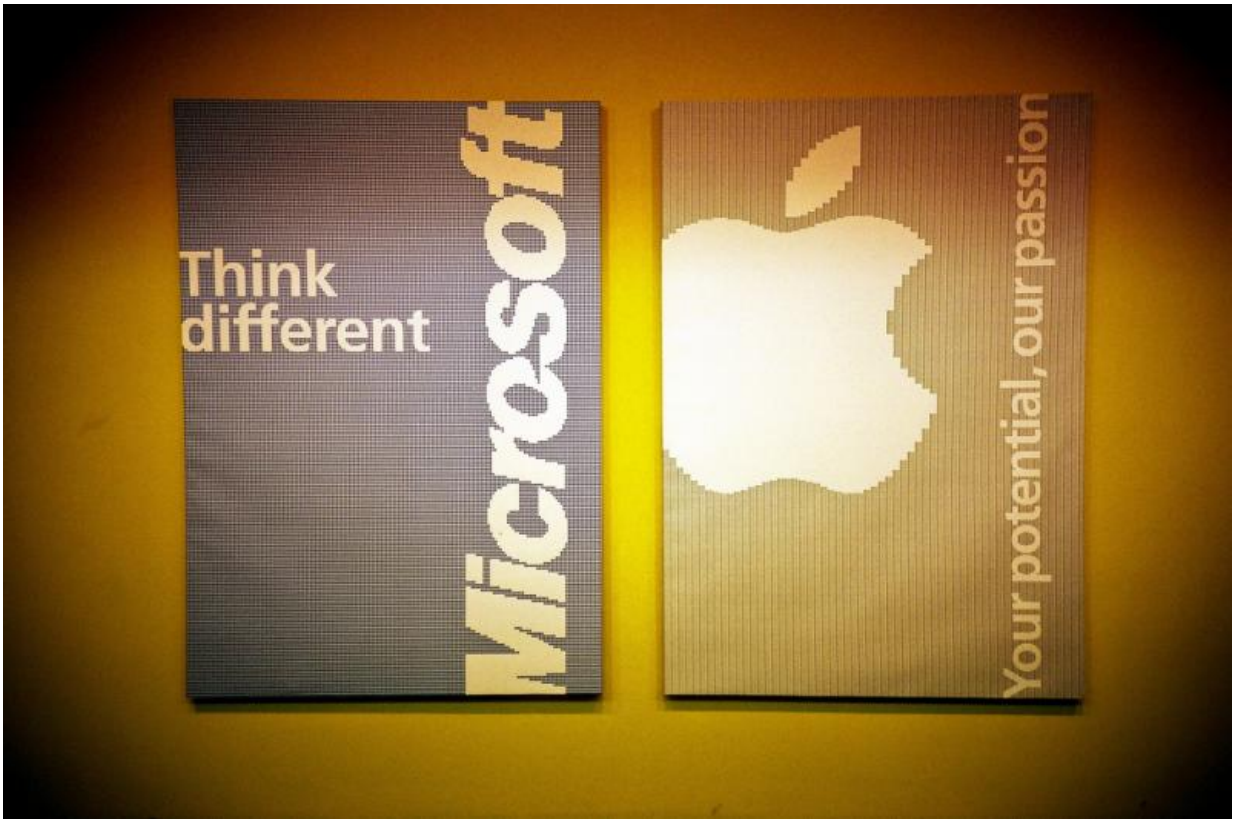
Which is more vulnerable to viruses and hackers: Windows 10 or Mac OS X?

August 12 2015, by Robert Merkel



Which operating system is safer from a hack attack? Credit: Flickr/Chaos, CC BY-NC-ND

During the 2000s, Apple ran a hugely successful advertising campaign for its line of Macintosh desktop computers. The ads poked fun at some

of the perceived bugbears of the Windows-based PCs of the era compared to the Mac.

One recurring theme of these ads was the greater vulnerability of Microsoft's PCs to viruses.

The perception that Macs are safer to use than PCs persists in some quarters to this day. But is it the case that Apple's latest OS X Yosemite is more secure than the newly-released Windows 10 from Microsoft?

