census

IT SECURITY RESEARCH, DEVELOPMENT AND SERVICES

# Attacking the Traveling Salesman

## Point-of-sale attacks on airline travelers

DEFCON 2014


Alex Zacharis

Nikos Tsagkarakis

info@census-labs.com

Census S.A.

http://census-labs.com/

# Contents

- Why target travelers?
- Point-of-Sale attacks in transportation
- Case Study
- Back to the Lab
- POS: exploiting different modules
  - Cameras everywhere
  - Scan that QR
  - RAM scrapping
- TS POS Malware
- Aztec Revenge Tool

# Why target travelers?

- The need for communication is greater than privacy and/or security
- The *unknown Internet access* landscape forces you to trust what you normally wouldn't
- WiFi:
  - Login to (corporate) email accounts
  - Login to social networks
- Carry mobile phones, tablets, laptops ,usually all on at the same time ;)
- No second thoughts about public Internet hotspots

# Point-of-Sale attacks in Transportation

Unlike traditional POS attacks in Commerce (ex. Target Incident):

- Credit card details
- Web credentials

We target International Travelers' information:

- Name
- Picture
- Flight number
- Destination
- Seat number
- Communication partners
- Other….

# How is the POS introduced

As in every known POS Attack (Retail, Healthcare, etc):

1. **The system may have unpatched vulnerabilities**
2. An employee of the victim company may introduce it by mistake (opening an email attachment containing malware)
3. The source might even be an employee looking to cause trouble.

# POS attack outcome

Who benefits?

- Cyber Criminals (Identity theft)
- Private Investigators (spying)
- Government Agencies (spying)

After a successful attack we can achieve:

- Travelers “profiling” without authorized access to Airport Data
- With enough data collected we can categorize travelers per:
    - **Destination** (ex. Who travelled from Greece to Germany in the last month)
    - **Company** (ex. All Aegean passengers)
    - **Class** (ex. Who is travelling 1rst class OR Business)
    - **Flight/Date** (ex. All passengers of a specific flight)
    - Combination of the above

# POS Systems Present

**What are the possible POS Systems of interest?**

- Check-in kiosks
- **Purchase WiFi time kiosks**
- Internet Access Points (Terminals)
- Luggage Locator kiosks

# Case Study: An International Airport in Greece

| TRAFFIC HIGHLIGHTS | | |
|---|---|---|
| TRAFFIC HIGHLIGHTS | 2011 | 2012 |
| **Total Number of Passengers (million)** | **14.4** | **12.9** |
| Domestic | 4.9 | 4.5 |
| International | 9.5 | 8.4 |
| Business Passengers | 30% | 30% |
| Connecting Passengers | 22% | 23% |

**January-March 2014**, Passenger traffic reached 2.4 million

**Lets talk numbers (rough estimation):**

**Estimated travelers per year:** 12 million

**Business Passengers (30%):** 3,6 million

**Business Passengers Using POS (1%): 36000**

# Purchase WiFi time kiosks

- Buy extra WiFi time

  (accepts coins and bills, gives change)
- Check flight details (Barcode/QR scanner)
- Make Internet phone calls (VOIP) (Webcam available)
- **Placement:** 6 in number located in high accessible location throughout the airport

# Kiosk Services: Buy Wifi

# Kiosk Services: VOIP calls

# Purchase WiFi time kiosks: Attack

- Escape interface and expose machine details:
  - OS: Windows 7
  - No antivirus
  - Internet Connection
  - Administrative modules (proxy)
- USB enabled
  - Useful for installing homemade POS malware direclty

# The ALT+TAB attack ;)

- Escaping the restrictive POS Interface
- Keyboard input sanitization failure
  - Left Alt + tab -> locked
  - Right Alt + tab -> works!!!

