



Attacking the Traveling Salesman

Point-of-sale attacks on airline travelers

DEFCON 2014



Contents

- Why target travelers?
- Point-of-Sale attacks in transportation
- Back to the Lab
- POS: exploiting QR Scanners
- 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.



Case Study

Purchase WiFi time kiosks

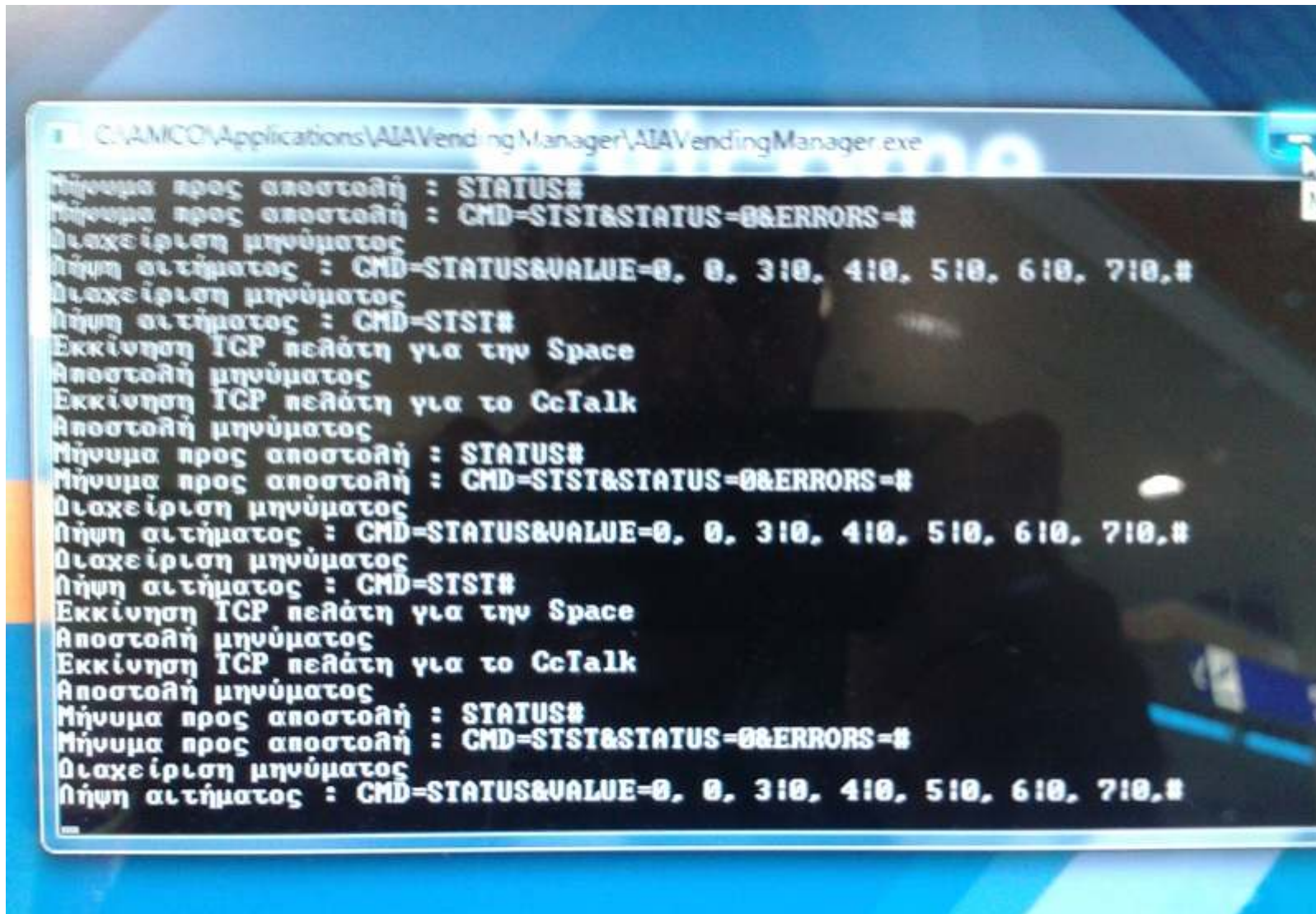
- Buy extra WiFi time (accepts coins and bills, gives change)
- Check flight details (Barcode/QR scanner)
- Make Internet phone calls (VOIP) (Webcam available)
- **Placement:** 6 in number located in high accessible location throughout the airport



