

No Dogs Allowed!

Aside from discrimination against dogs, there's a story here about how antivirus can help to protect you from unknown threats.



Randy Abrams

If I walk up to a restaurant with a Catahoula Leopard Dog, the odds are that nobody in the restaurant has ever seen this breed

of dog before. So, why won't they let me in with an animal they have never seen before? The answer is heuristics. Heuristics use rules to solve problems. Perhaps you have never seen a Catahoula Leopard dog, but if you did you would recognize it as a dog. The animal looks like several other animals you have seen that are also dogs. You know it isn't a cat, or a bear. Now take a moment to try to describe a dog. Could someone mistake your description for a bear? Does your description fit all dogs?

There is a special type of heuristic that high quality antivirus, such as ESET's NOD32 use - generic signatures. Normal antivirus signatures detect one specific threat each. The bad guys constantly modify existing threats to break detection.

Generic signatures measure how different something is from something that we know is bad. Just as in your mind you will know that a Catahoula Leopard dog isn't different enough from any other dog to be anything but a dog, some bad programs are not different enough to be anything else. The swizzor trojan is an example of where generic signatures are essential. Virtually every time a user encounters the swizzor trojan it is a brand new modified sample. If we do not detect the threat before it is created then it is too late to prevent infection.

For the Swizzor Trojan, and other threats, we have been able to create generic signatures each able to detect thousands of these mutants before they are generated. If we had to use a unique signature for each sample swizzor would be all we had time to detect and it would be too late.

In some cases generic signatures can be used for exploit detection as well. When a vulnerability is found in software the methods used to exploit the vulnerability may differ, but they are often so similar that we know what we are facing without having seen the specific exploit before.

The ability to program antivirus to "think" like a person is crucial if we are to remain an effective industry. ESET started using heuristics in NOD32 back in 1998. Generic detection is just one of the methods that allow us to catch malicious software that we have never seen before.

If you wish to submit questions or comments to "Ask the Expert" please feel free to send them to askeset@eset.com.



Randy Abrams is Director of Technical Education for ESET

AskESET@eset.com

www.eset.com

610 West Ash Street, Suite 1900

San Diego, CA 92101 • 866.496-ESET

ESET paid for this space and is solely responsible for its content.