# USB Port accessible

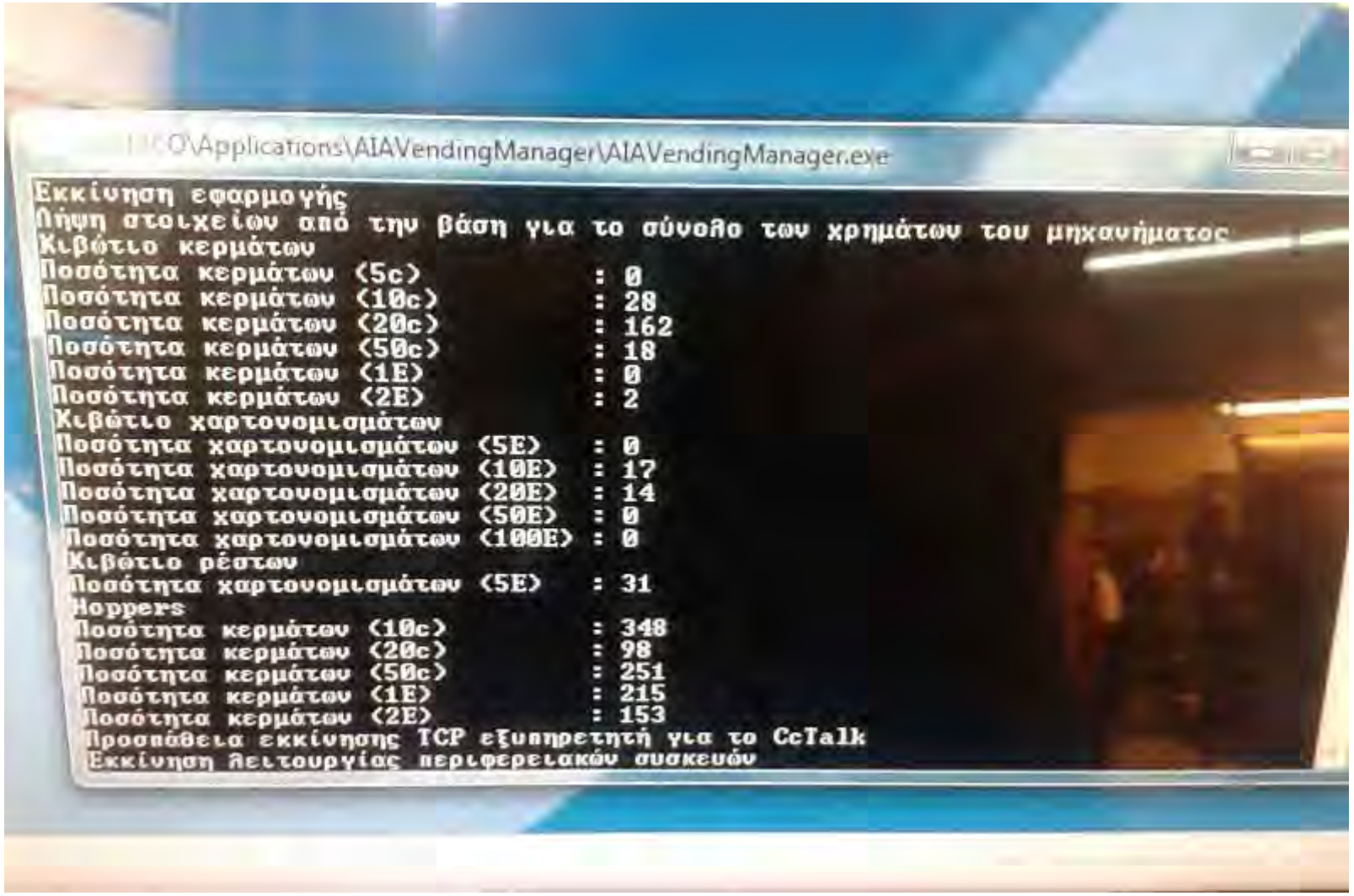
**USB port exposed/active**

# Exposing administrative modules

- Bad sanitization of user input from keyboard
- Basic Windows commands can be issued from keyboard in order to switch view to administrative interface
- Administrative interface enabled with full privileges directly issuing hardware commands
  - Like for example the **PAY command ;)**
  - **Other Commands:**
    - **Status**
    - **Start/Stop**
    - **Set Override**

# Admin interface #1

# Admin interface #2




**TOTAL: 736 Euros in coins**

# Admin interface #3


**Paying Ourselves Through Admin Module**

# Informing the Airport

**March, 2014**

- Presentation of the attacks to Administration, IT and Security team of the Airport.
- **Real life example:** Cashing out Money!
- **A month later**

The ALT+TAB bug was fixed and the USB port was protected.

**USB port Secured**

**BUT** the System was still vulnerable after the patch…

# New attack Vectors

Looking for new attack vectors to make the system crash and expose the underlying admin interface…

