BEST PRACTICES FOR BANKS

Reducing the Risks of ATM Cash-Outs

(Developed by the Bankers Electronic Crimes Task Force)

INTRODUCTION

ATM Cash-Outs and ATM Jackpotting are both terms that refer to a category of attack that typically has a single purpose of illegitimately dispensing cash from an ATM. These attacks can also work against Interactive Teller Machines (ITM). The term ATM in this document will refer to both types of machines.

These types of theft have dated back to at least 2008 when $9 million was stolen. One of the most recent large thefts in mid-2016 was a reported $2.3 million taken from 34 machines in Taiwan. The theft was performed without touching the ATMs' keypad or inserting a card. The frequency of these types of thefts has been increasing. Due to the size of the potential thefts, it is important for all banks to begin measuring and limiting their risk.

BACKGROUND ON ATM CASH-OUT

ATM Cash-Out thefts often involve the use of debit cards linked to just a few accounts, which could all be from just one financial institution. Some thefts do not use account access but access the maintenance mode of the ATM and signal it to dispense cash. The financial liability in these situations differs but can be quite large.

Risk exposure is not always clear. ATM ownership and contractual arrangements to implement usage of ATMs is a complex field. Some banks:

- own their ATMs and completely manage the ATMs;
- own their ATMs but contract with a third party to manage the operations;
- pay a "branding fee" to put their name on ATMs that are fully owned and serviced by a third party;
- "lease" from a third party the cash in their machines; or
- use a mixture of these arrangements across the various markets they serve.

These broad and varied methods for implementing ATM usage necessitates that banks carefully analyze what their financial exposure could be when an ATM Cash-Out theft occurs. The need for a careful analysis is compounded by the broad and varied methods for carrying out the crime, which ensures that forensic investigations will play a central role in identifying liability. This complexity creates different responsibilities and liabilities for each bank. A comprehensive analysis of these complex and varied arrangements and the associated risk mitigation strategies are beyond the scope of this document. Each institution will need to study their unique situation, and identify their unique risks. These Best Practices are a starting point for evaluating risks and for reducing risks of ATMs being compromised. Going forward, increased industry collaboration should help to further mitigate these risks.

TYPES OF ATM CASH-OUT ATTACKS

Three distinct attack vectors have been recognized at this time:

1) Compromising web consoles
2) Injecting malware into the internal processing unit of the ATM
3) Connecting a "black box" device to the ATM

It is important to understand all three attack types to effectively defend against them.

Web Console Attacks - Some systems permit bankers to log into a console/portal "from the Internet" to modify the settings of their ATMs. When this method of managing ATMs is an option, an attacker can compromise the credentials of an administrator and can log into the ATM control system to override controls or remove limits from the machine (or limits per customer) to allow for unlimited transactions. This attack method is believed to be the most common.

Malware Based Attacks - Malware attacks compromise the internal processing unit of the ATM itself to cause the unit to trigger the dispensing of cash. Infection can take place either by using the network the unit is attached to, or by connecting an infected portable device to either transfer the malware or cause the ATM unit to reboot from the infected device.

Black Box Attacks - Black box jackpotting is a different approach whereby a device ("black box") is connected to the ATM, bypassing the internal processing unit, and directly targeting the cash dispensing unit. Black box attacks are generally specific and limited to a targeted ATM model. They require the attacker to drill a hole in a precise location to insert and connect the device, or to simply unlock the ATM cabinet with black market keys, since only a few standard keys exist for some models.

SUMMARY

To understand and mitigate the risks of ATM jackpotting, banks must understand the exact implementation method(s) they use and how their ATM units connect and communicate. A documented assessment is a fundamental first step, which will need to evolve as the complexity of an institution's implementation is better understood.

Limiting physical access to the units is as important as controlling the upstream and downstream network communication avenues.

Hardware and software components that connect to the devices must be hardened against compromise, monitoring capabilities must be implemented to receive alerts for anomalies, and appropriate response and recovery processes must exist to ensure swift and appropriate action should a compromise occur.

BEST PRACTICES FOR BANKS

Reducing the Risks of ATM Cash-Outs

(Developed by the Bankers Electronic Crimes Task Force)

IDENTIFY

I1. Know what the bank has – a risk assessment is crucial.

- How are the ATMs networked?
- What security, both physical and logical, is in place?
    - Who has access to ATMs (employees, ATM vendors, other service personnel)?

I2. Develop detailed data flow diagrams and network topology diagrams to understand the connectivity types.

- How are the ATMs connected to the network?
    - Segregated?
    - Behind a firewall?
- How are the ATMs connected to the switch or processing hub?

I3. Identify bank roles and responsibility should ATM Jackpotting occur through the bank's ATMs.

- Has the bank's environment been defined/documented?
- Have all contracts related the bank's ATM arrangements been reviewed?

I4. Identify third party risk

- Who drives the bank's ATMs? Who has access to service them?
- What controls does the bank's ATM service provider have in place?
- What controls does the bank's ATM driver have in place?
- What security controls are in place for:
    - Unusual volume activity,
    - Unusual dollar amounts, and
    - Unusual activity during non-peak times?

I5. Is software support (for patching vulnerabilities) evaluated, regardless of whose responsibility it is?

