

New variant of Mac Trojan discovered, targeting Tibet

nakedsecurity.sophos.com/2012/11/13/new-mac-trojan/

By Graham Cluley

13 Nov 2012



It's true to say that there's a lot lot less malware in existence for

Macs than there is for Windows PCs. But that doesn't mean that it doesn't exist at all.

And clinging onto the statistics of the much smaller proportion of Mac malware compared to Windows malware is going to be cold comfort if your Apple Mac is the one which ends up getting infected.

The latest Mac malware seen by the experts at SophosLabs, is a new variant of the OSX/Imuler Trojan horse. In the past, earlier variants of the OSX/Imuler malware has been spread via [topless photos of a Russian supermodel](#) or embedded deep inside [boobytrapped PDF files](#).

This time, it appears that the a version of the Imuler Trojan has been used in an targeted attack against sympathisers of the Dalai Lama and the Tibetan government, as the malware appears to have been packaged with images of Tibetan organisations.



If your Mac was successfully infected by malware like this, you have effectively given remote control of your computer and your data to an invisible and unknown party. They could steal files from your Mac, spy on your emails, and plant further malware onto your systems.

(It will be left as an exercise to the reader to come up with a shortlist of who might have an interest in breaking into the computers of Tibetan organisations).

Customers of Sophos, including users of **Sophos's free anti-virus for Mac**, are protected against the malware which has been detected as a variant of the OSX/Imuler-B backdoor Trojan since the early hours of 11th November 2012.

Users of other Mac anti-virus products may be wise to check with their vendors if they are protected.

This new malware variant may not be widespread – but it is another indication that the malware threat on Macs is real, and should not be underestimated.