‘Jackpotting’ attacks are now hitting US ATMs, report says

The Secret Service has been warning US financial institutions that domestic ATMs are being targeted in jackpotting attacks, according to a new report from well-known security journalist Brian Krebs.

Jackpotting, in which thieves use a variety of tools to hack into ATMs and cause them to dispense large amounts of cash on demand, has been a legitimate threat for several years now. The late computer hacker Barnaby Jack famously showed off an ATM exploit at the Black Hat conference back in 2010. But until now, jackpotting was mostly a threat in Europe, Asia, and Mexico.

According to the Krebs report, the US Secret Service recently sent out a confidential alert to multiple financial institutions warning that the “targeted stand-alone ATMs are routinely located in pharmacies, big box retailers, and drive-thru ATMs.”

Thieves are posing as ATM technicians and hacking into the machines

The thieves have been posing as ATM technicians and, using a medical endoscope, locate an area within the machine where they can attach their own computers. The original hard disk of the ATM is removed and replaced with a disk that mirrors the ATM’s own software. At that point, the ATM appears out of service to regular customers, while fraudsters can remotely control it and force it to spit out cash, using “money mules” to actually collect the cash.

It’s unclear which particular strain of malware is being used in this case, though the Krebs report suggests that it could be a strain of malware known as Ploutus.D. Last spring, researchers from Kaspersky Lab wrote about , including using a

file-less malware known as ATMitch.

In this recent spate of US attacks, fraudsters appear to be targeting Diebold Nixdorf-made ATMs, which has said in a statement that “potentially all front-load AFD based Opteva models” could be vulnerable. Another ATM manufacturer, NCR Corporation, has also warned customers about the potential attacks, though it has said the attacks currently “appear focused on non-NCR ATMs.” ATMs still running Windows XP are said to be particularly vulnerable, according to the Krebs report.

https://www.theverge.com/2018/1/29/16947832/jackpotting-atm-machine-hack-cash-malware