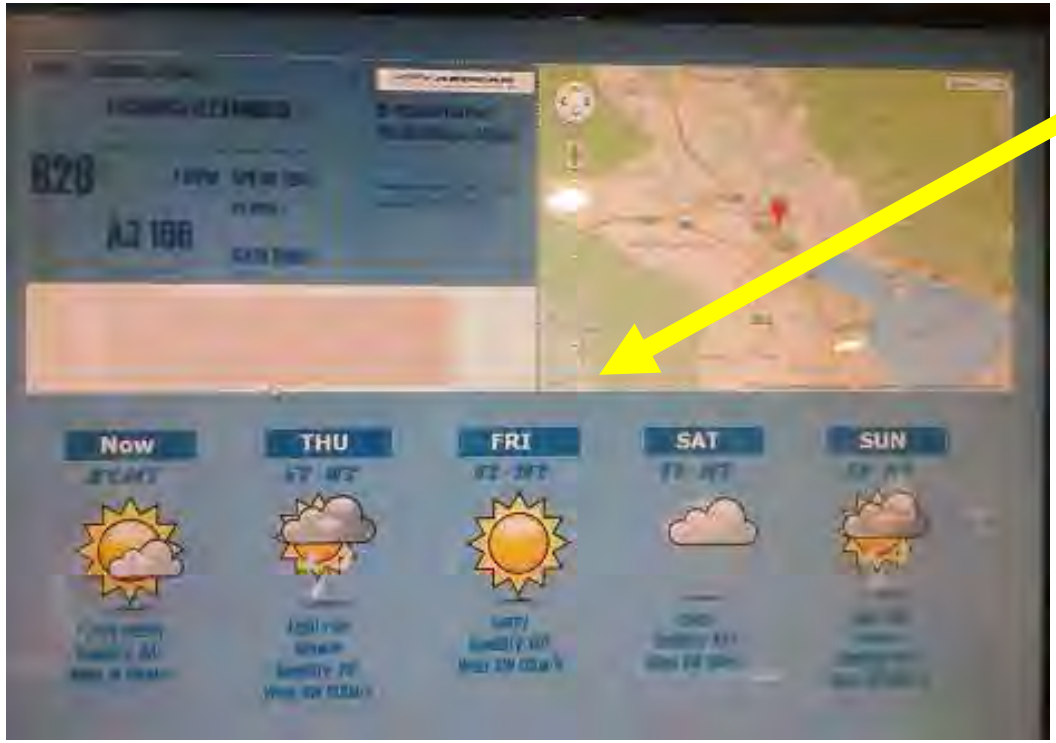
But how?

-Full Interface Testing

-Barcode Fuzzing  (We need a Tool)

# Interface Testing

- Exposing The Administrative interface by causing the app to try to connect to the Internet.
- A Pop Up connection blocker causes the interface to expose the minimized Admin Interface Window.

