

WSLabs, Malicious Web site / Malicious Code: Audi&#...

Article URL

www.securityhome.eu/mailings/mailling.php?mid=272

Author

SecurityHome.eu

Published: 24 May 2007

Websense® Security Labs(TM) has discovered that the official site of Audi in Taiwan has been compromised.

The site www.audi.com.tw contains an iframe that leads to another page located on the domain www.misofthelp.com. This site is obfuscated, using the 7-bit US-ASCII bypass technique. Once this obfuscation technique is bypassed, the script is further obfuscated. The resulting decoded page reveals a Visual Basic Script that contains an ADOdb (database extraction library) exploit. The exploit within the page downloads and executes a file called update.exe (Trojan PWS).

For additional details and information on how to detect and prevent this type of attack:

<http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=776>