Protecting Public Workstations

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

In my last column, I looked at how the Kinko’s public Internet workstations were compromised by Juju Jiang using a keystroke logger program left running on those systems. I referred to an article about that criminal’s activities by Lisa Napoli. What particularly interested me was Napoli’s statement, “Making the public aware of the vulnerability of shared Internet access terminals is one thing. Remedying this vulnerability is quite another.” She followed this surprising assertion with a quotation from an FBI agent who said, “I don’t know how you manage the risk . . .”

Well, university network administrators do.

In universities and other schools around the world, students have access to computers linked to the campus networks; how are these systems protected against tampering such as installation of unauthorized software – including keyloggers? Well, in the first place, systems with access controls are configured to preclude access with administrator privileges. But everyone knows that user ID / password combinations are a dreadfully weak method for preventing unauthorized access. Passwords can be compromised by shoulder-surfing, because they’re written down, or using brute-force cracking of poorly-secured one-way encrypted password files. But there is a simple method for reducing potential damage: clone the workstations disks every night. That is, the disk of each PC on the network is rewritten with a fresh, uncontaminated copy of the entire contents of the drive.

There are several products available which can automatically deploy the authorized disk image to hundreds or thousands of workstations provided you have adequate server speeds and network bandwidth. There’s a helpful review of several of these tools written by Cornell W. Robinson III in _Network Computing_ which I’ve referenced below; I have provided the specific URLs to help readers avoid having to search through the general sites given in that article. In addition, the references below point to the Frisbee project of the School of Computing at University of Utah. I also found a summary on the Microsoft site called “Automating and Customizing Installations: Choosing a Disk-Imaging Program” that provides a checklist for Windows Server 2003 and Windows XP Professional users.

Any of the products listed would reduce (not eliminate) the window of exposure on public terminals. So as users, all of us should be careful about what we reveal on such terminals. And don’t use the same password on multiple commercial sites on the Internet – you don’t want compromise of one of those passwords to open up every account you use.

Finally, readers should note that the imaging software supports not only preservation of data integrity and trustworthiness but also provides a speedy mechanism for restoring functionality of a damaged system: restore the disk image of the operating-system drive and you don’t have to reinstall the software. These tools support the principle of a known-good copy of the operating system: take an image immediately after installing the operating system and before using – and potentially damaging – it. Then before installing new software (applications, drivers. . . .) you
can restore the original image, do your installation, and take a new image (properly documented) for the next time you need to start from a clean environment.

***

For further reading:

altiris Deployment solution
< http://www.altiris.com/products/deploymentsol/>


< http://www.nytimes.com/2003/08/07/technology/circuits/07kink.html > [restricted access]; see also
< http://www.crime-research.org/eng/news/2003/08/Mess0702.html > and
< http://www.iht.com/articles/105567.html >

PowerQuest DeploymentCenter Library 2.0
< http://www.powerquest.com/deploycenterlibrary/> 


Symantec Ghost Corporate Edition 7.5

***

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.