Exposing administrative modules

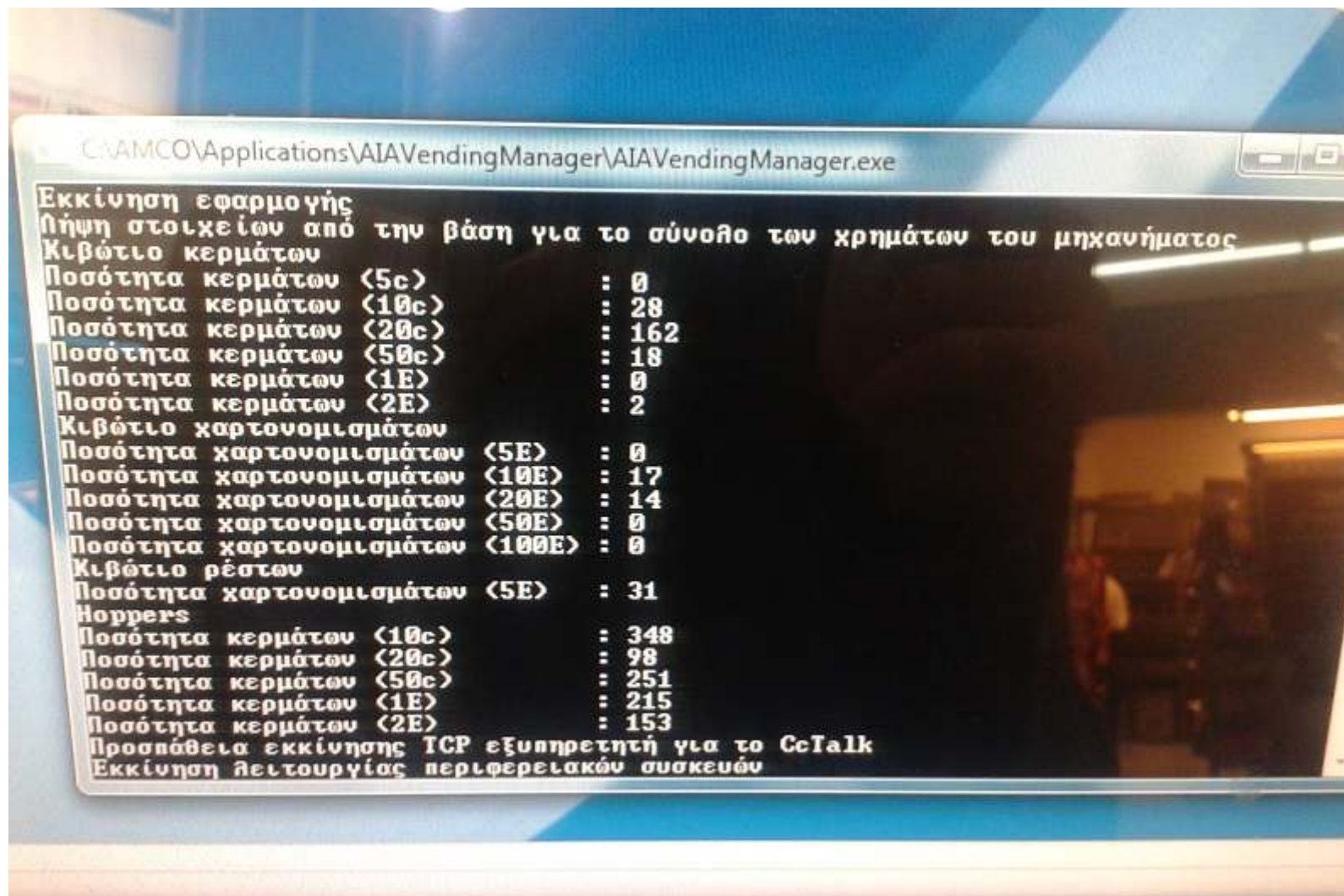
- Bad sanitization of user input
- Basic Windows commands can be issued from keyboard in order to switch view to administrative interface
- Administrative interface enabled with full privileges directly issuing hardware commands
 - Like for example the **PAY command ;)**
 - **Other Commands:**
 - **Status**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

