

FOR IMMEDIATE RELEASE

Contact:

Nataly Koukoushkina
Passware Inc.
+1 (650) 472-3716 ext. 101
media@lostpassword.com

Passware Warns: Microsoft Windows Sleep Feature Poses Security Risk

Passware enhances Passware Kit software for instant decryption of TrueCrypt and BitLocker by analyzing a hibernation file

Mountain View, Calif. (December 9, 2010) – [Passware, Inc.](#), a provider of password recovery, decryption, and electronic evidence discovery software for corporations, law enforcement organizations, government agencies and private investigators, warns that a sleep feature in Windows significantly reduces security of full disk encryption. Passware enhances Passware Kit, its leading software for computer forensics, for accessing the data stored automatically when a computer is ‘put to sleep’ and subsequent instant decryption of drives encrypted with TrueCrypt or BitLocker.

For computer forensics, Passware offers [Passware Kit Forensic 10.3](#) to decrypt hard disks encrypted with BitLocker or TrueCrypt in a matter of minutes if the target computer is running. The latest enhancements to Passware Kit make instant decryption for powered-off computers possible by analyzing a single hibernation file. Created automatically when a system enters hibernation, this file (hiberfil.sys) often contains data that may breach computer security. If a computer with a mounted TrueCrypt or BitLocker To Go hard disk has hibernated at least once, Passware Kit will instantly decrypt the hard disk even if the computer is no longer running.

“The complexity of IT security is not limited to anti-malware, anti-virus, phishing and other actions, but extends to behaviors that exploit little known flaws in operating systems,” said Dmitry Sumin, president of Passware, Inc. “As a pioneer in hard disk decryption, we are the first company to turn this hibernation vulnerability into a forensic feature. Coupled with our understanding of the need for strategic IT decisions that protect against IT security risks, including the ability to capitalize on technology flaws, we believe Passware Kit will continue as the leading software used for encrypted evidence discovery in computer forensics.”

Cybercrime Plays a Role in Corporate IT Security

Understanding what cybercrime is, how to defend against it, and means for conducting successful computer forensics are critical for companies that want to operate effectively in the 21st century. Based on law enforcement agency reports that cybercrime, along with terrorism, drug crime, and fraud, pose the world’s greatest threats to personal and corporate IT security, there’s a growing need for effective computer forensics among corporate IT managers.

Andy Malone, CEO and senior technology of quality training (UK) Ltd. & Dive Deeper Events EMEA recently presented “Cybercrime – Clear and Present Danger” session (TechEd Europe, November 2010, Berlin). In this session he included a step-by-step demonstration of BitLocker

decryption process performed with Passware Kit Forensic while discussing latest tools, tactics, and trends of the cybercrime trade. Malone notes, “This latest version of Passware Kit is the absolute definitive tool for investigators. With the ability to extract encryption keys from a Hiberfil.sys file, there really is nowhere for the bad guy to run.”

Pricing, Availability and Webinar Demonstrations of Passware Technology

Passware Kit 10.3 is available now from [Passware](#) and a network of resellers worldwide. The manufacturer's suggested price for Forensic edition starts at \$795 with one year of free updates. To view Malone's demonstration of Passware visit: <http://on.fb.me/pw-rec-bl> or [attend a free webinar](#) to see additional demonstrations of the power of Passware Kit. Additional product information and screen shots are available here: <http://www.lostpassword.com/kit-forensic.htm>.

About Passware Inc.

Founded in 1998, Passware Inc. is the worldwide leading maker of password recovery, decryption, and electronic evidence discovery software. Law enforcement and government agencies, institutions, corporations and private investigators, help desk personnel, and thousands of private consumers rely on Passware software products to ensure data availability in the event of lost passwords. Passware [customers](#) include many Fortune 100 companies and various US federal and state agencies, such as IRS, US Army, US Department of Defense (DOD), US Department of Justice, US Department of Homeland Security, US Department of Transportation, US Postal Service, US Secret Service, US Senate, and US Supreme Court. More information about Passware, Inc. is available at <http://www.lostpassword.com/>.

Passware is a privately held corporation with headquarters in Mountain View, Calif. and a software development and engineering office in Moscow, Russia.

###