Crooks have acquired proprietary Diebold software to “jackpot” ATMs

reader comments

88 with 69 posters participating

Share this story

Diebold Nixdorf, which made $3.3 billion from ATM sales and service last year, is warning stores, banks, and other customers of a new hardware-based form of “jackpotting,” the industry term for attacks that thieves use to quickly empty ATMs.

The new variation uses a device that runs parts of the company’s proprietary software stack. Attackers then connect the device to the ATM internals and issue commands. Successful attacks can result in a stream of cash, sometimes dispensed as fast as 40 bills every 23 seconds. The devices are attached either by gaining access to a key that unlocks the ATM chassis or by drilling holes or otherwise breaking the physical locks to gain access to the machine internals.

In previous jackpotting attacks, the attached devices, known in the industry as black boxes, usually invoked programming interfaces contained in the ATM operating system to funnel commands that ultimately reached the hardware component that dispenses cash. More recently, Diebold Nixdorf has observed a spate of black box attacks that incorporated parts of the company’s proprietary software.

“Some of the successful attacks show a new adapted Modus Operandi on how the attack is performed,” Diebold Nixdorf warned in an active security alert that was issued last week and provided to Ars by a company representative. “Although the fraudster is still connecting an external device, at this stage of our investigations it appears that this device also contains parts of the software stack of the attacked ATM.”

The advisory said elsewhere:

> *In general, jackpotting refers to a category of attacks aiming to dispense cash from an ATM illegitimately. The black box variant of jackpotting does not utilize the software stack of the ATM to dispense money from the terminal. Instead, the fraudster connects his own device, the “black box,” to the dispenser and targets the communication to the cash-handling device directly.*
>
> *In the recent incidents, attackers are focusing on outdoor systems and are destroying parts of the fascia in order to gain physical access to the head compartment. Next, the USB cable between the CMD-V4 dispenser and the special electronics, or the cable between special electronics and the ATM PC, was unplugged. This cable is connected to the black box of the attacker in order to send illegitimate dispense commands.*
>
> *Some incidents indicate that the black box contains individual parts of the software stack of the attacked ATM. The investigation into how these parts were obtained by the fraudster is ongoing. One possibility could be via an offline attack against an unencrypted hard disc.*

Mimicking the ATM computer

The growing number of attacks target the company’s ProCash line terminals, particularly the ProCash 2050xs USB model. The

ongoing attacks are occurring in “certain European countries,” the advisory said.

Bruno Oliveira, an expert in ATM security, said he had heard of the earlier form of black-box attack. The connected device manipulates the APIs included in OS extensions such as XFS or CFS, which communicate with remote servers operated by financial institutions. Black boxes, which mimic an ATM’s internal PC, can either be laptops or Raspberry or Arduino hardware that’s fairly easy to build, Oliveira said. Black boxes are one of four jackpotting techniques that Diebold Nixdorf describes here.

In some cases, the attached devices connect directly to the cash dispenser and issue commands for it to spit out cash. The other form of black-box attack plugs into network cables and records cardholder information as it’s relayed back and forth between the ATM and the transaction center that processes the session. The attached device then changes authorized maximum withdrawal amounts or masquerades as the host system to allow the ATM to dispense large sums of money.

The above-linked jackpotting brochure describes two other types of attacks. The first swaps out the legitimate hard drive with one created by the attackers. The other uses phishing attacks against bank employees. Once attackers obtain access inside the network of a financial institution, they issue commands that infect ATMs with malware that can be used to clean out the machines.

Good news and bad news

The new attack variation described by Diebold is both good and bad news for consumers. On the one hand, there’s no indication thieves are using their recently acquired software stack to steal card data. The bad news is that attackers appear to have their hands on proprietary software that makes attacks more effective. The recent increase in successful jackpotting

ultimately results in higher fees, as financial institutions pass on the costs caused by the losses. Diebold has issued a variety of defenses that ATM owners can take to protect against the attacks.

There’s little ATM users can do to prevent jackpotting. Still, it’s important to use only ATMs belonging to major banks and eschew those from mom-and-pop businesses. It’s also a good idea to shield the keyboard while entering PINs and to check bank statements each month in search of any unauthorized transactions.

https://arstechnica.com/?p=1692972