Admin interface #1



```
C:\AMCC\Applications\AIAVendingManager\AIAVendingManager.exe
Μήνυμα προς αποστολή : STATUS#
Μήνυμα προς αποστολή : CMD=STST&STATUS=0&ERRORS=#
Διαχείριση μηνύματος
Αήψη αιτήματος : CMD=STATUS&VALUE=0, 0, 310, 410, 510, 610, 710,#
Διαχείριση μηνύματος
Αήψη αιτήματος : CMD=STST#
Εκκίνηση TCP πελάτη για την Space
Αποστολή μηνύματος
Εκκίνηση TCP πελάτη για το CcTalk
Αποστολή μηνύματος
Μήνυμα προς αποστολή : STATUS#
Μήνυμα προς αποστολή : CMD=STST&STATUS=0&ERRORS=#
Διαχείριση μηνύματος
Αήψη αιτήματος : CMD=STATUS&VALUE=0, 0, 310, 410, 510, 610, 710,#
Διαχείριση μηνύματος
Αήψη αιτήματος : CMD=STST#
Εκκίνηση TCP πελάτη για την Space
Αποστολή μηνύματος
Εκκίνηση TCP πελάτη για το CcTalk
Αποστολή μηνύματος
Μήνυμα προς αποστολή : STATUS#
Μήνυμα προς αποστολή : CMD=STST&STATUS=0&ERRORS=#
Διαχείριση μηνύματος
Αήψη αιτήματος : CMD=STATUS&VALUE=0, 0, 310, 410, 510, 610, 710,#
```

Admin interface #2



TOTAL: 736 Euros in coins

Admin interface #3



Paying Ourselves Through Admin Module

New attack Vectors

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

But how?

-Barcode Fuzzing (We need a Tool)



Back to the Lab

Back to the Lab

The Need:

Develop a malware to install in the kiosk that:

- 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)**

BCBP Code Technical Info

- General Info
 - **Bar Coded Boarding Pass**
 - IATA, 2005
 - Used by more than 200 airlines (36 use mobile)
 - In Paper: **PDF417**
 - Digital: **Aztec code**, Datamatrix and QR code



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

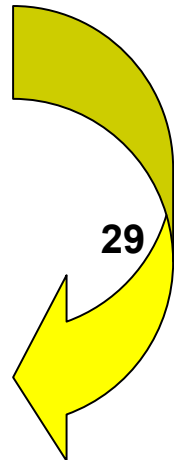
2: The version number.

18: Field size of another variable field.

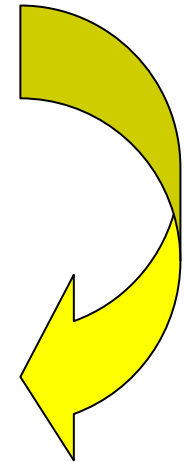
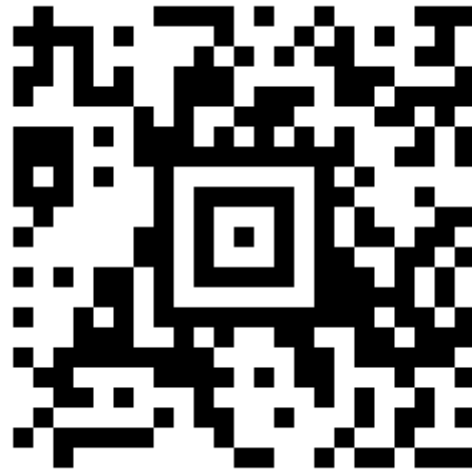
W: check-in source.

B: Airline designator of boarding pass issuer.

29: Airline specific data



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.

