Aplura, LLC
4036 Wildwood Way
Ellicott City, MD 21042
301-523-2110 (w)
410-864-8386 (f)

Focused Information Security
www.aplura.com

ATM Skimmers

Essay By: Sean Wilkerson

September 22, 2009

ATM skimmers have been around for years with over a Billion dollars in recorded-losses attributed to them; however, many people are still not familiar.

An ATM skimmer is an "add-on" device which an attacker installs onto an existing ATM to steal information from its users. It typically comes in two parts:

1. The card-reader which gathers the info from the magnetic stripe and front of the card
2. A camera which collects the keystrokes made while entering a PIN.

Traditionally these devices stored the information internally requiring the villain to come back later and retrieve the data; however, attackers recently leverage wi-fi or cell-phone technology which allows them to remotely collect the information and they do not need to go back to the "scene."

ATM Skimming is a big problem outside of the United States.

When I traveled to Eastern Europe for work in 2006, I was told to not trust a single ATM in the country (including the one in the lobby of the fancy hotel) except for the ones in the US government offices.

This video from Brazil came out a week ago and demonstrates how quickly an attacker can appear to be as a customer at an ATM while he installs a skimming device. Since the entire footage is seen from a surveillance video, you also get to watch the man's subsequent arrest.

ATM skimmers in the US are a growing threat as well and increasingly difficult to spot. Watch this short news clip of a skimming device found in central PA earlier this year.

Attackers who use ATM skimmers are very creative with how they hide their cameras and devices, which makes it challenging to detect them. Therefore you cannot rely on observation skills alone, to protect you.

Sometimes the bad guys don't bother with "hacking" an existing machine and simply install their own phony one, such as the one placed at "Defcon", a well-known annual Hacking convention, last month. Even at a hacking convention where suspicions run high, this ATM was able to trick many attendees into inserting their card and PIN.

Risk Perspective

ATM-usage is a convenience and as such there are trade-offs. Mitigating steps can be taken to help reduce the risk of financial and identity loss.

First, when using an ATM be aware of your situation. If something looks suspicious with a machine, move on to another. Several of this essay's links provide advice on how to spot modified ATMs and more detailed guides can be found on the Internet to offer further explanation. You must consider that technology continually improves both for the good guys and the bad. Skimmers can be difficult to visually detect and will become more so as time goes on; therefore you cannot rely only on your "wits" to keep your money and credit safe.

Always monitor your account transactions and report anything suspicious. Consider signing up for fraud-protection through the credit-reporting agencies. As a consumer, you can do this yourself by contacting one of the credit-reporting agencies directly and requesting a "Fraud Alert" be placed on your account. This takes a little more manual effort from the consumer, but there is no cost.

Finally, you can mitigate the impact of a compromised account by not using an ATM card tied directly to your "main checking" account. Consider an alternate checking account and maintain a balance to support your ATM-withdraw needs. If this alternate-account were to become compromised (via ATM skimming or otherwise) your primary expenses (rent, mortgage, car, insurance, etc.) would not be impacted at all.