Best Practices for Preventing ATM Malware, Black Box and Cyber-Attacks

International Minimum Security Guidelines and Best Practices

Produced by the ATM Industry Association

Contributors Include:

Copyright Information

e-mail Mike Lee, ATMIA's CEO, at mike@atmia.com

Disclaimer

The ATM Industry Association (ATMIA) publishes this best practice manual in furtherance of its non-profit and tax-exempt purposes to enhance the security of ATM systems from malware, black box and cyber-attacks. ATMIA has taken reasonable measures to provide objective information and recommendations to the industry but cannot guarantee the accuracy, completeness, efficacy, timeliness or other aspects of this publication. ATMIA cannot ensure compliance with the laws or regulations of any country and does not represent that the information in this publication is consistent with any particular principles, standards, or guidance of any country or entity. There is no effort or intention to create standards for any business activities. These best practices are intended to be read as recommendations only and the responsibility rests with those wishing to implement them to ensure they do so after their own independent relevant risk assessments and in accordance with their own regulatory frameworks. Further, neither ATMIA nor its officers, directors, members, employees or agents shall be liable for any loss, damage or claim with respect to any activity or practice arising from any reading of this manual; all such liabilities, including direct, special, indirect or inconsequential damages, are expressly disclaimed. Information provided in this publication is "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or freedom from infringement. The name and marks ATM Industry Association, ATMIA and related trademarks are the property of ATMIA.

Please note this manual contains security best practices and should not be left lying around or freely copied without due care for its distribution and safekeeping.

Table of Contents

Foreword 4
Executive Summary 5
Acknowledgements 6
Chapter 1. Introduction 7
Chapter 2. ATM Malware 9
2.1. Overview 9
2.2. Malware Functionality 9
2.3. Malware Installation 9
2.4. Accessing the ATM 10
2.5. Execution of Malware 10
2.6. Detection of Malware 10
2.7. ATM Malware Case Study Examples 11
2.7.1. Skimer-A 11
2.7.2. Unknown 12
2.7.3. Scrooge 12
2.7.4. Siberian Malware 12
2.7.5. Dump Memory Grabber 12
2.7.6. Backdoor Ploutus 13
2.7.7. Backdoor Ploutus, Version B/Ploutos 13
2.7.8. Trojan.Skimer.18 13
2.7.9. Atmh4ck 14
2.7.10. Backdoor Ploutus, Version B/Ploutus (SMS) 14
2.7.11. Unknown 15
2.7.12. Backdoor.Padpin 15
2.7.13. Macau Malware 15
2.7.14. Unknown 16
2.7.15. Backdoor.MSIL.Tyupkin 16
2.7.16. Trojan.Skimmer (New Variant) 16
Chapter 3. Black Box Attacks 17
3.1. Overview 17
3.2. Black Box Functionality 17
3.3. Attaching Black Box Devices 18
3.4. Accessing the ATM 18
3.5. Executing Black Box Attacks 18
3.6. Detecting Black Box Attacks 18
Chapter 4. Hijacking ATM Control and Authorization Systems 20
4.1. Overview 20
4.2. Carbanak Case Study 20
4.3. Man-in-the-Middle Case Study 21
Chapter 5. Best Practices 22
5.1. Mitigation Best Practices 22
Chapter 6. Further Reading and Links 24
6.1. Useful Reading 24
6.2. Standards Documentation 24

Foreword

In October 2014, the ATM Software Security Committee released Version 3 of the ATM Software Security Best Practices Guide. Containing 127 pages, it provides an extremely in-depth analysis of software architectures, standards compliance, risks and mitigation factors relevant to ATM software and systems.

Cyber-attacks targeting ATMs and the systems that control them has become an ever important financial and reputational threat in many countries and regions. This document specifically focuses on actual criminal techniques known to have been perpetrated globally and identifies best practices that can be deployed to reduce the risk of such attacks being successful.