- Are end-of-life software assessments performed?
- Has Windows XP been replaced?

PROTECT

P1. Control physical access.

- Are only those with a need able to physically access the bank's ATMs?
  - Do you regularly review who has access to the bank's ATMs (employees and third parties)?
- If ATMs are inside the institution, are they behind a locked door?

P2. Consider making ATM cabinets more secure.

- Have default or master style keys and locks been changed to unique sets?
- Has adding cabinet alarms been considered?

P3. Segment ATMs from the rest of the bank's network via firewall, VLANs, etc.

- Have you used logical security to help reduce an adversaries' movement?

P4. Ensure ATM hard drives are encrypted, BIOS systems are read only or password protected and that boot devices in BIOS are internal only (primary HHD, no CD or USB boot allowed).

P5. Ensure that a strict password policy is in place.

- Is it required that default passwords be changed?
- Are complex passwords used?

P6. Maintain regular cyber hygiene practices consistent with other bank systems.

- Are end of life software packages replaced / updated?
- Are good patching policies followed?
  - If managed by a third party, are their practices reviewed?
  - Has AutoPlay within Windows been disabled?
- Is the use of external devices (flash drives, memory cards, CD ROM, etc.) limited?
- Is installation of unnecessary software (e.g. Acrobat Reader, RDP, etc.) prohibited?

P7. Ensure proper training of staff members.

- Is social engineering training done regularly, since adversaries have to get either physical or logical access to launch an attack?

P8. Utilize resources to regularly receive information regarding new threats and schemes to reduce the risks of ATM Jackpotting schemes (FS-ISAC and ATM vendor).

P9. Evaluate other ATMs controls.

- Are skimming devices detected?
- Have malware controls been installed?

P10 Use dedicated computers that are not connected to (or that are segmented from) the bank’s network to access ATM consoles / ATM portals.

- Have the computers been configured to prevent email access, web access (other than to the ATM portal) and use of USB drives (unless needed)?

DETECT

D1. Establish a known clean baseline for all ATM hardware that can be used as a measurement to determine any deviations.

- What is usual volume activity for all time periods?
- What are typical patterns of dollar amount withdrawals and frequency?
- What is usual activity during non-peak times?
- Is the cash level monitored and is that the only indicator of compromise for attacks that do not use cards / accounts?
- Is the volume/dollar activity monitored across the bank's ATM estate?
- Is the volume/dollar activity monitored across the bank's card base?

D2. Monitor system hardware and software for any discreet or overt changes to the operating system, BIOS, boot configuration, or hardware configuration.

D3. Receive alerts if the USB port is utilized.

D4. Limit administrator rights, and receive alerts if login occurs.

D5. Implement real time monitoring of software activity on ATMs to detect unusual activity.

D6. Establish processes to regularly inspect units physically for unauthorized access or tampering.

- Has a list of indicators of physical tampering been created?
- Has the frequency of inspections been specified?

RESPOND

Rd1. Act immediately and with urgency when anomalies ae detected.

Rd2. Ensure that the institution has an appropriately written (and tested) Incident Response Plan – and follow it.

  a. Does it ensure that the attack vector is identified and mitigated?

  b. Are the bank's device models and system types documented?

    a. If a skimmer or black box is found on an ATM, how many other ATMs of that brand and type does the bank have? Where are they?

    b. Are all other ATMs of the same model / family reviewed to ensure no additional compromises?

Rd3. Contact appropriate law enforcement, legal counsel, and insurance representatives immediately.

Rd4. Consider shutting down the ATM network and/or turning off all ATM cards if widespread fraudulent withdrawals are occurring.

RECOVER

Rr1. Have a contract for forensics services.

Rr2. Ensure clean-state backups are readily available and tested.

Rr3. Perform a lessons-learned debrief after a full and complete recovery.

Rr4. Document how to prevent this in the future for the same type of event or for different locations.

ADDITIONAL RESOURCES

FFIEC Joint Statement – Cyber-attacks on…ATM and Card Authorization Systems
https://www.ffiec.gov/press/PDF/FFIEC%20ATM%20Cash-Out%20Statement.pdf

The following information is from non-government sources and for-profit corporations. Some information is available to non-customers and includes non-product specific information that can be helpful to non-customers. No endorsement is implied.

NCR Logical Security (Configuration and Deployment Best Practices)
https://www.ncr.com/wp-content/uploads/15FIN3755_Configuration_and_Deployment_Best_Practices_Guide.pdf

ATM Marketplace / DieboldNixdorf White Paper:
Managing ATM Security: Layered Approaches
http://www.dieboldnixdorf.com/en-us/company/strategic-topics/security/atm-attacks-whitepaper

Banks using Diebold ATMs are encouraged to contact their Diebold ATM sales representative and request the following documents:

- Diebold/Nixdorf Corporate Security & Fraud Management Fact Sheet: ***ATM Malware Alice*** dated December 22, 2016

- Diebold/Nixdorf ***ATM Fraud and Security*** White Paper

VISA ATM Jackpotting Alert
https://usa.visa.com/dam/VCOM/global/partner-with-us/documents/visa-technical-analysis-atm-jackpottingmalware.pdf