Security by obscurity

Whatever the technical vulnerabilities of the two systems, the historical lack of malware targeting Apple systems was at least in part due to Apple's own lack of market share.

Definitive statistics for the market share of operating systems are hard to come by, but one useful estimate is available from the server traffic records of Wikimedia (the non-profit organisation that runs Wikipedia).

In April 2009 (the earliest date from which records are readily available) nearly 90% of traffic came from computers running Windows, compared to only 6% for Mac. By July 2015 Windows had dropped to 41.7% and Mac to 5.4%. Most of the rest now comes from smartphones and tablets running Apple's iOS and Google's Android.

So back in 2009, Windows represented a far larger target than Mac for profit-seeking virus and malware authors. While that is still the case today, the relative payoffs have changed substantially. Mac users tend to be wealthier than average and are likely to be more heavily concentrated in wealthier developed countries, which may attract malware authors to Macs.

Hardening up

Over the years both Microsoft and Apple have taken many measures to reduce the risks from malware. Both devote considerable time and resources to removing security-related faults in their own software and preventing the introduction of new ones.

Microsoft has disclosed information about its Security Development Lifecycle, both to encourage confidence and to promote the development of more secure software across the industry. Apple is much less forthcoming about the specifics of its internal security efforts.

However, security bugs are still being discovered in released versions of both OS X and Windows on a regular basis. What has changed for the better is the ease and speed with which security fixes to software are distributed and installed.

Microsoft's policy relating to the disclosure of security flaws says it will publicly reveal a vulnerability, even without a fix, if it becomes aware the vulnerability is being exploited. Apple's policy is to never comment on security faults until they have been fixed.

Both companies have also introduced a number of features that make it harder for bugs to be exploited to allow attackers to take control of systems.

App stores and walled gardens

Perhaps the biggest change to the security of the two major desktop operating systems is through the combination of app stores, signed applications and "sandboxing". In combination, these features go a long way to make sure that the only software running on OS X or Windows is:

- written by an identifiable developer
- audited by Microsoft or Apple before being available from their app store
- "sandboxed" so that it can only perform the actions it legitimately needs to, rather than having full access to everything on the system.

Aside from the security implications, app stores have commercial implications. Only applications approved by Apple or Microsoft can be sold through them, and those companies take a cut of any sales.

These walled gardens are of concern if you believe (as I do) in the "freedom to tinker". But they do significantly reduce both the potential for malware to make its way onto systems, and the harm such malware can do if they somehow get through.

The technical details of the Windows and the OS X app stores and sandboxing models are slightly different to each other, although the end results are reasonably similar.

But there is a straightforward way to bypass these protections: many users need the ability to run their older applications, so both operating systems provide mechanisms to install and run non-sandboxed code.

Successful attacks on non-sandboxed applications leave the rest of the user's computer vulnerable. The existence of a mechanism to install and run any program downloaded from the internet also gives malware authors a "social engineering" attack – in a nutshell, tricking users into running downloaded software that contains malware.

Windows 10 has a new sandboxing model for corporate applications called Device Guard that will make it harder for unauthorised applications to be executed.

It is currently restricted to the Enterprise version of Windows 10 because its mechanisms for approving older applications to run are too unwieldy for home users. But, over time, some version of the Device Guard system will likely filter down to the home editions of Windows, making life more difficult for malware authors.

The verdict

So which is the safer operating system to use? For what it's worth, I use both Windows and OS X (as well as Linux, Android and occasionally iOS), and I see no particular reason to choose between them on security grounds. I share the concerns of David Glance, writing on The Conversation, about Windows 10's privacy policies, but that's not strictly a security issue.

All operating systems are vulnerable to hackers, but the risks can be reduced if you adopt basic computer security measures. These include installing anti-malware software and installing operating system and application security updates promptly.

And there are other risks you face regardless of the operating system you choose. Web browsers and plugins, other applications and the security practices of the websites that you visit are agnostic to whether you're on Windows or Mac.

Source: The Conversation

hackers-windows-mac.html