Uptick in ATM Jackpotting Attacks

During the previous six months, there has been an increase in both ATM successful and unsuccessful jackpotting attempts. The Secret Service has recently seen traditional malware, black box, and man-in-the-middle (MiTM) attacks on ATMs in Utah, Minnesota, Texas, Colorado, Idaho, Maryland, Georgia, South Carolina, North Carolina, Tennessee, California, Pennsylvania, Oregon, Washington, and New York. These incidents have occurred across multiple ATM manufacturer brands and are believed to have been perpetrated by at least seven different criminal groups.

Subjects were observed opening and accessing the ATMs using magnets and generic keys designed to unlock an ATM's exterior. The subjects are believed to still be in the U.S. and are expected to continue to carry out additional ATM attacks.

Malware Jackpotting

Malware jackpotting occurs when malware is introduced to the ATM hard drive, usually using a portable device (i.e., USB). The malware is then used to issue dispense commands to the ATM using the existing ATM computer and ATM dispenser connection, which results in the ATM dispensing cash to the criminal.

Black Box Jackpotting

Black box jackpotting occurs when the legitimate ATM dispenser is disconnected from the ATM computer and an unauthorized external device, such as a laptop or tablet, is connected directly to the ATM dispenser. The unauthorized device (i.e., black box) is used to send dispense commands directly to the cash dispenser, which results in the ATM dispensing cash to the criminal operating the black box.

MiTM Jackpotting

MiTM jackpotting attacks focus on the communication between the ATM's computer and the acquirer's host system, which is responsible for approving or denying transactions. Criminals install an unauthorized device between the ATM's PC and network cable connection to spoof the acquirer's host system response. This method is used to dispense cash without debiting the account associated with the transaction. Transactions are repeated until the ATM is depleted of cash.

Mitigation and Prevention

The Secret Service recommends that financial institutions and retailers who own and operate ATMs to proactively reach out to their ATM manufacturers to ensure that their ATM fleets are up-to-date on all security recommendations. The following recommended processes should be considered.

- Follow the safety and security recommendations of ATM manufacturers to ensure the ATMs have the latest updates (such as firmware), protections, hardware, and software. This can help prevent a variety of physical and logical attacks.
- Ensure that the operating system and configurations are up-to-date.
- Ensure that ATM hard drives are encrypted.
- Secure network communication with TLS encryption.
- Limit physical access to ATMs. Generic keys can lead to stealing, copying, or purchasing keys to access multiple ATMs.
- Implement access controls for ATM service technicians, to include multi-factor authentication where possible.

Response

If you suspect that an ATM is compromised using these jackpotting techniques, you should perform the following steps if attempting to confirm the compromise.

- Before opening the ATM, wear gloves to avoid contaminating any potential DNA evidence and prints.
- Before removing any unauthorized devices from the ATM, photograph all components, hard drive, and any attached devices.

You should contact your local law enforcement agency to report the compromise. Law enforcement personnel will examine the ATM for evidence.

Contact your *local field office Cyber Fraud Task Force* to report.