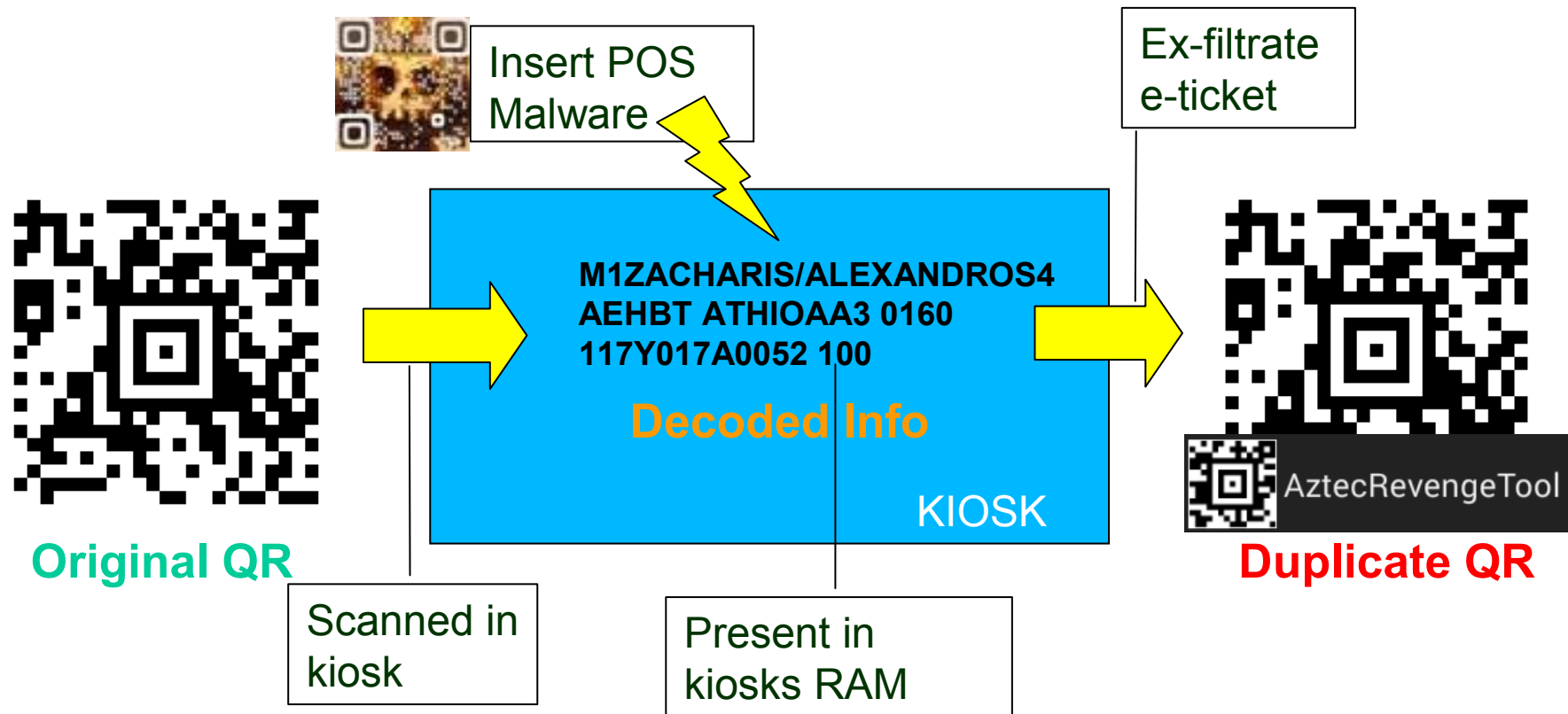
Y: Cabin – Economy in this case. Others including F (First) and J (Business).

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.

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

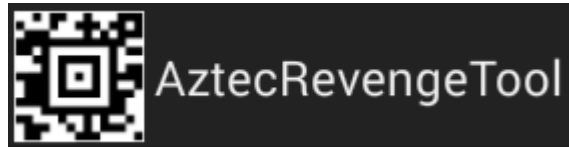
1. Dumping process memory with volatility:

```
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 iyT5M1ZACHARIS/ALEXANDRO  
S E5YBG6J ATHIOAA3 0166 136Y020D0025 147>218 W B 29  
hyyyyyyiu vT5 OdPdyaga
```

3. Storing Unique Values (Discarding Duplicates)



Aztec Revenge Tool

Aztec commands from your phone (Aztec Revenge Tool)

