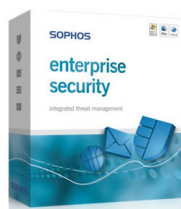


1 July 2008



Sophos - security solutions for businesses  
Sophos

By: George Craciun, Security News Editor

## [Amazon EC2 Spreads Malware](#)

### *Sophos warns about new threat*

Over the last couple of days, Sophos has detected a normal amount of spam messaging traffic. The spam messages informed you that you needed an "Important Windows Update", which is one of the oldest and best known tricks in the book, but in fact linked you to a malware spreading site. The intriguing thing is that the spam was not coming from a well known botnet, but from Amazon EC2 (short for Amazon Elastic Compute Cloud). After further study Sophos found out that in fact it was a spam campaign aimed at Amazon.com's EC2. No one has determined yet why EC2 is being targeted. One possibility is that by using a well known, trustworthy site, users will be fooled into getting infected. Another theory is that the spammers have infected a bunch of hosts with plenty of bandwidth to use. If this keeps up, it is possible that the whole cloud will lose its trusted status and join countless others in the DNSBL (short for DNS-based block list). In order to stay protected, you should disregard any message with the following subject lines: "Critical Microsoft Update, Critical Update Notification, Important Microsoft Update, Important Update Notification, Important Windows Update." Basically, anything stating that you need some sort of critical update. If you decide to open the spam you will notice that it informs you the Windows OS needs to be updated because it has a critical flaw. You have to update whenever it is convenient for you, but you must update if you want to be protected. A link is inserted in the message, cleverly disguised as a link towards "Microsoft Update". It even has instructions: "by clicking here and simply pressing "Open" or "Run" to begin the automatic update". Sophos warns not to do so as you will be infected with Mal/Encpk-AO.