Spyware Misidentification

Anti-spyware companies want to portray their software as a means to eliminate unauthorized or illegal monitoring of Internet activities. Unfortunately, these software packages are only as good as their research.

Some Anti-spyware programs fail to detect malicious code, and almost as damaging, they often misidentify important enterprise level monitoring and diagnostic software packages. These Anti-spyware programs are frequently inaccurately updated, and as a result, often misidentify important software used for corporate security and regulatory compliance programs.

Misidentification of monitoring software and other network utilities is unfortunate since many of these packages are designed to allow operation without end-user notification or permission. This silent operation allows enterprise security officers, Government Inspectors General and officials with Regulatory Compliance responsibilities to undertake investigations that pursue inappropriate and often illegal Internet usage by employees, such as leaking of trade secrets or using corporate computers to traffic in child pornography. Once Anti-spyware reveals the use of monitoring software to an end-user under surveillance, an investigation is compromised.

Conversely, when Anti-spyware notifies the user that legitimate enterprise-level monitoring software is active when it is not, network administrators waste valuable time and resources proving a negative to management. One such example is ***Spyware Doctor*** by PCTools. Unfortunately for some of the users of this program, Spyware Doctor incorrectly identifies Pearl Echo as being installed on the enterprise network and workstations when it is not.

In several instances, the Pearl Software technical support group has verified that ***Spyware Doctor*** incorrectly identifies a commonly registered active-x component as a Pearl Echo installation. In all instances, the enterprise network administrator and Pearl Software's technical support team have been able to determine with complete certainty that no copies of Pearl Software's products are present in the enterprises' networks. This is a result of Spyware programs treating all third party network monitoring code as malicious until proven otherwise.

The best means to avoid this type of problem is to use Internet filtering technology that prevents the downloading of Spyware **at its source**. Programs such as our Website•Echo™ and Echo•Filters™ products reinforce an enterprise's Acceptable Use Policies by blocking network users from communicating with the origin sites for Spyware. This is a far more effective method of control than an imperfect research effort which hopes to properly identify all permutations of malicious code available on the Internet.

Contact: If you can document an incident where Pearl Echo is being misidentified by an Anti-spyware product, Pearl Software will provide you with a one-time 10% discount off of your first purchase of any of our products. To speak with Pearl Software concerning use of our products to assist you in your efforts to stem the incursion of spyware and malicious code in your network, please contact us at 800-732-7596 Opt 4.