To combat fraud, it is imperative that all ATM deployers in all regions and countries take best practices very seriously, and implement all guidelines and best practices contained herein to the greatest extent possible.

Mike Lee, CEO ATMIA

April 2015

Executive Summary

Please note that this Executive Summary cannot replace reading the whole manual. The summary is merely a guide as to the content and main principles of these best practices.

The aim of this guide is to help ATMIA members identify and mitigate sophisticated attacks against ATMs from malware, black box electronics and other cyber-attack methods.

1. Over the last few years there has been an increase in reported incidents of ATM fraud involving malicious software (malware) running on ATMs, sophisticated electronic (black box) devices attached to ATMs, the hijacking of ATM control systems and the interception and modification of ATM transaction authorization messages (man-in-the-middle attacks).
2. A common purpose of ATM malware is to force the dispenser to deliver all or some of the cash held within the ATM. Other purposes include interception and storage of cardholder data and other sensitive information.
3. Black box electronics attached directly to an ATM can allow the perpetrator to exert control over the functioning of the ATM.
4. Black boxes designed to control the dispenser allow the perpetrator to dispense cash without the need to perform a transaction using a card and PIN.
5. If a perpetrator gains access to an organization's ATM control and authorization systems, the perpetrator has the potential to take full control of the system, including account balances and withdrawal limits; in addition, the perpetrator may be able to directly manipulate specific ATMs in the network.
6. ATMIA members concerned about ATM malware, black box and other cyber-attacks can adopt a range of best practices to help mitigate risk.

Acknowledgements

ATMIA is indebted to the individual contribution of the following experts:

Technical Editor: Douglas Russell, DFR Risk Management Ltd.

Contributor: Juan Jesus Leon Cobos, GMV

Contributor: Irmantas Brazaitis, Smart Card Security Ltd.

Finally, we wish to thank the original contributors to Version 3 of the Software Security Best Practices guide from which this document has evolved:

Henry Schwarz, Triton

Juan Jesus Leon Cobos, GMV

Irmantas Brazaitis, Smart Card Security Ltd.

Jim Tomaney, Q-ATM Ltd.

Douglas Russell, DFR Risk Management Ltd.

Chapter 1. Introduction

Over the last few years there has been an increase in reported incidents of ATM fraud involving the following:

- ATM Malware – malicious software running on ATMs
- Black Box Electronics – sophisticated electronic devices attached to ATMs
- Hijacking of Control Systems
- Man-In-The-Middle Attacks – the interception and modification of ATM transaction authorization messages

The primary objectives of such attacks include:

- Compromising data (including cardholder information);
- Forcing the ATM dispenser to deliver cash without the need to use a genuine card and PIN to perform a transaction (jackpotting and cash-out attacks); and
- Obtaining more cash than is debited from an account.

Attacks have been successful against various ATM models from different suppliers running different versions of ATM software and equipped with different levels of fraud protection solutions.

As a result of the increase in reported incidents, financial institutions have increased their awareness of cyber-attacks. In addition, the April 2014 end-of-life status for MS Windows XP, and the resulting discontinuation of security patches for the XP operating system (OS), has raised awareness of security issues. On a positive note, the increased awareness has encouraged knowledge and understanding of cyber-threats, thereby paving the way for better protection.

However, it should be noted that no published attacks to date have made use of OS vulnerabilities; therefore, no significant impact in the incidence of cyber-attacks due to XP end-of-life is expected in the short-term. This conclusion is supported by the following:

- Experience from NT end-of-life: no attacks that specifically exploited NT vulnerabilities took place; yet a considerable number of NT installations remained in the field after end-of-life, some of which are still in existence.
- Regular patching of an ATM OS is usually subject to extensive testing, which requires planning and time. Because timeframes for Microsoft patch releases and ATM software deployment vary, the ATM OS is typically behind the most current security patch level.

