October 7, 2020

BULLETIN: THE THREAT OF ATM CASH-OUTS PAYMENT SECURITY

The PCI Security Standards Council (PCI SSC) and the ATM Industry Association (ATMIA) want to highlight an emerging threat that requires urgent attention.

What is the threat?

An ATM "cash-out" attack is an elaborate and choreographed attack in which criminals breach a bank or payment card processor and manipulate fraud detection controls as well as alter customer accounts so there are no limits to withdraw money from numerous ATMs in a short period of time. Criminals often manipulate balances and withdrawal limits to allow ATM withdrawals until ATM machines are empty of cash.

How do these attacks work?

An ATM cash-out attack requires careful planning and execution. Often, the criminal enterprise gains remote access to a card management system to alter the fraud prevention controls such as withdrawal limits or PIN number of compromised cardholder accounts. This is commonly done by inserting malware via phishing or social engineering methods into a financial institution or payment processor's systems.

The criminal enterprise then can create new accounts or use compromised existing accounts and/or distribute compromised debit/credit cards to a group of people who make withdrawals at ATMs in a coordinated manner. With control of the card management system, criminals can manipulate balances and withdrawal limits to allow ATM withdrawals until ATM machines are empty of cash.

These attacks usually do not exploit vulnerabilities in the ATM itself. The ATM is used to withdraw cash after vulnerabilities in the card issuers authorization system have been exploited.

Who is most at risk?

Financial institutions, and payment processors are most at financial risk and likely to be the target of these large-scale, coordinated attacks. These institutions stand to potentially lose millions of dollars in a very short time period and can have exposure in multiple regions around the world as the result of this highly organized, well-orchestrated criminal attack.

What are some DETECTION best practices?

Since ATM "cash-out" attacks can happen quickly and drain millions of dollars in a short period of time, the ability to detect these threats before they can cause damage is critical. Some ways to detect this type of attack are:

- ✓ Velocity monitoring of underlying accounts and volume
- ✓ 24/7 monitoring capabilities including File Integrity Monitoring Systems (FIMs)
- ✓ Reporting system that sounds the alarm immediately when suspicious activity is identified
- ✓ Development and practice of an incident response management system
- ✓ Check for unexpected traffic sources (e.g. IP addresses)
- ✓ Look for unauthorized execution of network tools

What are some PREVENTION best practices?

The best protection to mitigate against ATM "cash-outs" is to adopt a layered defense that includes people, processes, and technology. Some recommendations to prevent ATM "cash-outs" include:

- ✓ Strong access controls to your systems and identification of third-party risks
- ✓ Employee monitoring systems to guard against an "inside job"
- ✓ Continuous phishing training for employees
- ✓ Multi-factor authentication
- ✓ Strong password management
- ✓ Require layers of authentication/approval for remote changes to account balances and transaction limits
- ✓ Implementation of required security patches in a timely manner (ASAP)
- ✓ Regular penetration testing
- ✓ Frequent reviews of access control mechanisms and access privileges
- ✓ Strict separation of roles that have privileged access to ensure no one user ID can perform sensitive functions
- ✓ Installation of file integrity monitoring software that can also serve as a detection mechanism
- ✓ Strict adherence to the entire PCI DSS

Organizations should implement Multi-Factor Authentication (MFA) for all access to their systems particularly to systems providing support or administrative functions. In doing so, organizations can prevent the likelihood of these repositories from being accessed by malicious threat actors and better secure their infrastructure.

Applying security patches for all software updates is critically important. ATM Cash-out attacks often begin when criminals have successfully inserted harmful malware into a payment system. By using the latest anti-virus software and keeping your patching current, this risk can be significantly decreased.

Organizations should install file integrity monitoring software and use only trusted software vendors. File integrity monitoring software can detect unusual patterns and alert you to potential problems/attacks. Choose software vendors that build security into their software products and provide ongoing support for security updates throughout the software lifecycle.

Reporting systems that sound the alarm on suspicious activity empower organizations to quickly identify attacks and deal with them in a timely manner. ATM Cash-out attacks often involve cyber criminals having access to systems for months as they learn the vulnerabilities within an organizations system and organize their plan of attack accordingly. Having a reporting system that can alert an organization of suspicious activity early in the process can help to stop an attack.

PCI DSS compliance is a good security foundation for creating a culture of security within your organization. PCI DSS requires many practices that can help against ATM Cash-out Testing attacks such as multi-factor authentication, patching, and installation of file integrity monitoring software.

###

About the PCI Security Standards Council
The PCI Security Standards Council (PCI SSC) leads a global, cross-industry effort to increase payment security by providing industry-driven, flexible and effective data security standards and programs that help businesses detect, mitigate and prevent cyberattacks and breaches. Connect with the PCI SSC on LinkedIn. Join the conversation on Twitter @PCISSC. Subscribe to the PCI Perspectives Blog.

About ATMIA
ATMIA is the leading non-profit trade association representing the entire global ATM industry. ATMIA serves more than 11,000 members from over 650 companies located in 70 countries spanning the entire

ATM ecosphere, including financial institutions, independent ATM deployers, equipment manufacturers, processors and a plethora of ATM service and value-added solution providers. To join us please visit: https://www.atmia.com/membership/join/