Hack makes ATMs spew out cash

July 30, 2010

Barnaby Jack demonstrates an attack on two automated teller machines during the Black Hat technology conference in Las Vegas. Photo: AP

A hacker has discovered a way to force ATMs to disgorge their cash by hijacking the computers inside them.

The attacks successfully targeted standalone ATMs, but they could potentially be used against the ATMs operated by mainstream banks.

Criminals have long known that ATMs aren't tamperproof.

The ATMs spewing out cash. Photo: AP

There are many types of attacks in use today, ranging from sophisticated to foolhardy: installing fake card readers to steal card numbers, hiding tiny surveillance cameras to capture PIN codes, covering the dispensing slot to intercept money and even hauling the ATMs away with trucks in the hopes of cracking them open later.

Computer hacker Barnaby Jack spent two years tinkering in his Silicon Valley apartment with ATMs he bought online. These were standalone machines, the type seen in front of convenience stores, rather than the ones in bank branches.

His goal was to find ways to take control of ATMs by exploiting weaknesses in the computers that run the machines.

He showed off his results at the Black Hat conference in Las Vegas, an annual gathering devoted to exposing the latest computer-security vulnerabilities.

His attacks have wide implications because they affect multiple types of ATMs and exploit weaknesses in software and security measures that are used throughout the industry.

His talk was one of the conference's most widely anticipated, as it had been pulled a year ago over concerns that fixes for the ATMs would not be in place in time. He used the extra year to craft more dangerous attacks.

Jack, who works as director of security research for Seattle-based IOActive, showed in a theatrical demonstration two ways he can get ATMs to spit out money.

Jack found that the physical keys that came with his machines were the same for all ATMs of that type made by that manufacturer. He figured this out by ordering three ATMs from different manufacturers for a few thousand dollars each. Then he compared the keys he got to pictures of other keys, found on the internet.

He used his key to unlock a compartment in the ATM that had standard USB slots. He then inserted a program he had written into one of them, commanding the ATM to dump its vaults.

Jack also hacked into ATMs by exploiting weaknesses in the way ATM makers communicate with the machines over the internet. Jack said the problem was that outsiders were permitted to bypass the need for a password. He didn't go into much more detail because he said the goal of his talk "isn't to teach everybody how to hack ATMs. It's to raise the issue and have ATM manufacturers be proactive about implementing fixes".

The remote style of attack is more dangerous because an attacker doesn't need to open up the ATMs.

It allows an attacker to gain full control of the ATMs. Besides ordering it to spit out money, attackers can silently harvest account data from anyone who uses the machines. It also affects more than just the standalone ATMs vulnerable to the physical attack; the method could potentially be used against the kinds of ATMs used by mainstream banks.

Jack said he didn't think he'd be able to break the ATMs when he first started probing them.

"My reaction was, 'This is the game-over vulnerability right here,'" he said of the remote hack. "Every ATM I've looked at, I've been able to find a flaw in. It's a scary thing."

Kurt Baumgartner, a senior security researcher with anti-virus software maker Kaspersky Lab, called the demonstration a "thrill" to watch and said it was important to improving the security of machines that can each hold tens of thousands of dollars in cash. However, he said he does not think it will result in widespread attacks because banks don't use the standalone systems and Jack did not release his attack code.

Jack would not identify the ATM makers. He put stickers over the ATM makers' names on the two machines used in his demonstration. But the audience, which burst into applause when he made the machines spit out money, could see from the screen prompts on the ATM that one of the machines was made by Tranax Technologies, based in Hayward, California. Tranax did not respond to email messages from The Associated Press.

Triton Systems, of Long Beach, confirmed that one of its ATMs was used in the demonstration. It said Jack alerted the company to the problems and that Triton now had a software update in place that prevents unauthorised software from running on its ATMs.

Bob Douglas, Triton's vice-president of engineering, said customers could buy ATMs with unique keys but generally do not, preferring to have a master key for cost and convenience.

"Imagine if you have an estate of several thousand ATMs and you want to access 20 or so of them in one day," he wrote in an email to the AP. "It would be a logistical nightmare to have all the right keys at just the right place at just the right time."

Other ATM manufacturers contacted by the AP also did not respond to messages.

Jack said the manufacturers whose machines he studied were deploying software fixes for both vulnerabilities, but added that the prevalence of remote-management software broadly opened up ATMs to hacker attacks.

AP

Source: smh.com.au

Top Technology articles

1. At war over WikiLeaks
2. Internet maverick Assange turns to mainstream media in his war on Washington
3. Hack makes ATMs spew out cash
4. Fans happy to be left with own devices as iPad sales boom
5. Labor to force people to connect to broadband

6. More Technology articles