However, we also expect that risks due to OS vulnerabilities will gain importance in the future for two main reasons:

- While they were relatively uncommon and poorly organized at the time of NT end-of-life, cyber-attacks are now on the rise. We know that cyber-mafias are behind many attacks today. These organizations will likely consider all possible attack vectors that exist, and they have access to the technology required to create sophisticated exploits.
- Financial institutions are deploying new ATM cyber-security controls at a fast rate compared to just one year ago. As financial institutions address existing attack vectors, we expect that cyber-crime organizations will look for new ways to attack ATMs.

In summary, while unpatched ATMs may not be a large concern today, a mid-term strategy is necessary to handle these OS vulnerabilities.

It is difficult to predict exactly when OS-related vulnerabilities will become relevant. Such vulnerabilities require different attack approaches in order to bypass state-of-the-art ATM security controls. A new attack method based on exploiting OS unpatched processes will likely focus on gaining network access rather than physical access to the ATM. This would be a significant change in the attack method; however, the recent Carbanak case shows that such attacks are feasible (see Carbanak Case Study on page 20).

Possibly, the best approach for now is focusing on existing malware and black-box attacks as they are carried out today, while in parallel, implementing a risk management policy that addresses the ever-changing scenario that ATM security is facing.

The following chapters explain several reported ATM attack types, with examples based on real case studies from a range of different countries and regions.

Chapter 2. ATM Malware

2.1. Overview

This chapter explains the type of ATM malware attacks that have been identified globally, and highlights indicators that can be used to detect such attacks. As different ATM models have been targeted, this chapter is intended to be ATM vendor-independent, and is based on our knowledge of global attacks to date.

2.2. Malware Functionality

There are a growing number of variants in ATM malware with different levels of functionality. Common goals of ATM malware include:

- Force dispenser to deliver all or some of the cash within the ATM (jackpotting/cash-out);
- Intercept and store card data (full track data, magnetic-stripe data or equivalent on a chip);
- Intercept and store in-the-clear PINs or encrypted PIN blocks;
- Decrypt encrypted PIN blocks by exploiting an insecure encrypting PIN Pad (EPP);
- Intercept and store initial ATM encryption key values and subsequent key change values; and
- Intercept and store ATM administrative codes and passwords.

2.3. Malware Installation

We know that ATM malware is installed in different ways. Examples of how confirmed malware attacks have been perpetrated include:

- Boot or auto-run using a USB device or CD/DVD disk which installs the malware on the ATM hard drive;
- Boot using a USB device or CD/DVD disk containing an operating system and application that allows control of the ATM directly;
- Access the Windows desktop and install malware onto the ATM hard drive from the command line;
- Use a composite USB human interface and storage device to copy malware onto the ATM hard drive; and

- Download and install malware over the network following compromise of ATM control systems.

2.4. Accessing the ATM

With the exception of network compromise, malware installation requires physical access to place components within the ATM top box or cabinet, such as the ATM's PC core and internal communications subsystem. Perpetrators have achieved access by the following methods:

- Using a physical key (genuine or copy) to open the cabinet;
- Sabotaging or picking the lock to open the cabinet;
- Cutting a hole in the ATM fascia or cabinet;
- Inserting a device via the card reader slot to interface with USB connectors or solder points;
- Impersonating a service technician to obtain access to the cabinet; and
- ATM owners or service company staff acquiring malicious access to the ATM cabinet.

2.5. Execution of Malware

After perpetrators install the malware, they execute it using several methods, including:

- Using a specific ATM card to trigger the malware;
- Entering a specific sequence of numbers on the PIN Pad;
- Issuing commands via a mobile phone connection previously installed within the ATM; and
- Using switches (buttons) on a composite USB human interface and storage device.

