

22 November 2008

By: Marius Oiaga, Technology News Editor



Rogue software:  
Windows Antivirus  
2008  
Microsoft

## [Fake Windows Antivirus Code Infected 1 Million Computers](#)

### *Rogue security solutions*

Even with Windows 7 in pre-Beta stage, Microsoft is emphasizing the need for end users to run security software with the operating system, indicating that it is working with members of the industry in order to have the first antivirus products tailored for the Windows client as early as the [Beta development milestone](#). Fact is that the necessity to install security solutions is valid for all Window operating systems, not just Windows 7, but at the same time, there are some antivirus products that users need to steer clear of. Just in November, Microsoft contributed to removing malicious code posing as Windows antivirus solutions from approximately 1 million computers worldwide.

Products including Micro Antivirus 2009, MS Antivirus, Spyware Preventer, Vista Antivirus 2008, Advanced Antivirus, System Antivirus 2008, Ultimate Antivirus 2008, Windows Antivirus, XPert Antivirus, Power Antivirus and Ultra Antivirus 2009 have a lot in common, but nothing whatsoever with genuine security products. Fake security software has grown to the size of a veritable plague, managing to deliver a consistent hit to the usability of infected PCs in order to blackmail the users into paying for the removal of incessantly nagging notifications.

Rogue security "software tells you that your system is crawling with bad stuff (for free!) and then offers to remove it for you (that'll cost you). Of course the stuff they report is completely bogus; they are incapable of finding any real malware. What's more they can be very insistent, repeatedly displaying popup warnings that make it virtually impossible to use your machine unless you pay to 'register' the program," revealed Microsoft's [Hamish O'Dea](#).

Scareware including Micro AV, MS Antivirus, Spyware Preventer, Vista Antivirus 2008, Advanced Antivirus, System Antivirus, Ultimate Antivirus 2008, Windows Antivirus 2008, XPert Antivirus, Power Antivirus and others are identified by Microsoft as members of the [Win32/FakeSecSen family](#).

The Modus Operandi is always the same. Installed on the users' machines, or simply when accessing a webpage, Win32/FakeSecSen will perform a fake scan of the PC for free and report inexistent problems, raging from malware infections to privacy concerns. However, once the inherent list of bogus malicious code infections has been produced and delivered to the end user, the false resolve is only made available for a fee. Paying for the rogue security software will only result in the product removing the threats which did not exist in the first place.

"An interesting, but not unusual, characteristic of Win32/FakeSecSen is that it uses many different disguises. As well as further contributing to the level of FUD and making them harder to keep track of, this might broaden their appeal to a wider audience - while one person may be convinced by something called "Ultimate Antivirus", another would be more likely to install 'Vista Antivirus 2008'. It may even lead to the same person being duped by the same rogue more than once," O'Dea explained.

994,061 Machines

As of November, [the Malicious Software Removal Tool](#) also added Win32/FakeSecSen to

the limited list of malicious code it is designed to hunt down. Since introduction into the MSRT, the rogue antivirus was removed from no less than 994,061 computers, according to Microsoft. The Redmond company estimates that for every 1,000 machines scanned in the U.S. alone, seven days ahead of November 19, approximately five had been infected with Win32/FakeSecSen.

"There is no surprise about the prevalence of these rogues given our earlier telemetry analysis on other Microsoft AV products and tools. For comparison, the #1 family last month was Renos with 389,036 distinct machines cleaned in the first week and 655,535 machines for the whole month. And the most significant result for MSRT this year was the June release when we added eight game password stealer families, was Win32/Taterf with 1,246,792 machines cleaned by week 1 and 1,536,831 machines for the whole month," [explained](#) Microsoft's Scott Wu, Scott Molenkamp and Hamish O'Dea.

Statistics provided by Microsoft pointed out that just 198,812 of the instances in which Win32/FakeSecSen had been removed actually contained an .EXE file. According to the company, this is illustrative of the fact that the rogue security software's executables had been removed manually or via [legitimate antivirus products](#), while the incomplete Win32/FakeSecSen files could represent failed installations.

The software giant claims that there is a connection between the Renos family of malicious code and Win32/FakeSecSen. This because malware such as TrojanDownloader:Win32/Renos.Y, TrojanDownloader:Win32/Renos.AY, TrojanDownloader:Win32/Renos.EK will also download Win32/FakeSecSen on infected machines. In this context, another scenario for the delivery of Win32/FakeSecSen involves the rogue security software ending up on a machine already infected by malware.

## Microsoft Products, Logos and Brands

Rogue security solutions are designed to prey on unsuspecting users, but the damage they deliver is far greater than the money extorted. Products under the Win32/FakeSecSen umbrella come in a variety of "packages" featuring Microsoft's logos and brands, but also very similar to the company's products, including the Windows Security Center.

"This is no coincidence. FakeSecSen even goes as far as adding its own imitation Security Center applet to the control panel, usually called 'MS AV', which just launches the fake scanner. Some say imitation is the sincerest form of flattery, but for anti-malware providers like Microsoft, the trust and confidence of our customers is vital and we hate to see anyone taken in by this sort of thing," O'Dea added.

Imitation as far as rogue security solutions are concerned is designed to reproduce a familiar look and feel for the end users, and make the fake software pass for a [genuine product](#). At the end of September 2008, Microsoft, together with the Washington Attorney

General Office, started to hunt down makers and distributors of rogue antivirus software. The Redmond company is committed to pursuing legal actions against software makers which build rogue antivirus solutions and deploy scareware tactics.