Heuristic Scanning - Where to Next?
Author: Lucas - eBCVG Technical Writer
Published: Friday, 17 September 2004 10:42 GMT

One of the fundamental problems within heuristic scanners is the issue of positive and negative scanning. Over the last couple of years a number of scanners have appeared in the consumer market with heuristic scanning abilities only. While this scanning approach will be the scanning method of the future unfortunately these products have failed miserably.

Products such as Symantec and Mcafee have sucessfully integrated a heuristic scanner with their current signature based scanner and has fared well so far.

What is Heuristic

Heuristics looks at characteristics of a file, such as size or architecture, as well as behaviors of its code to determine the likelihood of an infection. Heuristics can sometimes find and stop many new viruses before they execute. Heuristics dont have a signatured based catalogue system, instead they look at hundreds of different behavours and indicators that a virus can use.

There are generally two types of Heuristic scanners, Generic and Static. Static Heuristics is similar to Signature based scanning however rather than scanning for individual viruses etc it scans for particular behavour patterns. This type of scanning can include DOS and Windows boot, executable and macro's. It can also be used to detect Worms. The heuristics run an analaysis of instructions for the files and determines whether these instructions is something a virus would do.

Macro viruses have somewhat declined due to heuristic detection methods built into Anti-Virus products and also heuristic options which are now included in Outlook, Word and Excel.

Heuristic Issues

The main problem with sole heuristic scanners is the inaccuracy of the scanning. The ideal situation is where your scanner provides either positive positive or negative negative scanning.

Positive Positive scanning is where it states you have an infected file and you actually do.

Negative Negative scanning is where it states the files are clean and they actually are.

At the present time however there is an alarmingly high number of scan engines which are giving positive negative and negative positive scans.

Positive Negative scanning is where it states you have an infected file where in fact you dont

Negative Positive of course is the opposite, your scanner states your files are ok when in fact theres an infection.

Obviously this could cause issues when your scanner is giving you this false sense of security, or alternatively forcing you to delete files when this isn't necessary. While that is an obvious downside to using a sole heurisitic scanner there are a number of positives.

- Unlike Signature based scanners which are re-active heuristic scanners have the ability to be pro-active. When a new virus enters the world it may infect numerous computers before there is a Signature update available. Antivirus companies require a copy of the file so they can examine it and create scan strings. With heuristic scanning the virus could be detected regardless of whether its a new baby or old. Of course it wont have available information about the file, it will just advise it has detected a file which 'could be a virus" You then have the option of deleting or ignoring.

- Heuristic scan engines are generally smaller in size and a lot quicker. Scan engines dont require huge databases of signature

quicker. Scan engines don't require huge databases of signature files to be able to detect a file. This in itself is an advantage.

Currently signature based scanning is the preferred method of scanning however this will change. Anti-virus companies have the current notion that because their scanner can detect 70,000 viruses this is excellent. What should determine an excellent scanner from an average one is not the ability to scan large numbers of viruses which have been out for a while but rather the ability to scan new viruses as they emerge. The company which masters this will have the AV industry at their feet.