

Criminals Hide Payment-Card Skimmers Inside Gas Station Pumps

Wave of recent bank-card skimming incidents demonstrate how sophisticated the scam has become

Feb 22, 2010 | 05:20 PM

By Kelly Jackson Higgins

DarkReading

Criminals hid bank card-skimming devices inside gas pumps -- in at least one case, even completely replacing the front panel of a pump -- in a recent wave of attacks that demonstrate a more sophisticated, insidious method of stealing money from unsuspecting victims filling up their gas tanks.

Some 180 gas stations in Utah, from Salt Lake City to Provo, were reportedly found with these skimming devices [sitting inside the gas pumps](#). The scam was first discovered when a California bank's fraud department discovered that multiple bank card victims reporting problems had all used the same gas pump at a 7-Eleven store in Utah.

Card skimming has been on the rise during the past year, with most attackers rigging or replacing merchant card readers with their own sniffer devices or ATM machines. The devices typically include a scanner, transmitter, camera, and, most recently, Bluetooth- or wireless-enabled links that shoot the stolen data back to the bad guys.

A similar attack occurred with a rigged ATM machine last year in Las Vegas during the Defcon hacker show: [Security researcher Chris Paget lost \\$200 to an ATM machine](#) in the Rio All-Suite Hotel & Casino that appeared to be operating normally, but failed to spit out cash. The U.S. Secret Service was investigating the incident, and it was unclear whether the machine was outfitted internally with a skimming device or had been tampered with for someone to grab the cash withdrawals at a later time.

Bruce Schneier, CTO for BT Counterpane and author of the Schneier on Security blog, says attackers in Europe are also moving skimming devices inside gas pumps as a way to avoid detection. He says the perpetrators could be insiders, but it's unclear. "The moral is that they are getting better and better at this," Schneier says.

Organized criminal gangs might be behind some of these attacks, he adds "Obviously, they are well-funded," Schneier says.

Police say data skimmed from the 7-Eleven store in Sandy, Utah, was used to steal more than \$11,000 from ATMs in California. Authorities estimate that victims lose millions of dollars a year to these types of attacks at gas stations nationwide.

Sgt. Troy Arnold from the Sandy police department told a local news outlets that the device in the 7-Eleven gas pump was the size of a cellular phone SIM card and was affixed to the card reader inside the pump. "It's a small device -- Bluetooth, the size of a SIM card -- that is attached to the actual credit card reader. And as we are placing our credit cards or debit cards into these gas pumps ... it's not collecting, but it's just transmitting the account information, the credit card number, to a different device that's within the range of the Bluetooth technology," Arnold [told a local Fox affiliate](#).

The device was removed in late January, and officials think it had been in place for about two months.

Bluetooth-enabled sniffers and wireless technology let the criminals gather data remotely rather than have to physically retrieve their contraband devices, the officials noted.

Back in December, a similar spree occurred in the Sacramento, Calif., area, where gas pumps at an AM/PM convenience store were outfitted with card skimmers, transmitters, and small cameras that siphon victims' debit card data. That information was then used to create a clone card, which the criminal uses at an ATM machine to withdraw money from the victim's account, according to a [published report](#).

"The consumer can't be expected to notice these things," BT Counterpane's Schneier says. And even if gas pumps are secured with tamper-proof seals of some sort, "no one is going to look for those," he says.