2.6. Detection of Malware

Because characteristics vary between different types of malware, detecting the presence of malware during installation or after execution can be difficult and may require a thorough forensic examination of the ATM hardware and software. Some versions of malware are designed to securely delete themselves after a specific time period, or after execution, which can further impede an investigation. Indicators can include:

- ATM cabinet opened (alarm or auto supervisor state activated);
- ATM powered down then powered up when power supply is normally reliable;
- System reboots, including system escapes without a recognized cause or error condition being recorded in the ATM logs;

- Logs, including Windows event logs, missing from the ATM hard drive;
- Indication that anti-malware software was disabled, including whitelisting solutions;
- Malicious files with the same name as genuine files being present in incorrect directories on the ATM hard drive;
- Unexpected and unauthorized software updates being installed;
- Known malware files and signatures being present on the ATM hard drive; and
- Inspection of local ATM logs showing pick fails or other dispenser operational errors without corresponding host records of cash dispense transactions being authorized.

2.7. ATM Malware Case Study Examples

This section provides a summary of some of the known ATM malware variants that have been identified since 2008. This should not be considered to be an exhaustive list.

Where a particular malware name has been regularly used to describe the malware, it is mentioned for reference only; the actual executable may have a different name.

Some of the malware examples are updates or variants of previous versions, and are listed separately to highlight the time-line of how they have evolved.

2.7.1. Skimer-A

Discovery: 2008
First Location: Russia
Primary Purpose: Card and PIN compromise, cash dispense
Infection Method: Physical access, Windows desktop

Although there is some indication that the malware was created in 2007, the Skimer-A Trojan was first reported as being used to target ATMs in Russia in 2008. Variants were later detected in Ukraine and Europe.

Loading the malware requires physical access to the ATM cabinet via the Windows desktop. The malware then intercepts and stores card data and PIN information, as well as dispenses cash. It encrypts the compromised data and later prints the data using the ATM receipt printer, and possibly writes the data to a special ATM card.

Perpetrators activate the malware using a specific magnetic stripe card which, when entered, opens a window on the ATM screen with a list of options, including one to remove the malware from the ATM and another to print captured data. Another option opens an additional window and prompts the user to enter numbers on the PIN Pad. If specific numbers are entered, there is an option to dispense cash.

2.7.2. Unknown

Discovery: 2009
First Location: USA
Primary Purpose: Cash dispense
Infection Method: Bank employee

Malware permits withdrawals from selected ATMs without a link to a valid account.

2.7.3. Scrooge

Discovery: 2010
First Location: Black Hat Security Conference
Primary Purpose: Card and PIN compromise, cash dispense
Infection Method: Remote Administrator Network Connection and USB

The Scrooge root kit, created by the late Barnaby Jack, was demonstrated at the Black Hat security conference in 2010. Two different models of ATM were exploited: one via a dial-up remote administration network and the other by accessing a USB socket. Card, PIN and administrator information were compromised, and the ATMs were made to dispense cash (jackpotted).

2.7.4. Siberian Malware

Discovery: 2010
First Location: Russia
Primary Purpose: Account compromise
Infection Method: Bank employee loading malware on ATM systems

Siberian malware is capable of compromising consumer account details following ATM transactions. Perpetrators then transfer funds to another account.

2.7.5. Dump Memory Grabber

Discovery: 2013
First Location: USA
Primary Purpose: Card compromise (track 1 and track 2)
Infection Method: Likely insider

The malware scans memory of the infected ATM or Point of Sale (POS) device, then captures and stores card data in a text file. A POS variant of the malware uses file transfer protocol (FTP) or email to retrieve the compromised data.

2.7.6. Backdoor Ploutus

Discovery: 2013
First Location: Mexico
Primary Purpose: Cash dispense
Infection Method: CD/DVD drive

Perpetrators load Backdoor Ploutus on the ATM hard drive via a bootable CD/DVD drive then activate the malware by entering a specific set of numbers on the PIN Pad or via an external keyboard attached to the ATM. The numbers include the date of activation, which limits the timeframe to exploit the malware. If the numbers entered are valid, a graphical user interface displays in Spanish on the ATM screen, including an option to select how many notes to dispense.

