NEW Jackpotting Attack Vector

Beginning on 05/13/2024, the Secret Service Global Investigative Operations Center (GIOC) has observed a new type of jackpotting attack that specifically targets the software used to change the settings on retail ATMs around the United States. For additional information, reference **GIOC Alert #24-005-I: "Uptick in Jackpotting"** sent on 03/22/2024.

Subjects remotely accessed the ATM software from a malicious IP Address, spoofing the Remote Management Solutions (RMS) program where they conduct a man-in-the-middle (MiTM) attack. The purpose of accessing this program was to raise the maximum withdrawal amount, and approve all declined transactions, debiting the ATM, but not the card that was used. There have been several individuals observed cashing out ATMs via the exposed vulnerability.

Man-in-the-middle (MiTM) attacks focus on the communication between the ATM and the acquirer's host system, which is responsible for approving or denying transactions. This new attack vector is initiated after the threat actors access systems through open network ports.

Mitigation and Prevention

1. ATMs without this type of RMS are not currently impacted.
2. ATMs with RMS (especially on wireless) need to change the default password and enable RMS SSL.
3. Key Encryption – Change the encryption type to MACing which has each transaction go through a MAC validation process. If the terminal or the host detects a miscalculation, a MAC Validation Error will be triggered.
4. MAC Address Sync – Similar to the MAC validation process above, the ATM application will validate the MAC Address of the device connected to the ATM. If a suspect device is connected between the ATM and the host, the ATM software can detect if the MAC address of the communication device has changed and will not dispense cash.
5. Conduct frequent risk assessments to have a detailed overview about your ATM fleet from a hardware and software perspective, your infrastructure, your processes, and the specific exposure in your market. If missing countermeasures are identified in the current framework, then seek a risk acceptance statement from senior management.

The Pittsburgh Field Office is investigating this new jackpotting attack vector. If your district has observed or reported this behavior, please pass all information to the GIOC at 202-406-6009 / GIOC@usss.dhs.gov.

This alert should only be shared with trusted law enforcement and financial institution partners.