

**INTERNET CRIME COMPLAINT CENTER (IC3)
MAY 8, 2012**

**MALWARE INSTALLED ON TRAVELERS' LAPTOPS THROUGH SOFTWARE UPDATES ON HOTEL
INTERNET CONNECTIONS**

Recent analysis from the FBI and other government agencies demonstrates that malicious actors are targeting travelers abroad through pop-up windows while establishing an Internet connection in their hotel rooms.

Recently, there have been instances of travelers' laptops being infected with malicious software while using hotel Internet connections. In these instances, the traveler was attempting to setup the hotel room Internet connection and was presented with a pop-up window notifying the user to update a widely-used software product. If the user clicked to accept and install the update, malicious software was installed on the laptop. The pop-up window appeared to be offering a routine update to a legitimate software product for which updates are frequently available.

The FBI recommends that all government, private industry, and academic personnel who travel abroad take extra caution before updating software products on their hotel Internet connection. Checking the author or digital certificate of any prompted update to see if it corresponds to the software vendor may reveal an attempted attack. The FBI also recommends that travelers perform software updates on laptops immediately before traveling, and that they download software updates directly from the software vendor's Web site if updates are necessary while abroad.

Anyone who believes they have been a target of this type of attack should immediately contact their local FBI office, and promptly report it to the IC3's website at www.IC3.gov. The IC3's complaint database links complaints together to refer them to the appropriate law enforcement agency for case consideration. The complaint information is also used to identify emerging trends and patterns.

Anthony L. Neumann

Information Technology Bureau Manager
City of Oshkosh