Written by **Steven J. DuBord** on August 4, 2009

Secret Service Checks Las Vegas ATMs

PC World reported on August 3 that the U.S. Secret Service is investigating some ATM machines in Las Vegas that are subtracting money from a user's account without dispensing any cash. Ironically, the problem was first reported by one of the presenters from a Defcon hacker conference being held in Vegas.

When the presenter, Chris Paget, tried to withdraw $200 from his account via an ATM at his hotel, the machine "whirred and chugged," as he described it, "but no money came out." He later verified that his account was debited and that he wasn't the only one. Paget spoke with a man who had tried to withdraw $1,000 and a woman who had attempted $400, both unsuccessfully. At least six people had the same experience at various ATMs throughout the hotel.

Paget runs a hardware security consulting firm and has expertise in credit-card security. He said the ATMs may have been infected with malicious software (malware) that was telling the machines to withhold the cash. The money could then be picked up later by someone who was in on the scam, but it's too early to know for sure that the problem wasn't simply a malfunction. Both the Secret Service and the Las Vegas Metropolitan Police Department are investigating the matter.

If it turns out that the ATMs were hacked, it wouldn't be the first criminal incident involving cash machines and Defcon. Earlier in the week, conference attendees spotted a bogus ATM in the lobby of another hotel. Shining a light on the machine's screen enabled them to see a PC inside. Law-enforcement officials came and removed the fake ATM.

In another twist of irony, Barnaby Jack, a researcher with Juniper Networks, was supposed to speak at the Defcon conference about a vulnerability in a new line of ATMs. But when the unnamed ATM vendor threatened legal action, Juniper Networks canceled the talk.

According to *PC World*, there are multiple ways an ATM can be compromised: "One scam is to attach a device to the ATM known as a skimmer that can record details stored on a card's magnetic stripe. A person's PIN (Personal Identification Number) can be captured with an overlay on the keypad or a video camera. Then, the card can be cloned." Another method involves placing malware in the ATM that can record information from the cards used in that machine. Earlier this year, such malware was discovered that "came from a financial institution that had been affected in Eastern Europe."

One of the tag lines Las Vegas has used to popularize its attractions goes something like: "Whatever happens in Vegas, stays in Vegas." This apparently no longer applies to the personal financial information of those who use hacked ATMs in Las Vegas. No matter where a person uses an ATM, caution is required. Our increasingly cashless society offers such a great potential for profit that

hackers are ever more willing to bet that they won’t get caught.