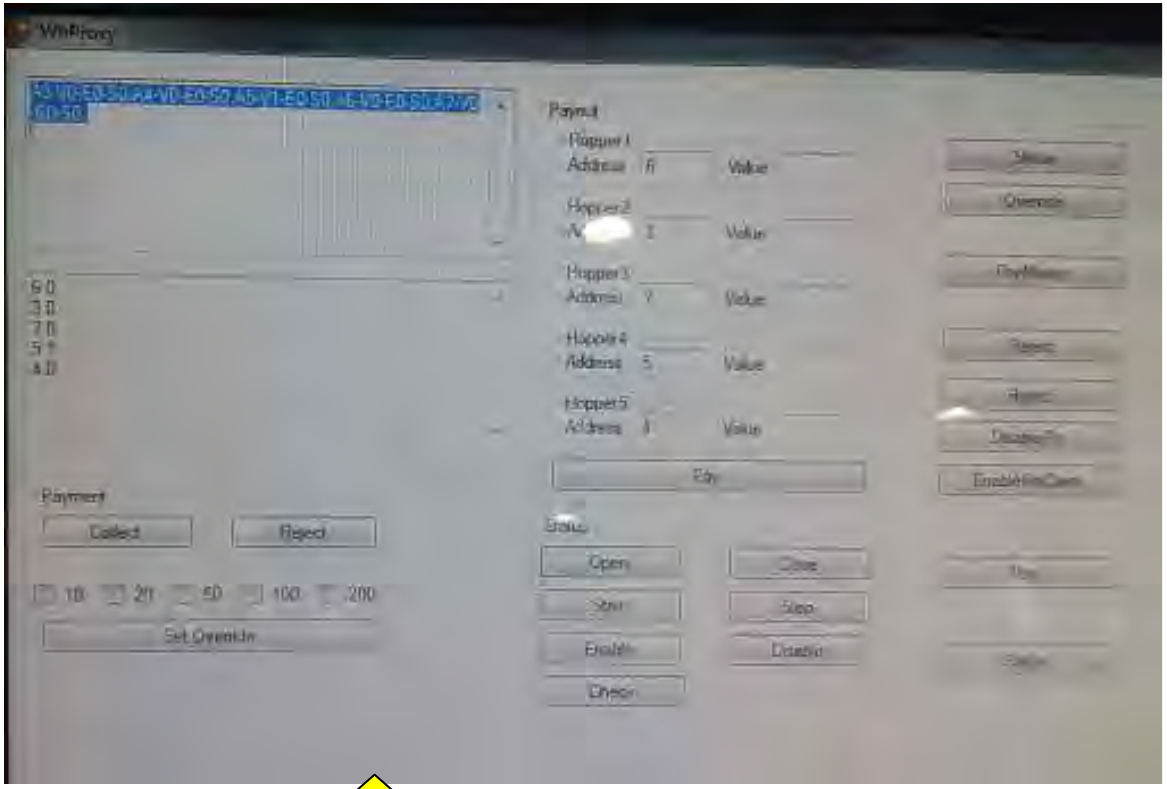




**Click causing popup action**

# Admin Interface Exposed


Focus Loss




Admin process running

Exposed Minimized Window

# Back to the Lab

**The Need:**

**Develop a malware to install in the kiosk that:**

- Exploits the WebCam Module
- Has RAM scrapping functionality
  - Get  scanned e-ticket details
- Receives Bar Code Commands

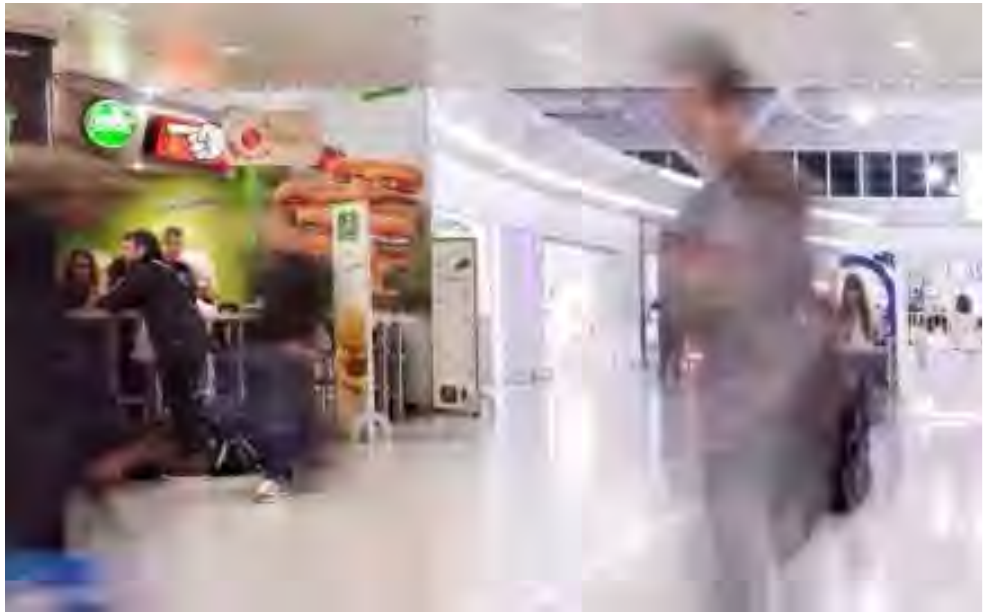
**Develop a tool that:**

- Fuzzes the barcode scanner to expose errors.
- Provide commands to our malware.

**Outcome:**

- **Inspiration for the Travelers Spy (TS) POS malware**
- **Creation of the Aztec Revenge Tool (Android Mobile App)**

# Camera Module Exploitation



WHY?

1. “Eyes” inside the Airport.

   (Multiple Spots, Requires Connect Back)

2. Capture Users Facial Image without consent during ticket scan event. (“full profiling”)

# Barcode Scanner + Privacy Issues

- Barcode scans e-tickets and retrieves travelers details
- Doesn’t log scans
- Scanned barcode info decoded and present in RAM
- Network calls containing travelers information
- Ticket formats tested:

  **BCBP (bar-coded boarding pass)**

  **Aztec (popular with E-tickets)**


# BCBP Code Technical Info

- General Info
  - **B**ar **C**oded **B**oarding **P**ass
  - IATA, 2005
  - Used by more than 200 airlines (36 use mobile)
  - In Paper: **PDF417**
  - Digital: **Aztec code**, Datamatrix and QR code

# PDF417 Technical Info

- Portable Data File,1991
- ISO standard 15438
- **417** each pattern consists of **4**

bars and spaces, each pattern is **17** units long.

