



Press Release

New AutoRun Disable Tool Protects Computers against USB-spreading Malware

Free tool released by Endpoint Protector prevents AutoRun-based malware spread through USB ports and other connections from infecting computers and networks

Boise, ID, USA and Bucharest, Romania, November 17th, 2010. Endpoint Protector launched the free AutoRun Disable tool, a solution designed to prevent malware infections spread through USB ports and other computer interfaces and which require the malicious software to start and run automatically once connected to the infected unit. AutoRun Disable by Endpoint Protector was designed to stop worms such as Conficker/Stuxnet, which take advantage of unsecured USB ports and lack of portable device control to spread out and infect as many computers as possible.

What AutoRun Disable by Endpoint Protector does is allow computer users to disable the possibly dangerous AutoRun feature of Windows (XP, Vista, 7). The major benefit is that it does not disable the feature for all devices, as the tool takes action selectively based on device types (USB and other removable devices, CD/DVD, internal or network drives) or specific drive letters. For example, a user can deny permission to the AutoRun function of USB portable devices and allow it for the CD/DVD drive.

“Conficker, Stuxnet, Downadup, no matter how you call the latest threats, the truth is they are all extremely easy to prevent. Device control and endpoint security solutions can prevent such threats from making a connection to a computer they target. AutoRun Disable by Endpoint Protector makes it even easier to protect individual computers and networks from such malware, as it is free, easy to install and use and effective. It successfully keeps malware threats away from the protected unit, while allowing needed drives to access the AutoRun feature and not impair the users habitual actions in any way”, explained Roman Foeckl, Endpoint Protector/CoSoSys CEO.

Even before the official release of AutoRun Disable by Endpoint Protector, the tool has been made available to potential users along with a publicly released easy five-step advisory helping them protect computers against the growing Stuxnet/Conficker:

<http://www.endpoint-security.info/2010/09/28/conficker-stuxnet-cososys-advisory/>

To download AutoRun Disable by Endpoint Protector, please visit:

http://download.cnet.com/AutoRun-Disable-by-Endpoint-Protector/3000-2239_4-75300368.html



About CoSoSys

CoSoSys is specialized in network endpoint security for Windows and Mac and development of software for portable storage device enhancement. The application portfolio includes functions from password security, data synchronization and network security. CoSoSys distributes its products globally through the world's leading hardware manufacturers, software Distributors, Resellers and directly to users at <http://www.CoSoSys.com> and <http://www.EndpointProtector.com>. CoSoSys enjoys a continuously growing installation base of users worldwide. The company has offices in Germany, the United States and Romania.

Images and additional materials:

http://www.endpointprotector.com/en/index.php/products/free_data_security_tools
<http://www.cososys.com/images.html>
http://www.cososys.com/press_room.html

Press Contacts:

Mirror Communications

Alina Popescu

Phone: +40 741 073753

E-mail: alina@mirror-communications.com

CoSoSys Ltd.

Anca Goron

Phone: +40 264 593 110 Ext. 113

E-mail: anca.goron@cososys.com