ATM: EVERY DAY TROUBLE

ALL CHARACTERS AND
EVENTS IN THIS SHOW--
EVEN THOSE BASED ON REAL
PEOPLE--ARE ENTIRELY FICTIONAL.

ALEXEY OSIPOV,
OLGA KOCHETOVA
KASPERSKY LAB

DefCamp#8
Where Hacking & Security Collide

ROOT@ROOT:~# WHOAMI

PENETRATION TESTING DEPARTMENT, KASPERSKY LAB

- @_ENDLESS_QUEST_, @GIFTSUNGIVEN
- ATM AND POS SECURITY ASSESSMENT
- PENETRATION TESTING
- FORENSIC INVESTIGATION

SPEAKERS AT MANY IT EVENTS

AUTHORS OF MULTIPLE ARTICLES, RESEARCHES AND ADVISORIES

OVERVIEW

ONE SHOULD

LEGO FOR ADULTS

- TOP BOX – SERVICE ZONE
  - PC
  - CARD READER
  - PIN PAD
  - OTHER
- BOTTOM – SAFE
  - CASH OUT MODULE (DISPENSER)
  - CASH IN MODULE (DEPOSIT UNIT)
  - RECYCLING MODULE (OUT AND IN)

SOFTWARE

- HOST (COMPUTER)
  - OS
  - GUI AND DEVICE CONTROL
  - ANTIVIRUS/INTEGRITY CONTROL SOFTWARE
  - VIDEO SURVEILLANCE
  - RADMIN/TEAMVIEWER AND OTHER CRAP
- DEVICES
  - SOME MICROCONTROLLERS WITH RTOS