- Linear barcode
- Use in:
  - Transportation
  - Identification cards
  - Inventory management

# BCBP (PDF417) Code Decoded Info

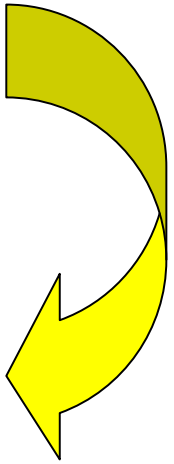
**RAW DATA:**
**M1ZACHARIS/ALEXANDROS E5YBG6J ATHIOAA3 0166 136Y020D0025 147>218 W B 29**

**M1:** Format code ‘M’ and 1 leg on the boarding pass.
**ZACHARIS/ALEXANDROS:** Passenger Name.
**E5YBG6J :** My booking reference.
**ATHIOAA3 :** Flying from ATH (Athens) to IOA (Ioannina) on A3 (Airplane Company: Aegean)
**0166 :** Flight number 166.
**136:** The Julian date.
**Y:** Cabin – Economy in this case. Others including F (First) and J (Business).
**020D:** Passengers seat.
**0025:** Sequence number. In this case passenger was the 25th person to check-in.
**147:** Field size of airline specific data message.
**>:**Beginning of the version number
**2:** The version number.
**18:** Field size of another variable field.
**W**: check-in source.
**B:** Airline designator of boarding pass issuer.
**29:** Airline specific data

# Aztec Code Technical Info

- 2D barcode, 1995
- ISO/IEC 24778:2008
- 1914 bytes of data encoded
- Use in transportation, especially E-tickets
- Present in Mobile Phones, handheld devices.

