



INTEGO SECURITY MEMO – October 17, 2008

Rogue Macintosh Security Software, MacGuard, Claims to Protect Macs

Exploit: MacGuard rogue Macintosh security software

Discovered: October 17, 2008

Risk: Low to Medium (no current risks to Macintosh computers, but a potential financial risk to purchasers)

Description: Intego has discovered a rogue program claiming to be Macintosh antivirus software. MacGuard¹ claims that it will “search your hard drive for malicious objects such as Adware, Spyware and Trojans, cleaning your files, eliminating the threats, and securing your privacy in just a matter of minutes.” However, the description of this software is merely a clone of a well-known Windows rogue security software tool that has been proven to be malicious. The software may be dangerous to Mac OS X, and there is a risk that the company “selling” this software may be scamming users and some sources suggest that they may be using the credit card numbers they harvest for nefarious purposes. Pandalabs suggests² that there may be 30 million computer users (essentially Windows users) infected by such rogue software.

MacGuard’s web site is the same as the site of Winiguard³ (with the word “Windows” replaced by “Mac OS X”), which is both a scam that attempts to sell useless software and a dangerous rouge tool that “hijacks the user’s desktop and typically displays exaggerated or false claims of spyware found to frighten the user into paying for the program,” according to Sunbelt Malware Research Labs⁴.

There are several signs that should alert users to the danger of this MacGuard program. First, the web site contains a graphic not of a Mac, but of a Dell computer. (An Apple logo is sloppily pasted over the computer’s monitor.) Second, the language on the site is confusing, and contains many typos; in addition, it doesn’t describe features that would appear in a Mac security program. The site claims such things as “Full Mac OS X Security Center Support” (there is a Windows Security Center in Windows, but nothing by that name in Mac OS X); and “Macguard finds out and removes more than 100000 Trojan horses, Spyware, Viruses, Hackers, Adware, Keyloggers and another harmware” (there are far from 100,000 types of malware that affect Mac OS X). The Winiguard web site provides a download that infects computers running Windows; the MacGuard site does not currently download any software when you click its Download link, but it is likely that it will do so at a future date.

Further evidence of the danger of this software is the ownership of the web site itself. Both domain names are registered to the same person, and the web site claims to be “owned and operated by Innovagest 2000 SL”, a company known to disseminate a well-known rogue anti-spyware tool for Windows.

Intego is issuing this memo to help Mac users understand that not every program that claims to protect Macs is indeed reliable, and that this one is potentially dangerous. Mac users that want to protect their Macs should look for trustworthy, reliable software that has proven itself over the years. They should check the mainstream Mac sites for reviews of such products to see if they are good, bad, or unknown.

Intego VirusBarrier will protect against this rogue software, if and when a download is available from the MacGuard web site. Intego will be posting more information, as it becomes available, on the Intego Mac Security Blog (<http://blog.intego.com>).

¹ <http://macguard.net>

² http://pandalabs.pandasecurity.com/archive/Who-Wants-to-Be-a-Millionaire_3F00_.aspx

³ <http://winiguard.com>

⁴ <http://research.sunbeltsoftware.com/threatdisplay.aspx?name=WiniGuard&threatid=442288>