YOU CAN INSTALL KALI ON *ANYTHING* ©

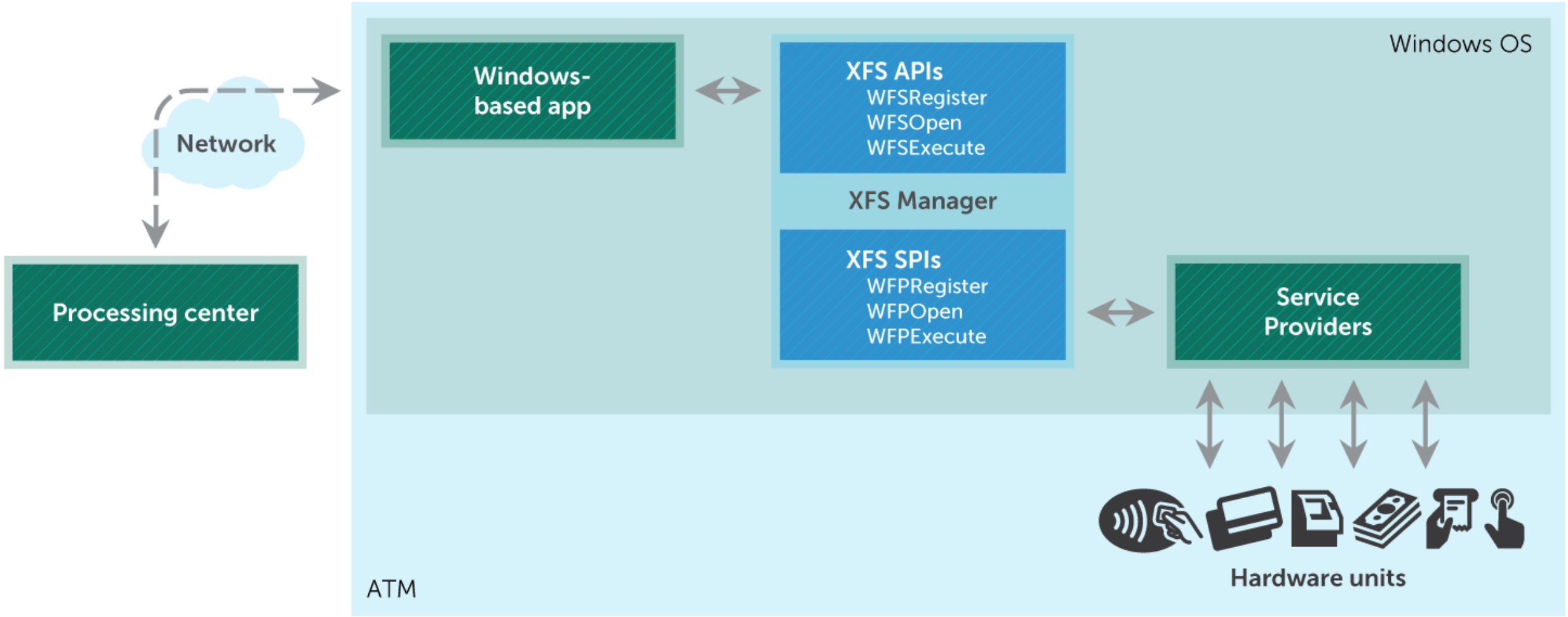
@KALILINUX
@DEFCAMPRO
@SECESPRESSO

DefCamp#8
Where Hacking & Security Collide

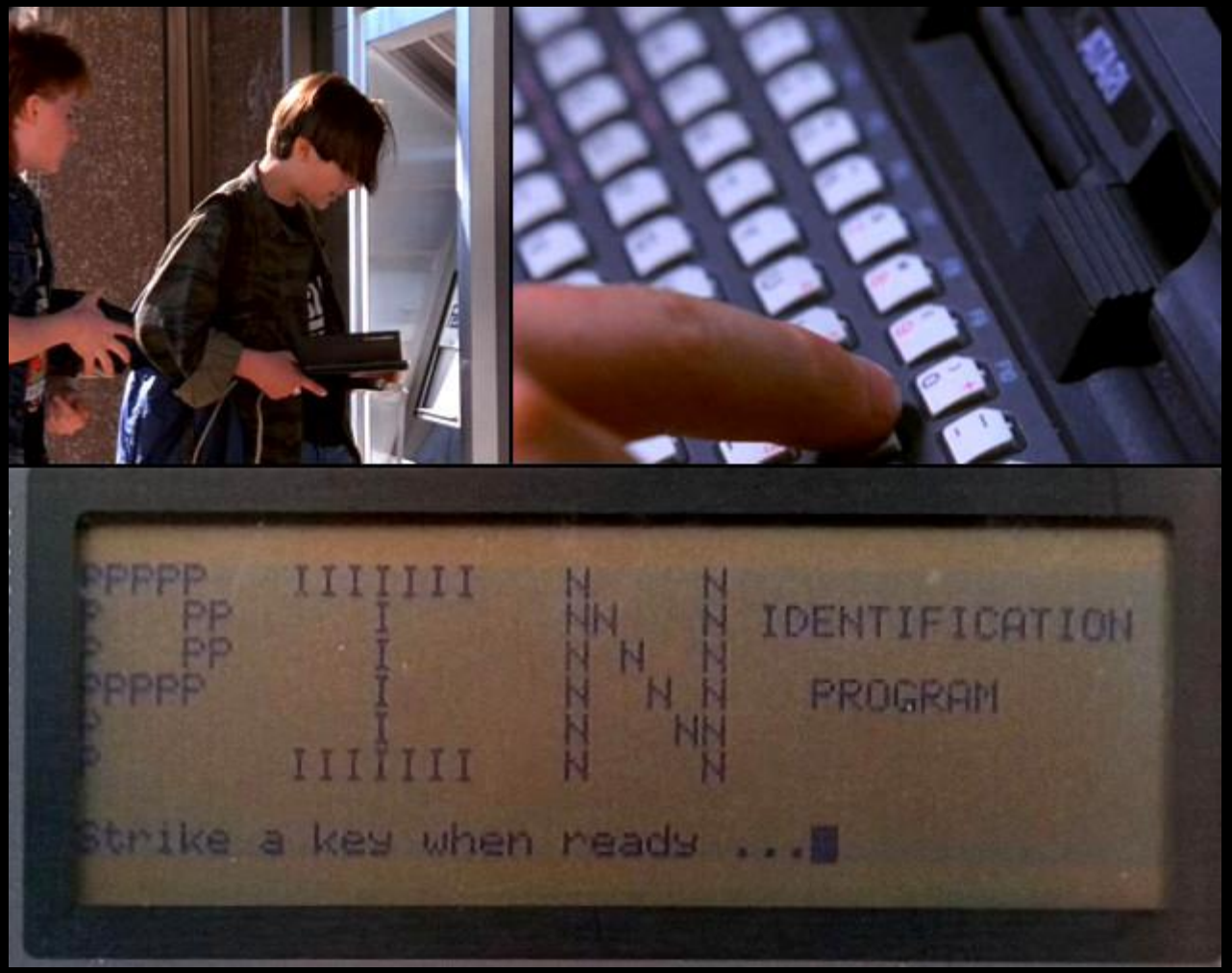
ARE YOU KIDDING ME?