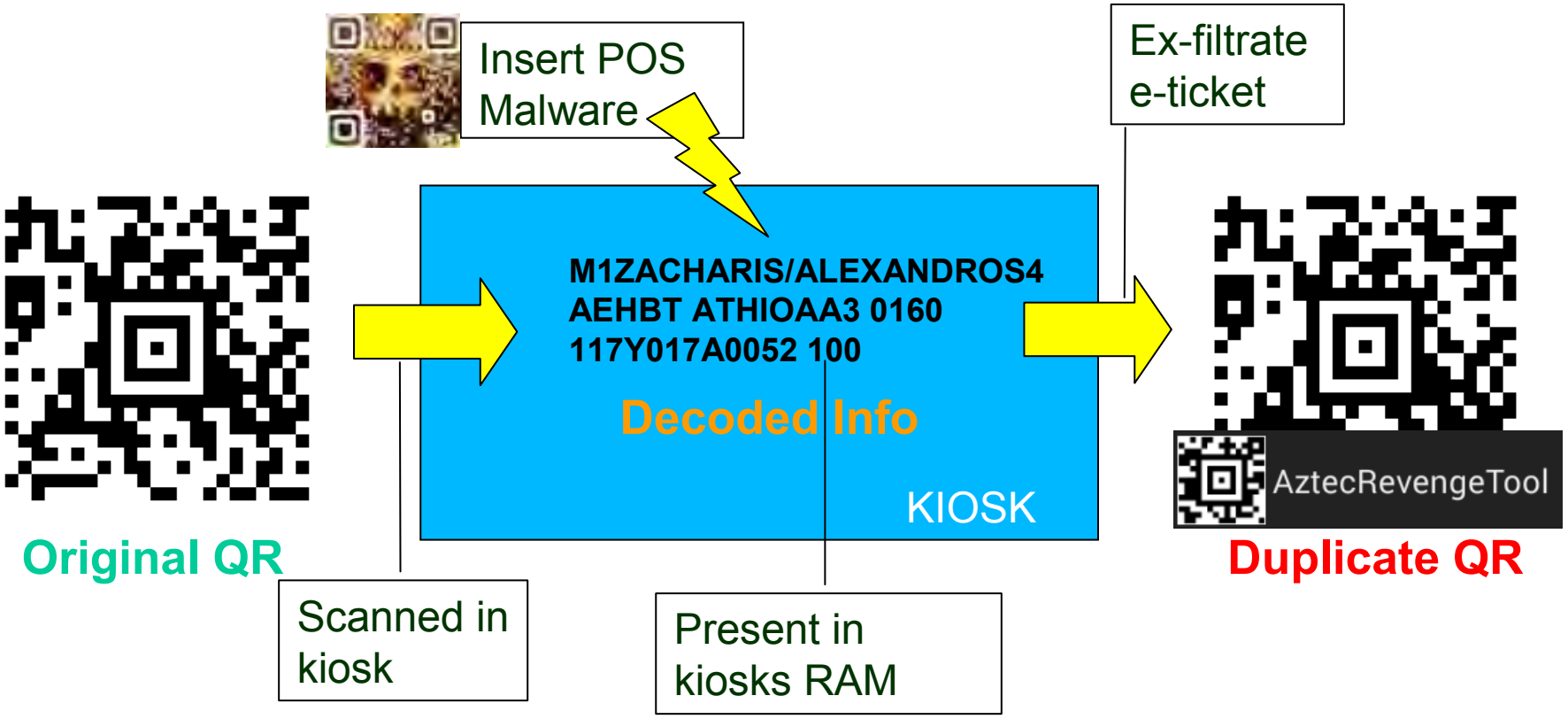
# BCBP Aztec Code Decoded Info



**M1ZACHARIS/ALEXANDROS4AEHBT ATHIOAA3 0160 117Y017A0052 100**

**M1:** Format code ‘M’ and 1 leg on the boarding pass.
**ZACHARIS/ALEXANDROS:** Passenger Name.
**4AEHBT:** My booking reference.
**ATHIOAA3:** Flying from ATH (Athens) to IOA (Ioannina) on A3 (Airplane Company: Aegean)
**0160:** Flight number 160.
**117:** The Julian date. In this case 117 is April 27.
**Y:** Cabin – Economy in this case. Others including F (First) and J (Business).
**017A:** Passengers seat.
**0052:** Sequence number. In this case passenger was the 52th person to check-in.
**100:** Field size of airline specific data message.

# Attack: Duplicate E-Ticket




- We need a tool to ex-filtrate e-tickets. (TS POS Malware)
- We need a tool for fast e-ticket duplication after we retrieve the data for the hacked machine (AztecRevengeTool)
- Use the cloned e-ticket to **impersonate** someone else and gain access to the Tax Free area of the Airport.

# TS POS Malware

# Travelers Spy (TS) POS malware

Based on our Use Case TS-POS malware should feature the following capabilities:

- Running on background
- Perform Ram Scrapping to identify E-tickets Already Scanned.
- On E-ticket scan event, Captures Image through Webcam
- Hook on Barcode Scanner Process  (if possible)
- Receive Commands through Aztec Code images when proper format bits are encoded in the image.
- Connect Back if Internet connectivity available.

# Image Capturing in action

- Hooking Barcode Scanner in order to trigger the image Capture in Time.
- Naming the image with a Time Stamp.
- Feature is disabled by default due to major drawbacks.

Problems:

- Timing the image capture
- Correlating Images with Travelers Data
- Large number of files, **Detectable**

# RAM Scrapping in action

RAM Scrapping Functionality:

1. Extract RAM of Barcode Scanner Proc
    - Map Interesting processes, Target the browser Process too!
    - Do it periodically (every two hours)
    - Windows API, **ReadProcessMemory function**
2. Search
    - String Identifiers (Unique Start, Stop Values, Fixed Size), Regular Expressions
    - Candidate Data (Store if not sure)
3. Exfiltrate Information
    - Is Internet Connection Available? (In our case yes)
    - If not? (Store Locally)

# RAM Scrapping example

1. **Dumping process memory with volatility:**

volatility-2.3.1.standalone.exe -f "Clean Xp-b71adf32.vmem" -p 980 memdump -D memory/

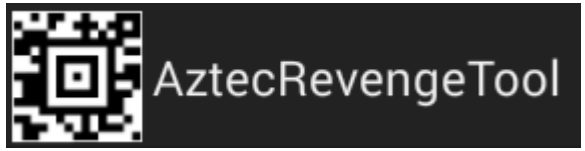
**2. Using Wingrep to locate scanned e-ticket (multiple hits):**

*20438: yyyyyyBBu OT5Barcode*
*1AyyyyyyOOu \6T5==========*
*==========Hyyyyyy\\u iyT5**M1ZACHARIS/ALEXANDROS E5YBG6J ATHIOAA3 0166 136Y020D0025 147>218 W B 29***
*hyyyyyyyiiu vT5 OdPdyaga*

**3. Storing Unique Values (Discarding Duplicates)**

# Aztec Code Command Set

- Why Use?
  - Important mainly for exfiltration reasons in case of no internet connection.
    - Ask malware to present specific data
    - Stop/Start extra functionality (image capturing)
  - Issue network scan commands to further infiltrate/pentest the network




# Aztec Revenge Tool

# Aztec commands from your phone (Aztec Revenge Tool)

**PoC Android Mobile**

**Supports:** PDF417, Aztec Code

**3 Modes of Operation:**

- E-ticket Duplicator Mode
- PENTEST Mode (Fuzzer)
  - Converts SQLi and web service payloads to Aztec Code images trying to fuzz Barcode scanners
- MALWARE COMMAND Mode
  - If our malware is already installed sends commands via Aztec Code images

# E-ticket Duplicator Mode

- Why Duplicate a retrieved  E-ticket:
  - Impersonation
  - Use it as basis to fuzz parameters expected by the system.
- How it works:

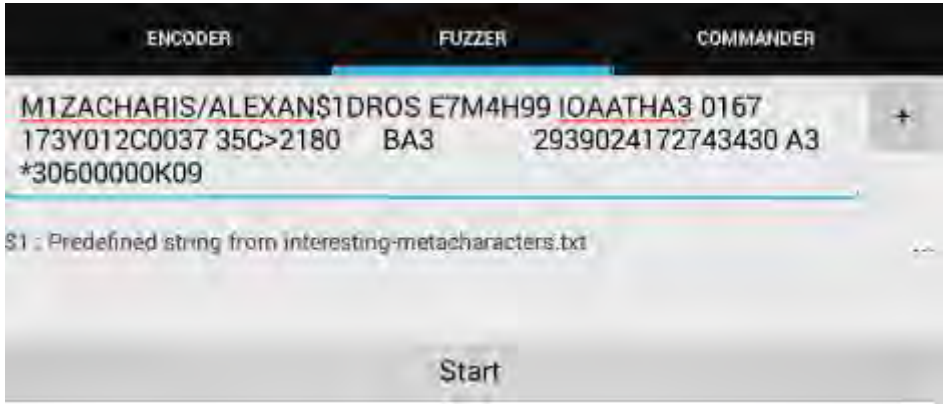
  Scans An image of the ticket in real time and decodes the content

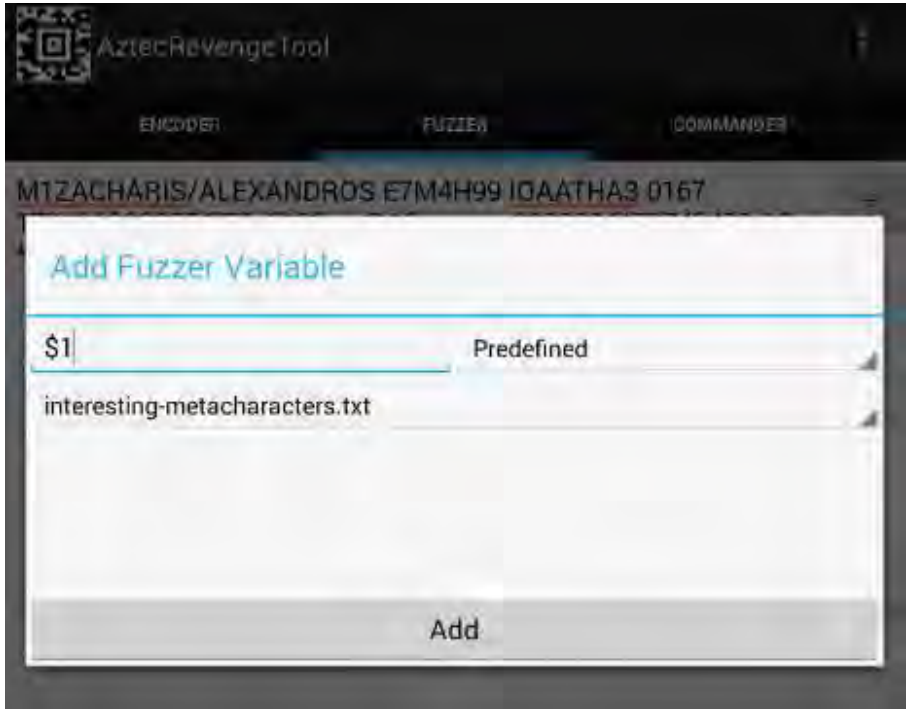
# Duplicating in Action

# Pentest Mode (Fuzzing)

- Fuzzing E-Ticket or other Barcode Scanners
- Fuzz Formats Supported:
  - String
  - Integer
  - Random String
  - Predefined (Sqli, Xss)
- Example Use (Airport):