2.7.7. Backdoor Ploutus, Version B/Ploutos

Discovery: 2013
First Location: Mexico
Primary Purpose: Cash dispense
Infection Method: CD/DVD drive

Perpetrators load Ploutus (B) on the ATM hard drive via a bootable CD/DVD Drive then activate the malware by entering a specific set of numbers on the PIN Pad. The numbers include the date of activation, which limits the timeframe to exploit the malware. If the numbers entered are valid, a window displays in English on the ATM screen displaying how much cash is available and logging activity as cash is dispensed. There is no option to select how many notes to dispense.

2.7.8. Trojan.Skimer.18

Discovery: 2013
First Location: Russia
Primary Purpose: Card and PIN compromise
Infection Method: Infected application

When Trojan Skimer 18 is present on an ATM, perpetrators can use a special chip card to activate the malware and cause a window to be displayed on the ATM screen that accepts input from the PIN Pad. Perpetrators also use the special chip card to store card and compromised PIN data.

2.7.9. Atmh4ck

Discovery: 2013
First Location: Chaos Communication Congress, Germany
Primary Purpose: Cash dispense
Infection Method: USB via cutting cabinet

German researchers (names withheld by request) demonstrated malware that is loaded by cutting a hole in an ATM cabinet to access a USB port and rebooting an ATM from their connected USB stick. A specific set of 12 numbers (000507607999) entered on the PIN Pad activated a menu window on a second desktop of the ATM screen displaying in Portuguese the quantity and value of notes (labelled R$, Brazilian Reals) in each cassette. A further set of 6 numbers was required to actually dispense cash based upon the concept of challenge and response, thus controlling the ability to exploit the malware.

Atmh4ck options included:

- Directing the dispenser to dispense cash,
- Clearing log files,
- Removing the malware from the ATM using a secure delete function, and
- Disabling ATM network adapters.

The malware demonstrated was reported as being based on malware recovered from genuine ATMs. The malware appeared to be specific to individually targeted ATMs, as the ATM hard drive volume serial number must match the specific customized malware.

2.7.10. Backdoor Ploutus, Version B/Ploutos (SMS)

Discovery: 2014
First Location: Unknown
Primary Purpose: Cash dispense
Infection Method: CD/DVD drive or USB device

Ploutus (B) is loaded via a bootable CD/DVD drive or USB device. Perpetrators activated the original version (2013) by entering a specific set of numbers on the PIN Pad. The updated version is activated by a Short Message Service (SMS) text message sent to a mobile phone tethered to a USB port. A second text message activates the cash dispense function.

2.7.11. Unknown

Discovery: 2014
First Location: Latin America
Primary Purpose: Cash dispense, Card and PIN compromise
Infection Method: USB device

In addition to dispensing cash and compromising card data and encrypted PIN blocks, the malware includes key logging of the maintenance keyboard. If the maintenance keyboard is used to enter initial Data Encryption Standard (DES) encryption keys, these keys, as well as subsequent host-initiated key changes, are compromised.

2.7.12. Backdoor.Padpin

Discovery: 2014
First Location: Russia, UK
Primary Purpose: Cash dispense
Infection Method: CD/DVD drive

Loaded by rebooting the ATM from the CD/DVD drive, this malware is copied onto the ATM hard disk and not prevented from running by certain whitelisting protection systems. The perpetrator activates cash dispense by inputting specific numbers on the PIN Pad. The malware can delete event logs and remove itself to hinder incident investigation. Although there are similarities to various Ploutus versions, Backdoor.Padpin is different malware.

2.7.13. Macau Malware

Discovery: 2014
First Location: Macau, Ukraine
Primary Purpose: Card and PIN compromise
Infection Method: USB interface via card reader slot

Believed to originate from Ukraine, Macau involves a sophisticated electronic device inserted via the card reader slot to make contact with USB solder points at the rear of the card reader. The composite USB device (both storage and human interface) copies malware onto the ATM hard drive. The malware collects card data and encrypted PIN blocks, which are then decrypted by exploiting an unprotected EPP on the ATM. Control chip cards are used to harvest card and PIN data and delete the malware.

