ATM Malware and Jackpotting Attacks Could Be Making a Return

By Nicole Lindsey

Published: 2019-10-23 · Archived: 2026-04-05 22:53:03 UTC

Just a few years ago, there were concerns that ATM malware and jackpotting attacks could represent a clear and present danger to the world's financial system, with ATM machines around the globe at risk of attack. In 2017 and 2018, for example, ATM malware and jackpotting attacks (in which ATM machines are reprogrammed by hackers to dispense cash in large amounts) suddenly started to appear in the U.S. and Europe for the first time. And now, evidence is mounting that these ATM malware and jackpotting attacks could be making a return a few years later, albeit with new twists and approaches.

The return of ATM malware and jackpotting attacks

Much of the new buzz around the return of jackpotting is based around a new joint investigation from VICE Motherboard and the German broadcaster Bayerischer Rundfunk (BR) into the technology and approaches used by German cybercriminals to pull off a series of bold and audacious attacks on German banks back in 2017. According to evidence assembled from bank and law enforcement officials, it now looks like ten different jackpotting attacks took place between February and November 2017, with combined losses of close to €1.4 million.

Given the similarity of these German attacks, there is a strong indication that cybercriminals linked to a single syndicate might be involved. The attacks appeared to be targeting ATM machines from Diebold Nixdorf and Santander Bank. The cybercriminals also showed a preference for a particular piece of ATM malware known as Cutlet Maker. (In Russian crime jargon, a "cutlet" refers not just to a piece of meat, but also to a bundle of bank notes.) When the bank ATM machines were hacked, they displayed a message from Cutlet Maker: "Ho-ho-ho! Let's make some cutlets today!" This message was accompanied by a picture of a chef and a piece of meat displayed on the monitor of the ATM.

An earlier form of this ATM malware first appeared back in 2010, when security researcher Barnaby Jack demonstrated at a Black Hat security conference how he could make an ATM machine spit out cash and display a "JACKPOT" message at the same time. For cybercriminals, there is apparent joy in not only carrying out a mini-bank heist, but also letting everyone know exactly how an ATM jackpotting attack was carried out.

How ATM malware and jackpotting attacks are carried out

The audacity of the traditional jackpotting ATM attack is based on the premise that cybercriminals need to gain physical access to an ATM machine – this is not an attack that can be pulled off online, or solely with the use of stolen credit cards. Instead, the cybercriminals need to install the malware code directly into the machine. The easiest way to do this is via a USB port, CD/DVD port, or networking socket inside the ATM machine – this requires cybercriminals to pry open part of the machine and attach a computing device into the USB port so that the jackpotting malware can be uploaded.

When these attacks started to take place in 2017, they were relatively novel and even ATM manufacturers didn't know how to prevent them from taking place. While ATM machines might look like fancy pieces of computing equipment from the outside, on the inside they are basically old, slow Windows machines that are hard to update with security patches. But very rapidly, banks and ATM operators figured out a way to install security software that actively searches out and denies any malware from going to work inside the ATM machine.

That helps to explain why, after a sudden burst of activity in 2017, we've heard very little about ATM malware and jackpotting exploits since then. But now, say security researchers, cybercriminals are simply changing their tactics, They are now favoring a more extreme tactic known as a "black box attack" (aka "logical attack) in which the cybercriminals must drill holes in the ATM, so that they can connect a laptop to the ATM. Once the connection is made, that is when they can physically attack the ATM's internal computer, in order to re-program it to spit out cash as if it were a Vegas slot machine. This process is not nearly as easy as earlier ATM attacks, of course.

Tim Erlin, VP, product management and strategy at Tripwire, comments on the current state of ATM security: "We like to think of cybersecurity as being limited to software, but the physical security of devices is part of the equation. If you logically protect a system, but leave exposed physical access, you have left risk unaddressed."

"Requiring that criminals physically access a machine to carry out an attack does limit the scalability of that attack technique," says Erlin. "We won't see hundreds of ATMs simultaneously jackpotted with this technique, but it's still a problem for the ATM owners. "Other industries have dealt with the threat of USB-based attacks by disabling the ports in the operating system or even going so far as to fill them with glue. While this is a particularly dramatic attack, using USB ports to carry out attacks isn't new."

Cybercriminals continue to innovate and change attack strategies

Given the time, expense and risk of sitting in front of an ATM machine and drilling a hole in it – something that presumably would be captured by security cameras or attract the attention of security personnel or bank customers – cybercriminals have been forced to change and adapt their tactics. That fact is made clear by another report, this one from the European Society for Secure Transactions (EAST). The EAST report indicates that traditional ATM malware and black box "logical" attacks are on the demise across Europe, presumably due to beefed up security at these machines.

During the first six months of 2019, the number of attacks declined by 43% compared to the year-earlier period. And cybercriminals only were able to carry out one successful attack, for less than $1,000. As a result, EAST says that related losses due to traditional ATM malware and jackpotting attacks fell by 100% compared to the year-earlier period.

Instead, attackers appear to be favoring much more of a dramatic “smash and grab” approach to ripping off ATM machines. The EAST report details a number of these physical attacks, which include a mix of “ram raids” (in which heavy objects are rammed into ATM machines in order to open them up), explosive device attacks (in which explosives are used to blow open a hole to the cash in the ATM), and even attacks where attackers simply carry away the entire ATM machine from the premises of a bank in order to break it open at a “safe” location.

In addition to these brute force attacks, cybercriminals are also experimenting with a form of ATM fraud known as TRF, a form of transaction reversal fraud in which ATM machines are “tricked” into thinking that a bank card has been jammed in the machine. At this point, the ATM machine has already prepared a certain amount of cash to dispense as part of the transaction – and that’s when cybercriminals go to work. At the exact moment that the ATM machine is reversing the transaction, the cybercriminals are prying open the cash drawer of the ATM to pull out the cash. This results in cash being dispensed at the same time as the money is being credited back to the account.

The cat-and-mouse game between cybercriminals and law enforcement

All of these examples should help to illustrate both how creative cyber criminals have become, and also how much more risky and dangerous ATM attacks have become. Some hackers would have you believe that, as soon as you purchase a piece of ATM malware like Cutlet Maker on the Dark Web, you can start a mini-crime spree of jackpotting at your local ATM machines. But, as the EAST report demonstrates, success rates are still very low, and even when they are successful, the amount of cash that can be withdrawn is less than might be expected.

Still, there is reason for concern that hackers will continue to innovate and come up with novel ATM malware and jackpotting schemes. It is, perhaps, only a matter of time before law enforcement officials in both Europe and the U.S begin to worry about a new crime spree of jackpotting attacks. After a brief lull, these ATM jackpotting attacks could return with greater size and sophistication.
