

For Immediate Release:

## **Technology Pathways releases ProDiscover Incident Response V3.0 with new capabilities to find Trojans and kernel mode rootkits**

***Computer forensic software can now quickly find suspect processes and files being cloaked by Trojans. Unix file system support added to ProDiscover family of products.***

Coronado, Ca, Feb 20, 2004, Technology Pathways, LLC

Technology Pathways today announces a major new release of ProDiscover™, its leading edge computer forensics software. With this new release, ProDiscover Incident Response can quickly identify if there are any processes or files on a system that are being "cloaked" by Trojans or kernel mode rootkits. This gives the incident response teams a new tool to determine if a system has been compromised after an intrusion.

Trojans and kernel mode rootkits can cloak running processes from system admin tools such as the Task Manager by altering the system calls used by the Task Manager to identify the processes running on a system. ProDiscover Incident Response now uses new techniques to identify processes that the Task Manager cannot see.

Equally important, Trojans and kernel mode rootkits can also cloak files from tools such as Explorer. ProDiscover Incident Response accesses the disk at the lowest possible level to find all files and compares this list to the files that can be seen by the suspect system to expose any cloaked files.

"This latest release is an important breakthrough in how incident response will be done in the future." stated Christopher L. T. Brown, CTO for Technology Pathways. "Unlike other system integrity approaches, we create baselines from the sector level to accurately attest to system integrity. Now system administrators have a tool to allow them to really see what is on a suspect system."

Additionally, there are several other new features included in ProDiscover Incident Response Release 3.0, including support for the UNIX file system. Now, ProDiscover users can forensically examine live UNIX systems operating within their network.

The ProDiscover family of computer forensic tools prices start at \$495. ProDiscover Incident Response is priced at \$1495 which includes support for both the Windows and UNIX file systems. ProDiscover Incident Response 3.0 will be demonstrated for the

first time at the RSA Conference 2004 at the Moscone Center in San Francisco on February 23-27.

Technology Pathways, LLC is a leading edge provider of computer and network security tools and services for the Corporate IT, government, education, and legal communities. The ProDiscover® family of products provides affordable software solutions in the areas of computer forensics, incident response, system auditing, internal investigations and electronic discovery. Our CISSP certified consultants provide security, forensic and discovery services to corporations and law firms. Technology Pathways products and services are utilized nationally by major corporations, law enforcement, and government agencies.

For more information please contact:  
Judy Smith, JPR Communications  
(818) 386-0403

(Editor's note: If you would like to arrange for a personal demo of ProDiscover Release 3.0 at the RSA Conference, please contact Judy Smith at JPR Communications.)