2.7.14. Unknown

Discovery: 2014
First Location: Unknown
Primary Purpose: Cash dispense
Infection Method: Network compromise

Perpetrators install the malware on ATMs following external compromise of an ATM deployer's internal network. An unknown method is then used to initiate cash dispense. After the attack, the malware securely deletes itself to hinder forensic examination.

2.7.15. Backdoor.MSIL.Tyupkin

Discovery: 2014
First Location: Eastern Europe
Primary Purpose: Cash dispense
Infection Method: Bootable CD/DVD

Perpetrators install the Tyupkin malware using a bootable CD/DVD. Once installed on the ATM hard disk, the malware allows perpetrators to activate the cash dispense option by entering specific numbers on the ATM keyboard, followed by a specific session key to limit the exploit.

Activation is also restricted to specific times (Sundays and Mondays). In addition to providing a method to dispense cash, Tyupkin disables the ATM's local area network connection and a whitelisting anti-malware solution.

2.7.16. Trojan.Skimmer (New Variant)

Discovery: 2015
First Location: Eastern Europe
Primary Purpose: Cash dispense, Card and PIN Compromise
Infection Method: Unknown

A new variant of Trojan.Skimmer is capable of card data logging, cash dispense, communication key logging and keyboard logging. Believed to be activated by entering a specific chip card, the malware prompts for numerical input on the ATM's PIN Pad. The numerical input corresponds to different commands that instruct the malware to perform specific tasks.

Similar to other versions of ATM malware, this trojan uses challenge and response to verify that the user is authorised to perform advanced functions, such as to dispense cash. Many believe this level of functionality is an effective way to allow the malware originator or controller to limit who can use the malware.

Chapter 3. Black Box Attacks

3.1. Overview

Black box is the term commonly used to describe technically sophisticated electronic devices that are attached directly to an ATM to allow the perpetrator to exert control over ATM functions.

Black boxes that have been identified range from the simple to the sophisticated, including:

- Simple form factor devices with electronic input and output sockets,
- LED indicators,
- Rudimentary toggle switches, and
- Devices based on modified laptop computers, smartphones, and tablets.

3.2. Black Box Functionality

Some black boxes can intercept information, such as cardholder data, administrator codes, passwords and encryption keys; others can inject malware onto the ATM's hard drive.

The focus of this section is on black boxes that directly control ATM functions.

The most commonly targeted ATM module for black box attacks is the dispenser. Black boxes designed to control the dispenser allow the perpetrator to dispense cash without any need to perform a transaction using a card and PIN.

Black boxes that are designed to take control of a module, such as to direct the dispenser to dispense cash, are known to overcome basic obfuscation methods intended to protect messages between the genuine ATM core and the dispenser.

3.3. Attaching Black Box Devices

Perpetrators attach black box electronic devices directly to the dispenser electronics or indirectly via the ATMs internal communications sub-system. A black box can operate in association with the genuine ATM software, or can completely replace the genuine ATM software, which is, in effect, similar to replacing the genuine ATM's PC core with the perpetrator's system.

3.4. Accessing the ATM

To attach a black box, perpetrators require internal access to the electronics within the ATM cabinet or top box. We know that access has been achieved by:

- Using a physical key (genuine or copy) to open the cabinet,
- Sabotaging or picking the lock to open the cabinet,
- Cutting a hole in the ATM fascia or cabinet,
- Impersonating a service technician to obtain access to the cabinet,
- ATM owner or service company staff maliciously accessing the cabinet.

3.5. Executing Black Box Attacks

Typically, perpetrators execute black box attacks using switches or keyboard input on their own electronics rather than through the ATM card reader or keyboard. This can include commands issued remotely to a smartphone-enabled black box pre-installed and connected to the dispenser within a compromised ATM.

3.6. Detecting Black Box Attacks

As black box attacks on the dispenser effectively isolate the fraudulent activity from the transaction authorization and ATM monitoring systems, detecting attacks in progress can be difficult.

