ATM Jackpotting Coordinated Attacks

During the previous 12 months, there has been an increase in observed ATM jackpotting attempts. The Secret Service has recently seen both traditional malware and man-in-the-middle (MITM) attacks on ATMs in New York, New Jersey, Texas, Illinois, Arizona, and Oklahoma. These incidents have occurred across multiple ATM brands and are believed to have been perpetrated by different criminal groups.

The Secret Service was made aware of recent coordinated ATM jackpotting incidents in the upstate New York area. A similar coordinated incident occurred just one month prior in Oklahoma. These coordinated incidents targeted approximately 35 ATMs and resulted in more than $1.5 million in loss in a matter of hours.

During these particular incidents, subjects were observed opening and accessing the ATMs using magnets and generic keys designed to unlock an ATM's exterior. Surveillance photos of subjects involved in these recent incidents are provided in this alert for the situational awareness of law enforcement and financial institution personnel. The Secret Service has received intelligence that the subjects pictured in the surveillance photos are still present in the U.S. and are expected to carry out additional ATM attacks.

What is ATM jackpotting?

ATM jackpotting is when malware is introduced to the ATM's hard drive or a MITM technique is used to interrupt communications with the ATM's hard drive. In either scenario, the ultimate goal of the criminal is to direct the ATM to dispense its cash.

How to protect against ATM jackpotting:

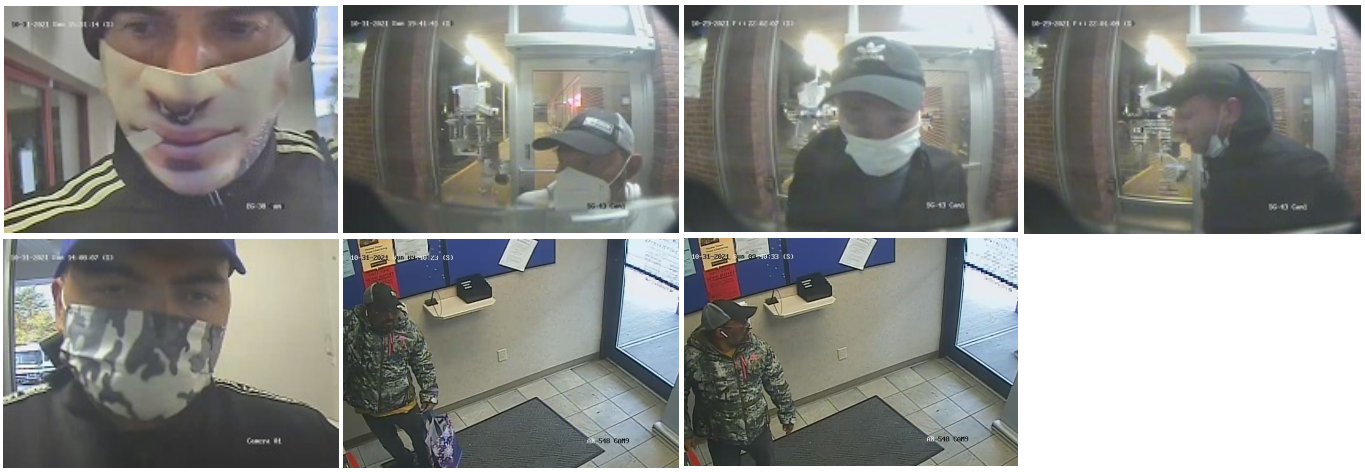
- Follow the safety and security recommendations of ATM manufacturers to ensure the ATMs have the latest updates, protections, hardware and software needed to prevent a variety of physical and logical attacks.
- Limit physical access to ATMs. Generic keys do not protect against individuals stealing, copying, or purchasing keys to access multiple ATMs.
- Implement access control for service technicians based on two-factor authentication.
- Ensure the latest firmware updates are installed.
- Keep the operating system, software, and configuration up to date.
- Ensure ATM hard drives are encrypted.

United States Secret Service
Global Investigative Operations Center

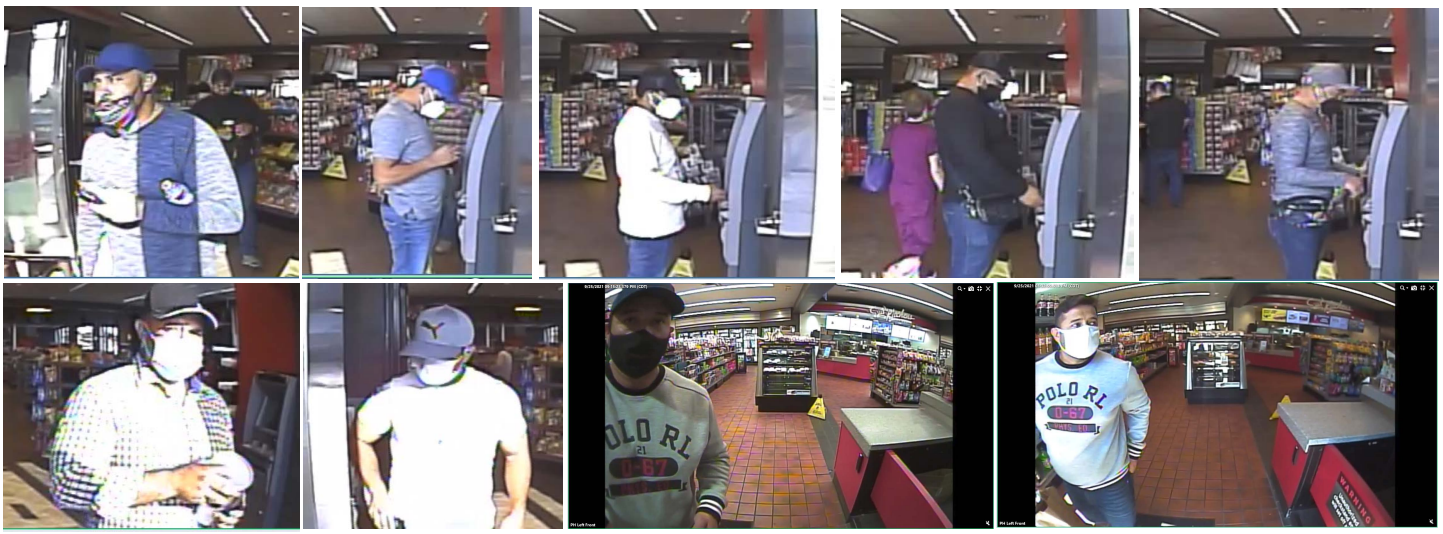
GIOC ALERT

TLP GREEN

Subjects observed in October 2021 in Upstate NY:



Subjects observed in September 2021 in OK, TX & AZ:



To report criminal activity, contact your local

U.S. Secret Service field office Cyber Fraud Task Force (CFTF).