Fighting Stealth Software

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In the preceding two newsletters, I’ve been looking at stealth software – “privacy protecting” programs that hide from system administrators.

If your security policies do not already include a clause to forbid installation of unauthorized software on corporate computers, include one; here are two examples from my favorite policy source, Charles Cresson Wood’s Information Security Policies Made Easy, version 9 (see <http://www.baselinesoft.com> for details). These policies (used with permission) are in section 8.03, “Protection against malicious software.” By the way, I’m looking forward to version 10 of the ISPME.

“19. User Installation Of Software

Policy: Users must not install software on their personal computers, network servers, or other machines without receiving advance authorization to do so from a local information security coordinator.

Commentary: Internet access has made many new programs available to the general user population. If users install such programs, or permit an installation process performed by an automatic installation routine, viruses could be propagated, system crashes initiated, and other problems created. This policy explicitly prohibiting users from installing any software unless previously approved by the information security coordinator. New personal computer software packages are available that will prevent personal computer users from running any software besides the software specifically approved by management. By implication, this policy prohibits the use of Java and ActiveX applets, but some users may not make the connection.”

“23. Downloading Software Using The Internet

Policy: End users must not download software from the Internet under any circumstances.

Commentary: This policy brings some order to what is often a very chaotic software update environment on end-user personal computers and workstations. End users in many organizations are taking the software update process into their own hands, and in the process they often create problems for the Help Desk and others working in the information systems area. This policy assumes that the organization has a process in place to distribute software and related upgrades. The policy works much better if its implementation includes workstation access control packages that prevent end users from updating software themselves. Also useful in the implementation of this policy would be an automated software license management package, that could periodically take an automated census to determine what software is installed on each machine. This policy assumes that all end-user machines are connected to a local area network, a wide area network, an intranet or some other network through which software updates may be pushed. The delay associated with testing software before it is installed across an organization is often desirable because this delay will permit serious bugs to be reported to public forums. Those performing
software testing can install patched versions that have corrected these problems."

As for specific technical measures to fight this kind of stealth software, I suggest several approaches for network managers faced with the possibility that their users are installing this product or any similar tools for evading corporate Internet-access policy:

* Warn your users that installing software that uses stealth mode is _prima facie_ evidence of malicious intent to violate corporate policies and will be viewed as a serious breach of ethics.

* If you find a stealth-mode program on a system, contact your anti-virus and anti-pest vendors and ask that it and any other product with “stealth” capability be added to the list of potentially harmful software so it can be located and expunged from user systems using anti-malware scans.

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see [http://www3.norwich.edu/msia](http://www3.norwich.edu/msia) for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at [mailto:mkabay@norwich.edu](mailto:mkabay@norwich.edu); Web site at [http://www.mekabay.com/index.htm](http://www.mekabay.com/index.htm).

Copyright © 2005 M. E. Kabay. All rights reserved.

Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.