For attacks that involve physically opening the ATM cabinet or top box, it is possible to use alarms or, if the ATM is fitted with an auto-supervisor switch, to monitor for the ATM entering supervisor mode unexpectedly.

When the black box is designed to be connected directly to the dispenser or to be installed between the genuine ATM core and the dispenser module, it is sometimes possible to detect the dispenser being temporarily disconnected and disappearing from the list of active configured modules.

In some ATM architectures, disconnecting an active module, such as the dispenser, can cause the ATM to reset or system escape. However, some attacks overcome this detection indicator by simulating the continued presence of the dispenser within the compromised ATM.

The feasibility of using each of these indicators to act as a method of detection also depends on the ATM remaining powered on and in active communication with the remote monitoring system. To avoid detection methods, perpetrators will sometimes power down the ATM before beginning their attack.

Also, some black box electronics require the ATM to be powered off and on, or rebooted, before the perpetrator can use the black box to control the dispenser. For ATM environments with reliable power supplies and communications, an ATM disappearing from the network and restarting unexpectedly can be used as a potential detection method.

After a black box has been installed and either left in place for a future attack or used and subsequently removed, well trained staff and service personnel can inspect the ATM for evidence of foreign electronics or to determine if the internal cables have been disturbed. This can include unclipped or untied cables, rerouted cables and cables left with loose or unsecured connections to the ATM's internal communications subsystem.

When a black box attack has successfully dispensed cash from the ATM, the ATM will often not balance correctly with transaction records at the host. Inspection of ATM maintenance logs (stored locally on the ATM) can sometimes provide evidence that the dispenser has been activated.

However, it is not uncommon, particularly when a large number of notes are dispensed in a short time period, for operational problems to occur. For example, the dispenser may fail to pick some of the notes, and this may be recorded as an event in the ATM's maintenance logs. Correlating the date and time stamp of such events with the central transaction authorization records at the host can be used to determine that the dispenser was actively dispensing at a time when no actual transactions were being authorized.

Indicators for detecting that a black box attack is occurring or has occurred can include the following:

- ATM cabinet opened (alarm or auto supervisor state activated);
- Dispenser module removed from the list of available modules;
- ATM system reboot, including system escapes, indicating a module was disconnected;
- ATM powered down then powered up when power supply is normally reliable;
- Inspection reports of black boxes or foreign electronic devices within an ATM;
- Inspection reports that internal ATM communications cables were untied, rerouted or loose;
- Inspection of local ATM logs showing pick fails or other dispenser operational errors without corresponding host records of cash dispense transactions being authorized.

Chapter 4. Hijacking ATM Control and Authorization Systems

4.1. Overview

If a perpetrator gains access to an organization's ATM control and authorization systems, he can take full control of almost all ATM functions, including account balances and withdrawal limits, as well as manipulation of specific ATMs in the network.

4.2. Carbanak Case Study

Discovery: 2015
First Location: Russia and Ukraine
Primary Purpose: Control bank systems, cash dispense
Infection Method: Spear phishing email to bank employees

Publicly reported in 2015, Carbanak is believed to have originated in Russia in 2013. The malware allows network access, sophisticated espionage surveillance and control of internal bank systems.

The Carbanak malware itself does not have to be resident on an ATM, although perpetrators can download other malware to the ATMs. Carbanak compromises the ATM's control systems, including:

- Compromising encryption keys,
- Forcing ATMs to dispense cash without requiring card insertion or PIN, and
- Changing value (denomination) of notes inside the ATM.

Carbanak also allows access to cardholder accounting details, such as account balances, which can be artificially inflated to permit larger amounts of cash to be transferred to accounts under the control of the perpetrator.

According to reports, multiple banks in multiple countries have been targeted.

4.3. Man-in-the-Middle Case Study

Discovery: 2015
First Location: Mexico
Primary Purpose: Dispense more than account debited
Infection Method: Malware on authorization system

During a cash dispense transaction, the ATM will normally send a request to the host, requesting authorization for the amount of cash requested. If the host approves, it will authorize the transaction and the ATM will dispense the amount approved.

