Issued 1/29/18

ATM Jackpotting Hacks Reach the US

The US Secret Service has warned ATM makers Diebold Nixdorf and NCR that "jackpotting" hacks, where crooks force machine to cough up large sums of cash, have reached the US after years of creating problems in Asia, Europe and Mexico. The attacks have focused largely on Diebold's front- loading Opteva ATMs in stand-alone locations, such as retail stores and drive-thrus, and have relied on a combination of malware and hardware to pull off heists. In previous attacks, the thieves disguised themselves as technicians to avoid drawing attention. After that, they hooked up a laptop with a mirror image of the ATM's operating system and malware (Diebold also mentioned replacing the hard drive outright). Security researcher Brian Krebs understands American ATMs have been hit with Ploutus.D, a variant of "jackpotting" malware that first launched in 2013. The mirror image needs to be paired with the ATM to work, but that's not as difficult as you might think -- the intruders used endoscopes to find and press the necessary reset button inside the machine. Once done, they attached keyboards and used activation codes to clean out ATMs within a matter of minutes. The Secret Service warned that ATMs still using Windows XP were particularly easy targets, and that updating to Windows 7 (let alone Windows 10) would protect against these specific attacks. Diebold also recommended updating to newer firmware and using the most secure configurations possible.