PoC Android Mobile

Supports: PDF417, Aztec Code

3 Modes of Operation:

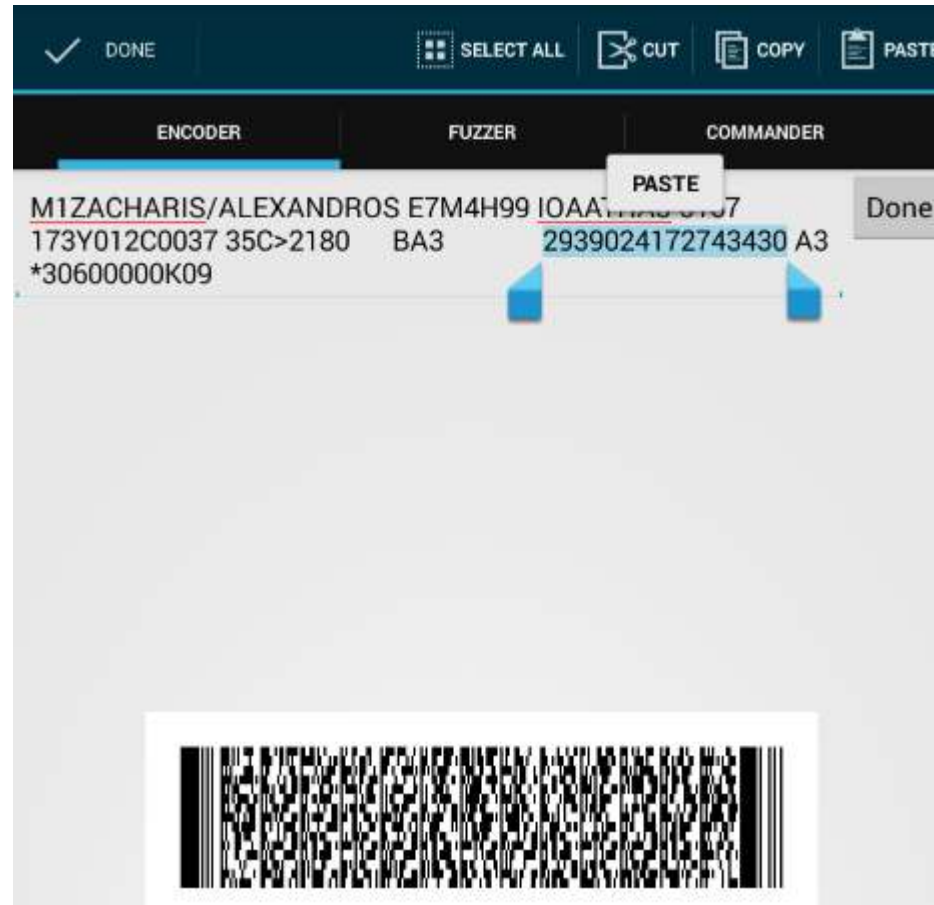
- E-ticket Duplicator Mode
- PENTEST Mode (Fuzzer)
 - Converts SQLi and web service payloads to Aztec Code images trying to fuzz Barcode scanners
- MALWARE COMMAND Mode
 - If our malware is already installed sends commands via Aztec Code images

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

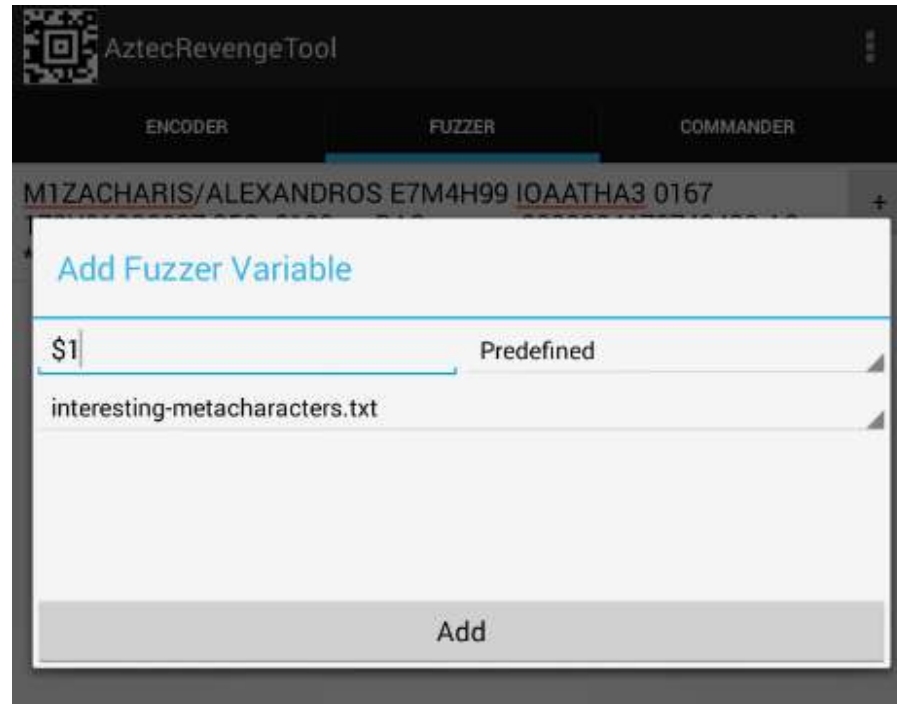
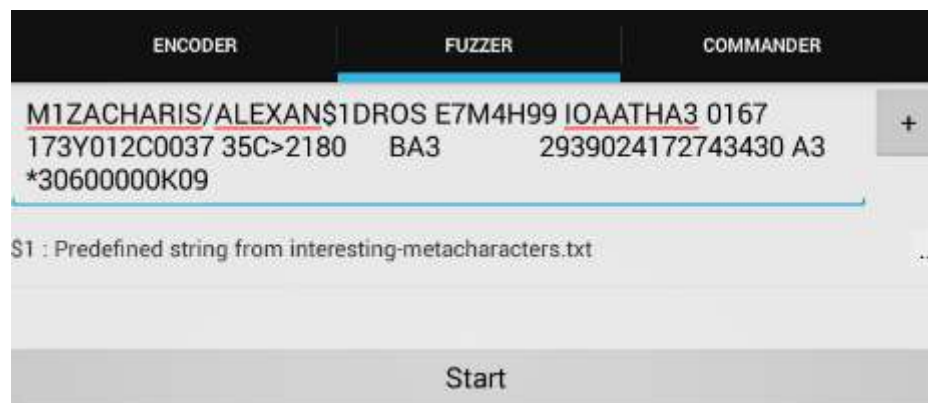