The Man-in-the-Middle malware on banks' systems can intercept the authorization approval being sent from the host to the ATM and modify the amount approved to a higher value. The ATM dispenses the higher value, but the account is debited by only the amount actually authorized by the host.

A variant of this type of malware can simulate the host and approve transactions without the knowledge of the host (host substitution or simulation), and thus no account is debited for the amount dispensed.

Chapter 5. Best Practices

5.1. Mitigation Best Practices

We encourage ATMIA members concerned about ATM malware, black box and other cyber-attacks to consider the following mitigation best practices:

- Train staff and service personnel to be vigilant in detecting any changes to the ATM which may indicate that unauthorized access to the ATM cabinet has occurred, including:
    - Inspection for holes cut in the fascia,
    - Damaged locks, and
    - Out-of-place internal cables.
- Engage ATM solution providers and other specialists for guidance on installing and correctly configuring any applicable hardware, firmware or software to detect and prevent malware and black box attacks.
- Ensure ATMs and all related systems comply with the latest PCI standards where applicable.
- Perform a risk assessment of the entire ATM estate, recognizing that different ATMs, even of the same model, can have different levels of software and firmware installed or configured.
- Ensure that firewalls and anti-malware protection are correctly configured, including whitelisting solutions that cannot be disabled without generating a remotely monitored alert and audit trail.
- Use a golden image disk known to be free of malware to deploy locked-down whitelisting. This will avoid the possibility of introducing malware that may already be present on other whitelisted ATMs.
- Prevent unauthorized USB devices from being installed (USB whitelisting).
- Deploy full hard disk encryption (FHDE) and encryption and authentication solutions to protect internal communications between the genuine ATM PC core and ATM modules, including the dispenser.
- Disable in BIOS the ability to boot or auto-run software from USB sticks and CD/DVD drives.

- Set and maintain strong BIOS password protection to prevent settings from being changed without correct authorization.
- Disable access to the Windows desktop at the ATM, and maintain a robust password management policy.
- Implement secure remote key loading for ATM encryption keys, and prevent the entering of encryption keys via the ATM supervisor or administrator keyboard.
- Enhance the physical security of the ATM cabinet or top box, including the use of high security locks, keys and alarm systems.
- Effectively monitor the operation of ATMs, paying special attention to unusual patterns of power outages, resets, communication failures and an uncharacteristic low number of transactions at normally high transacting ATMs.
- Implement strong encryption between the ATM and the host.
- Enable message authentication codes (MAC) to protect the integrity of messages between the ATM and the host.
- Monitor closed circuit television (CCTV) coverage of the ATM location for unusual activity at and around the ATM.
- Ensure access to the ATM cabinet is restricted to verifiably authorized persons and that such access is electronically logged.
- Educate staff regarding the dangers of inadvertently introducing malware into the enterprise's systems.
- Maintain a physically and logically secure environment across the organization.
- Monitor intelligence reports regarding new and emerging threats.
- Report instances (including failed attempts) to defraud or compromise systems to the appropriate law enforcement and regulatory authorities.

Chapter 6. Further Reading and Links

6.1. Useful Reading

PCI SSC Data Security Standards Overview:
https://www.pcisecuritystandards.org/security_standards/index.php

ATMIA Best Practices:
https://www.atmia.com/best-practices/

ATMIA alerts:
https://www.atmia.com/education/security/fraud-alerts/

ATMsecurity.com reports of ATM Malware:
http://www.atmsecurity.com/index.php?searchword=atm+malware&ordering=newest&searchphrase=exact&limit=0&option=com_search

6.2. Standards Documentation

PCI standards documentation can be found at the following link:
https://www.pcisecuritystandards.org

- Data Security Standard (PCI DSS)
- Payment Application Data Security Standard (PA-DSS)
- PIN Transaction Security (PCI PTS) – formerly known as PIN Entry Device (PCI PED)