Allied Solutions

Fraud Risk Bulletin

Exclusive, As-It-Happens Risk Updates and Insights

ATM/ITM Jackpotting will empty your ATM/ITM

SUMMARY

Due to the nature of ATM/ITM Jackpotting (cash out), this threat has the potential to cause tremendous losses for financial institutions.

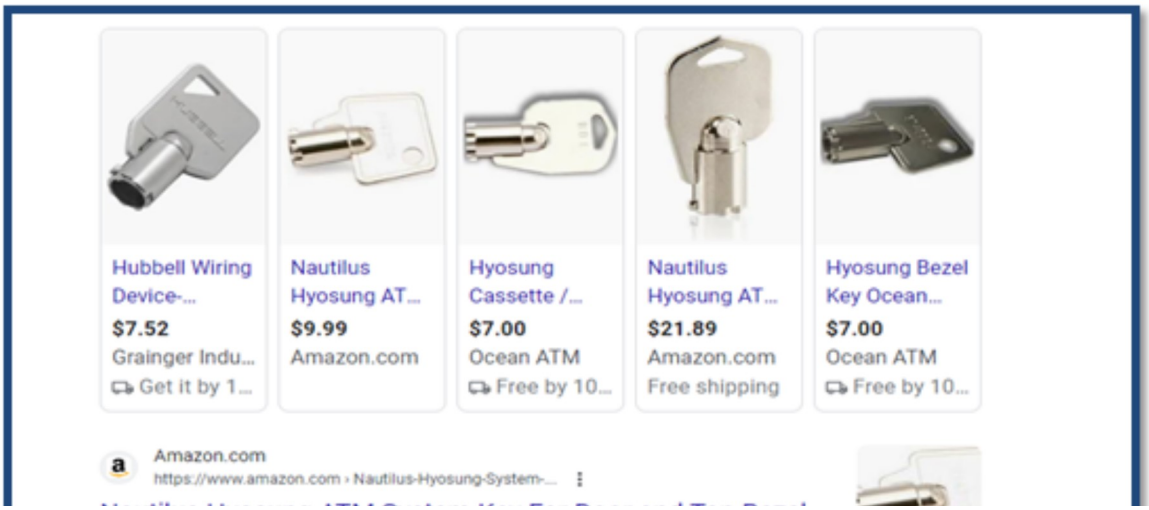
HOW DOES ATM/ITM JACKPOTTING FRAUD HAPPEN?

For an ATM/ITM jackpotting operation, you need to have **physical access** to the ATM/ITM and a rogue device. A **rogue device** is a wireless hardware attack tool, like a portable computer, that doesn't have permission to access a network but exists to cause harm, steal information, and disrupt the network's normal operations. The criminal then manipulates settings on the machine to dispense cash until the machine is empty. The cash dispensed is not tied to the balance of any one accountholder.

DETAILS

Physical Access

- *Universal keys* – a quick online search for "universal ATM keys" pulls up several options for quick purchase. These keys are designed to open nearly any ATM/ITM enclosure… providing access to the computer that controls the machine wide open for manipulation by an attacker.



Rogue Access – to Dispense Cash Out

- Once the attacker has physical access to the ATM/ITM, malware is installed using the internal hardware ports. The USB port is the most common infection point. After the malware is installed, a code is entered to dispense the cash.
- Once infected with malware, the ATM/ITM's middleware is targeted to orchestrate the attack. Middleware is an application programming interface (API) that is used to communicate with the ATM's peripherals (e.g., the PIN pad and money cassettes).
- Remote attacks typically present less risk of being caught. In the remote attacks, fraudsters access the financial institution's local network, bypassing existing defenses, which allows them to gain control over the ATM/ITM.

RISK MITIGATION STEPS

- Ensure each of your ATM/ITMs have one or more specially designed keys to limit access and thwart universal keys.
- Arm the top hat with of the ATM/ITM with an alarm, alerting you of the physical breach before the cash dispense commences.
- Encrypt the ATM/ITM hard drive to protect the data and make data manipulation more difficult for attackers.
- Ensure that any unused USB or network ports (CAT5/CAT6) on the ATM are deactivated.
- Use strong passwords, make sure it is not the default password.
- Create a whitelist to prevent unauthorized applications from being installed.
- Make sure the ATM/ITM is included in software updates and security patches.
- Work with ATM/ITM vendors to ensure jackpotting exposures are properly addressed.
- Ensure ATM/ITM operating software is supported and install security patches as soon as possible after they are made available by the manufacturer.
- Perform daily ATM/ITM inspections to ensure lighting is adequate, the atm is not obstructed or concealed, and cameras and alarms are functioning properly.
- Confirm that you have all ATM/ITM settings in a controlled "authorized" setting so if the ATM/ITM is under attack for cash out, the ATM/ITM shuts down.

RISK MITIGATION RESOURCES

- Article: "Examining Cutting Edge ATM Software Attacks"
- Article: "Three Plead Guilty to ATM 'Jackpotting"
- Article: "Jackpotting Attacks are Back – But Banks Can Fight Back"
- View Allied's Risk Resource Library

information purposes only and the financial institutions should work with their legal counsel with respect to any legal matter referenced on this article.

 LinkedIn  Facebook