Duplicating in Action



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

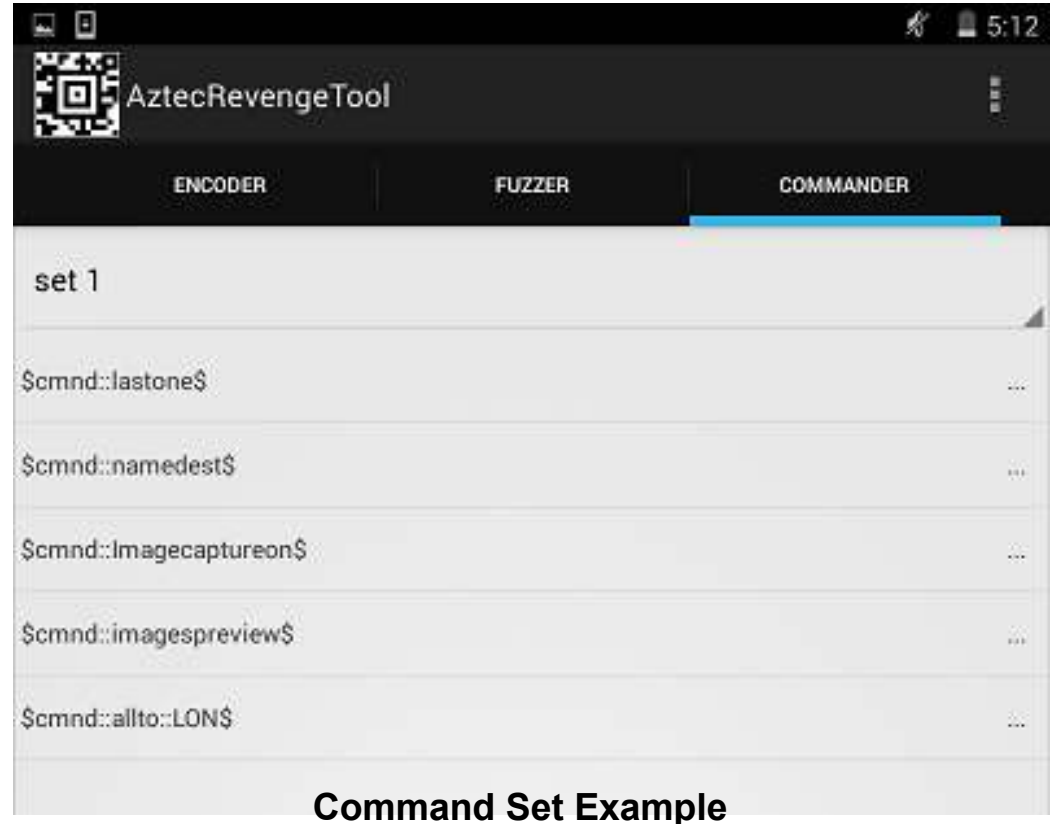


Fuzzing in Action



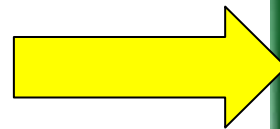
Command Mode

- 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



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?



25
DEFCON

