

When is a disclosure not a disclosure?

A number of months ago, this column covered a topic that related to the increased attention that the Apple Mac OS X was receiving from the Malware authors and the hacking community in general.

A number of OS X security patches had been released and a small amount of Malware appeared in terms of worms and viruses. None of these had been in any way successful in propagating.

There was some discussion on different forums and blogs about the apparent smugness of the Mac community when it comes to the integrity of their operating system.

This fuelled some of the negative human elements we all harbour that wish harm upon someone else that seems to be better off than we, and is also smug about it at the same time.

At the recent Black Hat security conference in Las Vegas, two senior researchers from the company SecureWorks ran a presentation where they demonstrated the ability to hack an Apple MacBook remotely. This was a sensational headline and instantly catapulted the two researchers and their company in to the limelight and seemingly a guarantee of entry to the hacking hall of fame. There was a media scrum surrounding these claimants and their demonstration of the attack. Many other newsworthy items at the conference were tossed like flotsam in the wake of the "Story of the Conference".

Dave Maynor and Jon Ellch of SecureWorks exploited a vulnerability that existed, they claimed, in the Apple Airport wireless network drivers on the MacBook. This exploit allowed them to execute code remotely on the laptop and take complete control of the computer. The headline rapidly circulating on these news stories was along the lines of "Gone in 60 seconds", as the pair claimed that is how long the attack takes to perpetrate.

To add insult to the injury of the Mac community, the pair referred to the "Mac user base aura of smugness on security." as one of the reasons that they targeted this vulnerability for exploit. The Mac community were reeling. Body blows such as this, they were not used to. Where was Steve Jobs with his words of wisdom and calm!

In the last couple of weeks, the pair have had to fess up.

The vulnerabilities that they exploited to take remote control of the MacBook were actually based on a 3rd party device driver that was installed on the laptop. The wireless card being used for the demonstration was a USB connected external one and not the Apple Airport card that is standard in the MacBook, and virtually all other Apple computers. This revelation seriously undermined the credibility of the two researchers and their company SecureWorks. They have had to admit that the faults lay not in the Apple OS X native drivers for the Apple Airport wireless adapter, but in the drivers of a yet un-named 3rd party USB wireless adapter. Interestingly, the SecureWorks web site refers to not naming the 3rd party adapter manufacturer: "As

part of a responsible disclosure policy, we are not disclosing the name of the third-party wireless device driver until a patch is available.”

I wonder why they thought that it was acceptable to state in the original presentation at Black Hat that the vulnerability lay with the Apple Airport driver, even though Apple had not been informed or a patch made available?

This issue comes back again to the responsibility that security researchers have today. It is not acceptable for a company to publicise a vulnerability, and the exploit code for this vulnerability in some cases, without having notified the manufacturer. Most researchers agree an acceptable period of time with the manufacturer to develop, test and deploy a patch for the issue before going public. In almost all circumstances, the manufacturer will give credit to the researchers in their announcements to ensure that the recognition is given for the effort expended.

The sort of tabloid sensationalism with which the SecureWorks researchers approached the Black Hat conference has to be seen as a sad day in the security research field. The information presented was factually incorrect and the presentation was crafted to undermine confidence in the Apple Mac OS X. This appears to have been motivated by the desire of the presenters for their 15 seconds of fame and their grudge against the perceived smugness of the Mac community.

This has backfired in the worst possible way for them, and they must now be seen in a sceptical light in the future on any research papers they present. What was a technical tour de-force for the researchers in getting exploit code to run on the back of a 3rd party USB wireless device driver vulnerability has been swept away.

The Mac community can quite rightly turn around, with a wry grin, and say “Told you so.....”

Rits Group Head Quarters
Information Security Centre
2052 Castle Drive
Citywest Business Campus
Co. Dublin
Ireland

Tel: +353 (0) 1 6420500
Fax: +353 (0) 1 4660468
Email: info@ritsgroup.com
Web: www.ritsgroup.com