Think your Mac’s beyond malware attack? Alas, those days are gone

For a long time Mac users would look at all the malware (malicious software) that infects Windows PCs and think how fortunate they were that such attacks did not happen to MAcs.

But now, it would seem, things are starting to change.

Over the weekend anti-virus software developer Kaspersky Lab announced that a new trojan horse – a program that pretends to be something else while giving control of the infected PC to a remote user – called SabPub, has been spreading among Macs.

The trojan can be spread by one of two methods:

- by opening a Microsoft Word document that arrives as an email attachment entitled “10th March Statement” [sic]
- by exploiting a vulnerability in Java – a programming language used to create add-ons for web browsers and other applications.

Once activated, the SabPub trojan opens a “backdoor” that allows attackers to gain full access to a victim’s system.

The news of SabPub (or Backdoor.OSX.SabPub.a as it’s formally known) follows the discovery of other Mac malware, including MacDefender, MacGuard and Flashback.

The last of these was found to have infected more than 650,000 Macs worldwide and was spread via a Java “applet” on infected websites.

(Late last week Apple made a standalone Flashback removal tool available for download.)

It would seem we are entering a new era where Mac users are as fair game to hackers as PC users.

Same as it ever was?

In reality, there has never been any fundamental reason why Macs should be immune to viruses and trojans or any other malware. But for a very long time there were some factors that made them a significantly smaller target than the PC.

First, the market share enjoyed by Windows PCs was so much greater than that of Macs. If a hacker was to construct malware that relied on a particular operating system to get around, it was far more likely to land on a PC than a Mac, so it made sense to write it for the PC.

PC and Mac operating systems rely on different architecture and although both are written in the language C, the version of C used in writing the Mac operating system is more robust than used on the PC.

Second, for a very long time, PCs ran software that was such an easy target. It was much easier to find exploitable flaws in PC software than it was for a Mac.

We are starting to see more nasties emerge on Macs than ever before. Dave Delaney

Windows software, at least in the early days, was not written in a particularly defensive way. Some of the ways the infamous Blue Screen of Death could be forced in earlier versions of Windows – such as the “Ping of Death”
where an echo request was sent with a payload greater than 64 kilobytes – seem extraordinarily simple these days.

Third, in the past, Macs tended to be purchased for commercial purposes rather than home users. As a result Macs were more likely to have patches applied and software updated than was the case for domestic users.

Finally, there was considerable antipathy towards Microsoft arising from the browser wars that saw PCs being targeted.

Apple didn’t necessarily command the respect and devotion it does today but at least its products inspired less loathing within the hacker community than did Windows products.

All of the above factors are much less the case than they once were. Indeed, the Mac has, to some extent, become a victim of its own success.

There are a lot more Macs around now and the iPad and iPhone dominate the tablet and smartphone markets respectively.

Additionally, Microsoft software seems to be much more stable than it used to be. Blue Screens Of Death may not be a thing of the past, but are perhaps less common than they once were.

Finally, Apple’s reputation has suffered in some ways over the past few years, notably in (possibly untrue) reports about conditions in its manufacturing plants and the company’s involvement in high-profile legal tactics that has not endeared it to the hacker community.

At the same time Microsoft has taken a more relaxed attitude to some mild hacking activity, such as the “jailbreaking” (overriding the intended limitations of) some of its systems.

And perhaps there is another reason that Macs are increasingly becoming the target of attacks; a reason that’s difficult to prove but worth speculating on.

Hacking has become more of a commercial activity than it used to be. It is interesting that MacGuard and MacDefender attempted to obtain credit card information from users and that Flashback caused infected hosts to join a botnet that could possibly be hired out in future.

It would seem that hackers nowadays are more motivated by commercial gain than ever before.

It would be an ironic outcome if the early antagonism directed toward Microsoft because of its supposedly ruthless commercialism was now directed toward Apple because of the ruthless commercialism of some hackers.