  **E–CheckIn Device**

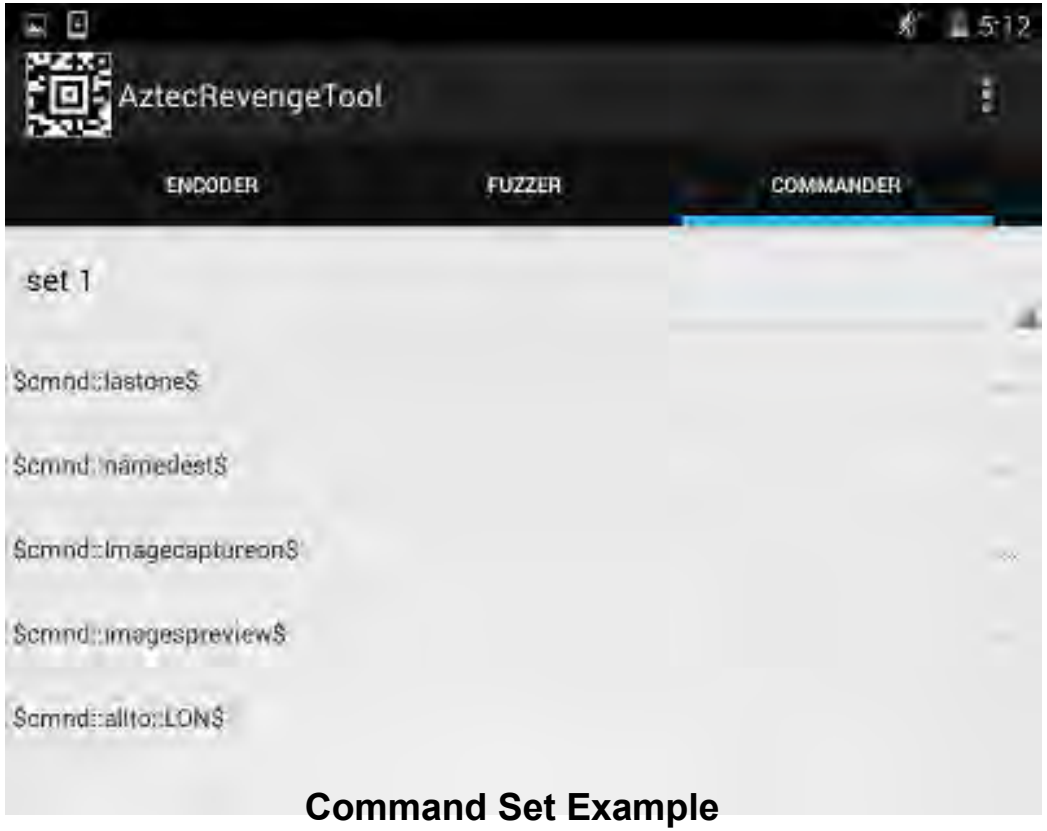


# Fuzzing in Action


# Command Mode

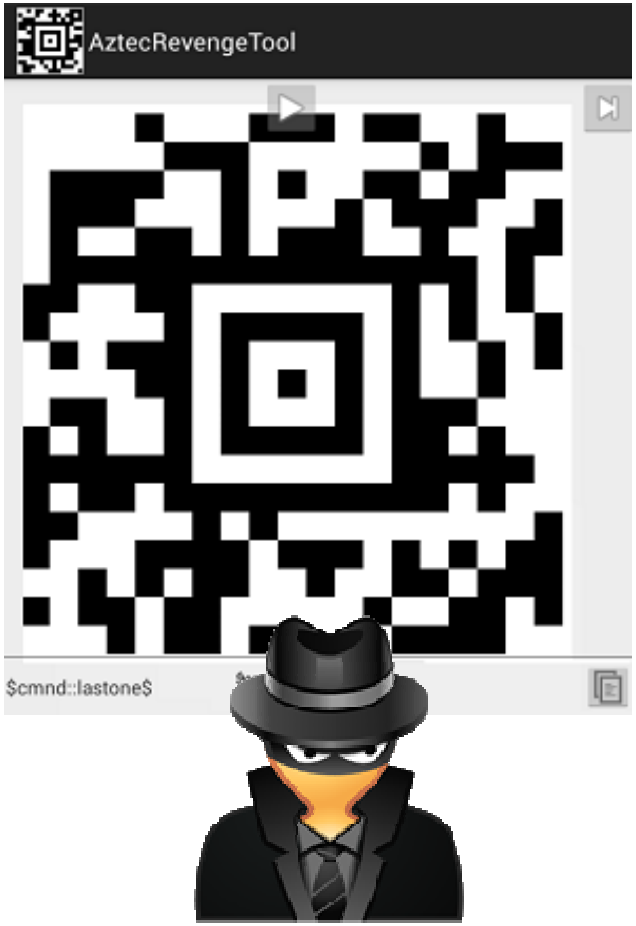
- Useful when no internet connectivity available
  - Dump RAM Captures
- Issuing Commands (Ex. Spy on a specific traveler or group)
- Perform Network Scan
- Image Capturing
- Cash Out Money




**Command Set Example**

# Combined Attack

**“LAST SCANNED TICKET” Command**





**TS POS Malware Retrieves/Prints Data on Screen**

# Conclusion

Recommendations:

1. Use strong passwords to access POS devices
2. Keep POS software up to date
3. Use firewalls to isolate the POS production network from other networks or the Internet
4. Employ antivirus tools
5. Limit access to the Internet from the production network
6. Disable all remote access to POS systems
7. Check software and hardware of POS as a whole, to discover more bugs that can be used in the exploitation process

# Questions?

census

IT SECURITY RESEARCH, DEVELOPMENT AND SERVICES


info@census-labs.com
Census S.A.
http://census-labs.com