

February 7, 2014 Release # 252 -- Begin Transmission --



Autorun worms are malicious programs that take advantage of the Windows AutoRun feature. They execute automatically when the device on which they are stored is plugged into a computer.





Autorun worms are commonly distributed on USB drives, automatically infecting computers as soon as the USB is plugged in. AutoPlay is a similar technology to AutoRun. It is initiated on removable media, prompting users to choose to listen to music with the default media player, or to open the disk in Windows Explorer. Attackers have similarly exploited AutoPlay, most famously via the Conficker worm.

Verdensetered being systems, Lecheneuer operating systems, Discible it!! Discible it!! Discible it!!

-- End of Transmission --

Information Security: It's a Shared Responsibility

REFERENCE(S): Sophos Ltd. (2012). *Threatsaurus: The A-Z of computer and data security threats.* Boston, USA | Oxford, UK

INTERNAL USE ONLY: For circulation within the PJ Lhuillier Group of Companies only.