

Apple's iPod a useful tool for criminals

July 3 2005

By K.I. MARSHALL WASHINGTON, July 1 (UPI) -- Apple's iPod and other portable digital media devices have become as useful to criminals as they are to the general public, computer-security experts have discovered.

"Similar to the way the personal computer became common in the home in the '80s and '90s, the iPod is becoming common today," Dr. Marcus Rogers, a cybercrime expert at Purdue University's Center for Education and Research in Information and Security, in West Lafayette, Ind., wrote in a recent report, "iPod Forensics."

This growing popularity, Rogers continued, "has allowed a criminal element to find 'alternative' uses for a seemingly harmless device, and the Apple iPod is finding its way into the criminal's bag of tricks."

The most apparent of these uses is corporate or personal information theft -- although the threat of information theft has existed since the advent of removal media such as the floppy disk.

"This is nothing new," Winn Schwartau, founder of Interpact Inc., in Seminole, Fla., an information-security services company. "If you go back 15 years the threat was floppies, then it was CDs, then Dipstick," Schwartau told United Press International. "The premise is identical, the opportunity is the same, and the crime is the same."

Interpact offers programs designed to educate corporate employees on proper security behavior, including use of removable storage.

The iPod's large capacity and ability to connect easily to a computer and transfer data rapidly via a Universal Serial Bus -- known commonly as a USB -- or FireWire port make it potentially more useful in information theft, said Abe Usher, founder of Sharp Ideas, an IT consulting firm in Centreville, Va.

"The iPod has wide adoption, is overlooked by security, and has large storage space," Usher told UPI in an e-mail. "CDs and floppy disks are not 'as dangerous' because they lack the space that an iPod has, and carrying a stack of CD-ROMs around is more conspicuous than carrying an iPod."

Usher recently sought to demonstrate the iPod's potential for corporate information theft by writing a program for the device that automatically copies all the documents from a computer as soon as the device is connected. Usher said he was able to copy all of the documents in his computer in 65 seconds. Last year, Gartner Inc., in Stamford, Conn., a technology-research firm, released "How to Tackle the Threat from Portable Storage Devices," a report that recognized the removable-digital-device threat to corporate security and suggested steps companies could take to reduce their vulnerability, including restricting or prohibiting portable media devices.

Most companies do not take the necessary precautions to limit access of portable devices to their computers. In a recent poll conducted by Centennial Software, a software security company in Swindon, United Kingdom, 87 percent of companies polled reported they had taken no steps to prevent unauthorized use of removable media devices in the workplace. Also, 51 percent of respondents said they were aware of the security threat from those devices.

"What we are looking at is 25 years of corporate apathy," Schwartau said. "We have too many executives in too many companies who think

that it will never happen to them and that it is too expensive."

One possible way of limiting access to iPods and other devices that use USB ports is to disable them. The problem is most new computing peripheral devices, such as printers, scanners, keyboards and mice, use USBs and could not function without them. Another option is to employ software that limits specific uses for USB ports. Several such products allow network administrators to restrict access to CD drives, floppy drives, wireless connections and USBs.

All portable digital media devices must be plugged in physically to a computer and Schwartau noted the human element of information theft is overlooked in the rush to blame technology.

"This is a people problem rather than a technology problem," he said. "What people require is education. If you look at Secret Service Records, they say that 80 percent of cybercrime cases involve an internal element, whether intentional or unintentional."

Schwartau said that as soon as employees are educated about proper security procedures, companies can differentiate between intentional and unintentional security breaches and focus their efforts on malicious attackers.

Along with their use in information theft, iPods and other portable media devices can be used to spread viruses or child pornography, or maintain records for criminal organizations, Rogers said. Despite the dangers, the technology has a useful potential in criminal investigations, but only if investigators know what to look for.

"The technology is neutral," Rogers told UPI in an e-mail. "Investigators and information security professionals need to be aware of the devices and their capabilities. Most investigators know to look for CDs and

floppies, but not to search music devices."

Rogers said whenever a device is recognized, it can become a wealth of information for investigators."The ability to trace the device not only to a system, but to an account and user on that system is a big plus for investigators," he said.

Copyright 2005 by United Press International

Citation: Apple's iPod a useful tool for criminals (2005, July 3) retrieved 9 April 2024 from <https://phys.org/news/2005-07-apple-ipod-tool-criminals.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--