ATM makers alert to cash-spitting attacks

January 30 2018, by Nancy Owano

Credit: CC0 Public Domain

Too much trouble. Holding up a bank means you need to buy a ski mask, map out bank exits, zap the surveillance cameras, threaten panic-stricken customers of bad consequences if anyone dares move. And then there is someone smarter than you who figures out how to sneak and call the cops anyway. You are toast.

Today's thieves skip the drama. They found an easier way, called jackpotting, and they can pocket their stash in minutes and walk off. It just takes an ATM and some tech savvy. If all this sounds like an advert to break the law, it is the opposite. Now ATM machine makers and US Secret Service authorities are on to their game and in time the game will be over.

Jackpotting is when criminals make ATMs that they attack roll out cash. *New York Post* said, "Money mules typically collect the spewed loot." It may be a new story for some US readers but such events have been reported in Europe and Asia.

Now Brian Krebs reported recently of the problem in the United States. His report referred to by many tech watching-sites tell the story of how thieves use a combo of software and hardware at ATMs to release, or, to re-phrase it, spit out the cash.

The U.S. Secret Service warned financial institutions that jackpotting attacks were spotted targeting cash machines in the United States, said Krebs.

As for the ATM makers, they responded to customers. ATM makers Diebold Nixdorf and NCR Corp. issued statements and sent out alerts over the weekend to those clients using their ATMs, Rogers said.

On Jan. 26, NCR sent an advisory to its customers saying it had received reports from the Secret Service and other sources about jackpotting attacks against ATMs in the United States.

(*Krebs On Security* began hearing rumblings about "logical attacks," hitting U.S. ATM operators. He asked NCR what if anything they knew about this. NCR had received unconfirmed reports, but nothing solid yet. Then NCR issued an advisory to its customers saying it had received

reports from the Secret Service and other sources about jackpotting in the U.S.)

Reached for comment, said Krebs, Diebold Nixdorf had an alert sent to customers warning of potential jackpotting in the United States. Attacks seemed to target front-loaded Opteva cash machines.

Furthermore, Reuters on Monday also reported that ATM makers Diebold Nixdorf and NCR Corp warned that cyber criminals were targeting ATMs with tools.

Shelby Rogers, *Interesting Engineering*, said attackers use an endoscope to find a specific internal part of the ATM. "Hackers then attach a laptop and run malware into the system."

Krebs on Security said "The Secret Service alert explains that the attackers typically use an endoscope—a slender, flexible instrument traditionally used in medicine to give physicians a look inside the human body—to locate the internal portion of the cash machine where they can attach a cord that allows them to sync their laptop with the ATM's computer."

Then what? *Krebs on Security*'s report noted crooks installing malware will contact co-conspirators who can remotely control the ATMs and force the machines to give cash.

Krebs on Security said a Diebold alert sent to customers warned of potential jackpotting attacks in the United States.

Krebs noted a January 2017 report from FireEye. Krebs wrote, "FireEye said all of the samples of Ploutus.D it examined targeted Diebold ATMs, but it warned that small changes to the malware's code could enable it to be used against 40 different ATM vendors in 80 countries."

Leigh-Anne Galloway, cybersecurity resilience lead at Positive Technologies was quoted in *Threatpost*: "We have seen quite an increase in logical attacks over the last couple of years and this is certainly one of the most novel. ATMs are still a critical link in communities, providing access to banking services for many people who may never visit a branch itself."

Krebs, referring to the Secret Service alert that said ATMs still running on Windows XP were especially vulnerable; ATM operators with XP were urged to update to a version of Windows 7.

Jackpot schemes, or "logical attacks," have threatened European and Asian banks.

This type of bank machine crime was discovered in Mexico in 2013, said FireEye.

The FireEye report mentioned something called Ploutus which enabled criminals to empty ATMs using a keyboard attached to the machine or via SMS message, said FireEye.

Last year, in January, *The Guardian* carried a report where Daniel Regalado of FireEye noticed ATM malware, where it was possible "for a money mule to obtain thousands of dollars in minutes."

The Guardian said, "Cash machines in more than a dozen countries across Europe were remotely attacked in 2016, according to Russian cybersecurity firm Group IB. Similar attacks were also reported in Thailand and Taiwan."