

## Safe Scoping

Application Brief 1016B

# Securing Your Scope & Network Against Threats

February 2009

### Summary

*Oscilloscopes that run Windows operating systems should be protected from malware just like any other PC. Users are strongly advised to use anti-virus software and to install OS patches. LeCroy is dedicated to ensuring that our products are shipped virus-free.*

Using a commonly available computer operating system such as Microsoft Windows on a LeCroy oscilloscope offers a multitude of advantages, such as the ability to link third party software into the scope operations and to connect a wide variety of hardware to the scope. The downside of using a common operating system is the threat of malware. LeCroy strongly encourages all users to minimize the risks that malware presents by using antivirus software on their oscilloscopes, and by keeping Windows updated by regularly installing OS patches.

Malware (including but not limited to viruses, Trojan horses, worms, bots, keyloggers and spyware) can infect a PC via many paths. Examples include websites, USB memory sticks, emails and your local network. Simply connecting an unprotected PC (or an unprotected Windows-based oscilloscope) to an 'infected' network is enough to infect it... within seconds.

There are more than a million known malware threats targeting personal computers, a number which grows every day. Operating system developers devote much time and energy to patching security breaches, and developers of malware are always looking for new weaknesses to exploit. Updating the operating system and applying updated virus definitions greatly reduces the probability of infection, but can never completely eliminate it.

LeCroy Corporation is dedicated to ensuring that our oscilloscopes are free of any malware when manufactured and calibrated, and we have taken aggressive steps to make sure that all oscilloscopes leave our manufacturing facility virus free:

- 1) Scopes are manufactured on an isolated, secure virus free network with no internet access.
- 2) Scopes are virus scanned and updated with all critical operating system updates before shipping, and a DSO security certificate is included.

3) Scopes running an MS Windows OS are shipped with an evaluation version of the award-winning NOD32 antivirus software from the company ESET. (See text box below)

4) All “demo” oscilloscopes carried by sales engineers have NOD32 installed.

These steps help to guarantee that any oscilloscope will be virus-free when delivered. From that point on it is the user's responsibility to insure the security of the scope.

Before connecting the scope to your company's network you should consult with your Information Systems (IS) department to find out what security policies apply to the scope. Remember that although the oscilloscope behaves as an instrument, to the network it appears to be a computer. Follow your company security policies with regards to security policies and virus protection.

It is also important to update both the virus definitions and operating system regularly. LeCroy recommends checking both virus definitions and operating system updates on a weekly basis. NOD32 automatically updates its virus definitions when connected to the internet, so keeping the definitions up to date is very simple. Be sure to always update the OS and anti-virus definitions if advised to do so by your company's system administrator or IS department.

It is important that you periodically run a virus scan on any scope that is connected to a network. Configure your anti-virus to periodically scan the system automatically. (Choose a time when the

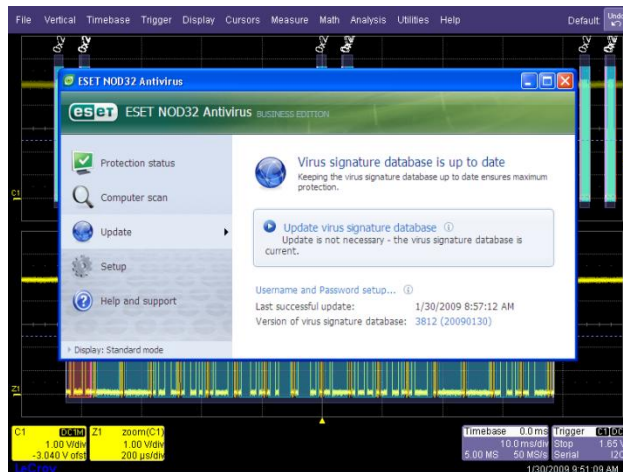


Figure 1: A typical antivirus software update page where weekly updates of virus definitions helps protect your scope

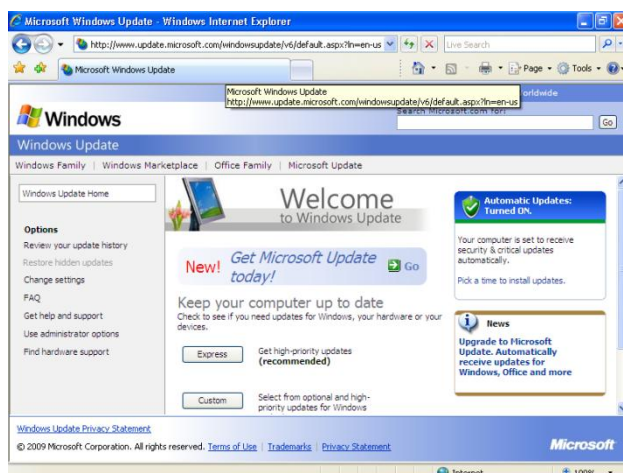


Figure 2: A typical operating system update page where weekly checks for operating system updates helps reduce vulnerability to viruses

oscilloscope is not in use.) Remember, the time you spend attending to security issues is minimal compared to the cost of having to clean up a system infected with a virus!

***NOD32: An Anti-Virus package well-suited to the needs of a Windows-based scope***  
LeCroy selected the NOD32 package from ESET for use on LeCroy-owned oscilloscopes after careful research and consideration. NOD32 has a very high detection rate, and includes real-time protection against both known and potential security threats. It scans quickly, and has a small footprint, which helps to minimize the boot time of the oscilloscope. ESET and the NOD32 package are well-known and highly respected among IT and security professionals, and is well-suited for use on your LeCroy oscilloscope.