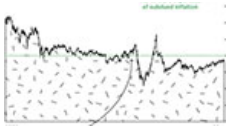

[Rule of 20: Is the Stock Market Fairly Valued?]

- **Videos**

[Does Alibaba Risk Getting Too Big in Buying Spree?]

[Does Beats Fill a Streaming Music Need for Apple?]

[Johnnie Walker Quenches China's Thirst for Luxury]

[Hang Ten: Strapless Kite Surfers Take to the Seas]

Data

Hackers Devise Wireless Methods for Stealing ATM Users' PINs

By Jordan Robertson May 08, 2014

Auburn Police Dept.

Pilfering the personal identification numbers of financial accounts, a potential jackpot for hackers, is tougher to pull off thanks to data encryption and other security technologies. Yet the arms race continues: Hackers are devising more creative methods to intercept PINs at ATMs, the clearest path to instant cash. “It just blows you away how sophisticated these folks are in thinking this stuff up,” says Bryan Sartin, director of the team at Verizon Communications (VZ) that investigates data breaches.

Schemes to steal PINs from ATMs and similar machines now include Hollywood-style corporate espionage, Sartin says. Crooks have long fitted ATMs and gas pumps with phony number pads and card readers to retrieve debit card PIN data. That was a risky approach, because they had to set up the equipment and then come back to remove it without getting caught. Now, with banks using wireless Internet connections to monitor ATM cash flow and update software, hackers can filch PINs remotely, according to a Verizon report. Fraudsters are also taking an *Ocean’s Eleven* approach—getting jobs with technical-support companies that give them access to ATMs, then installing malware that can transmit PIN data to an e-mail address or a phone.

Regulators at the Federal Financial Institutions Examination Council warned in April that the ATMs of small and midsize banks are preferred targets for criminals who hack bank Web pages to boost ATM withdrawal limits and then clean out people’s accounts. Remote hacks of Web-connected ATMs are a fast-growing problem, says Avivah Litan, an analyst at researcher Gartner. In March, the Federal Bureau of Investigation announced charges against 17 people in an alleged skimming scheme that the FBI says stretched from Bulgaria to Chicago.

Story: The First Windows XP Security Problem Microsoft Won't Fix

The memory chips and transmitters that enable PIN hacking are also getting thin and light enough to avoid setting off security equipment that card companies have installed at retail stores in the past few years, says David Robertson, publisher of the *Nilson Report*, a newsletter focused on the payment industry. Often, the hackers’ gear can’t be detected by the software that remotely monitors the weight of point-of-sale terminals, Robertson says: “They’ve done it in a way that suggests a very serious effort to try to crack this industry.”

Although it’s tough to estimate the total lost to these attacks, the U.S. Secret Service estimated annual losses from ATM skimming at more than $1 billion in 2008, its most recent published figure. Sartin says U.S. companies were frequently the targets of the 130 skimming breaches his team studied from last year for its report.

In part, Robertson says, that’s because U.S. consumers carry antiquated magnetic-stripe cards that are more vulnerable to PIN capture than cards with RFID chips, which verify that the original card is present for every transaction. “There’s nothing about PINs in 2014 that’s different than PINs in 1994,” he says. “ATMs are in need of even more defense.”

Story: Endgame's First Acquisition Takes It Beyond Cyber Weapons
Story: New Security Report: The Target Hack Was Just the Beginning
Story: Next Debate on Phones' Kill Switches: Who Turns Them On?
Story: How T-Mobile Increases Competition Without Lowering Your Phone Bill

The bottom line: *Hackers are taking advantage of wirelessly connected ATMs and other card readers to pull off smoother PIN data thefts.*

Robertson is a reporter for Bloomberg News in San Francisco.