DefCamp#8
Where Hacking & Security Collide

HOW IT WORKS?


Network
Processing center
Windows-based app
Windows OS
XFS APIs
WFSRegister
WFSOpen
WFSExecute
XFS Manager
XFS SPIs
WFPRegister
WFPOpen
WFPExecute
Service Providers
Hardware units
ATM

THINGS FROM THE 1990S

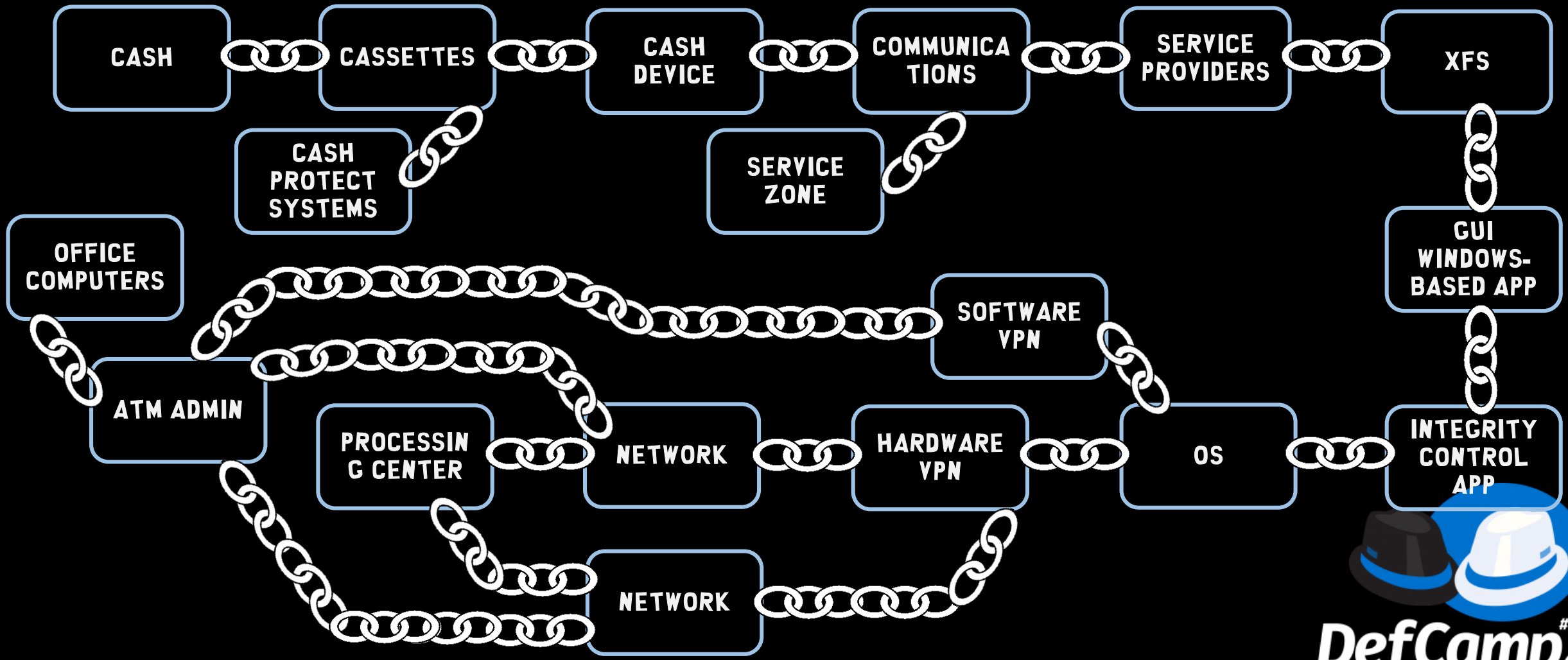


ATTACK TECHNIQUES

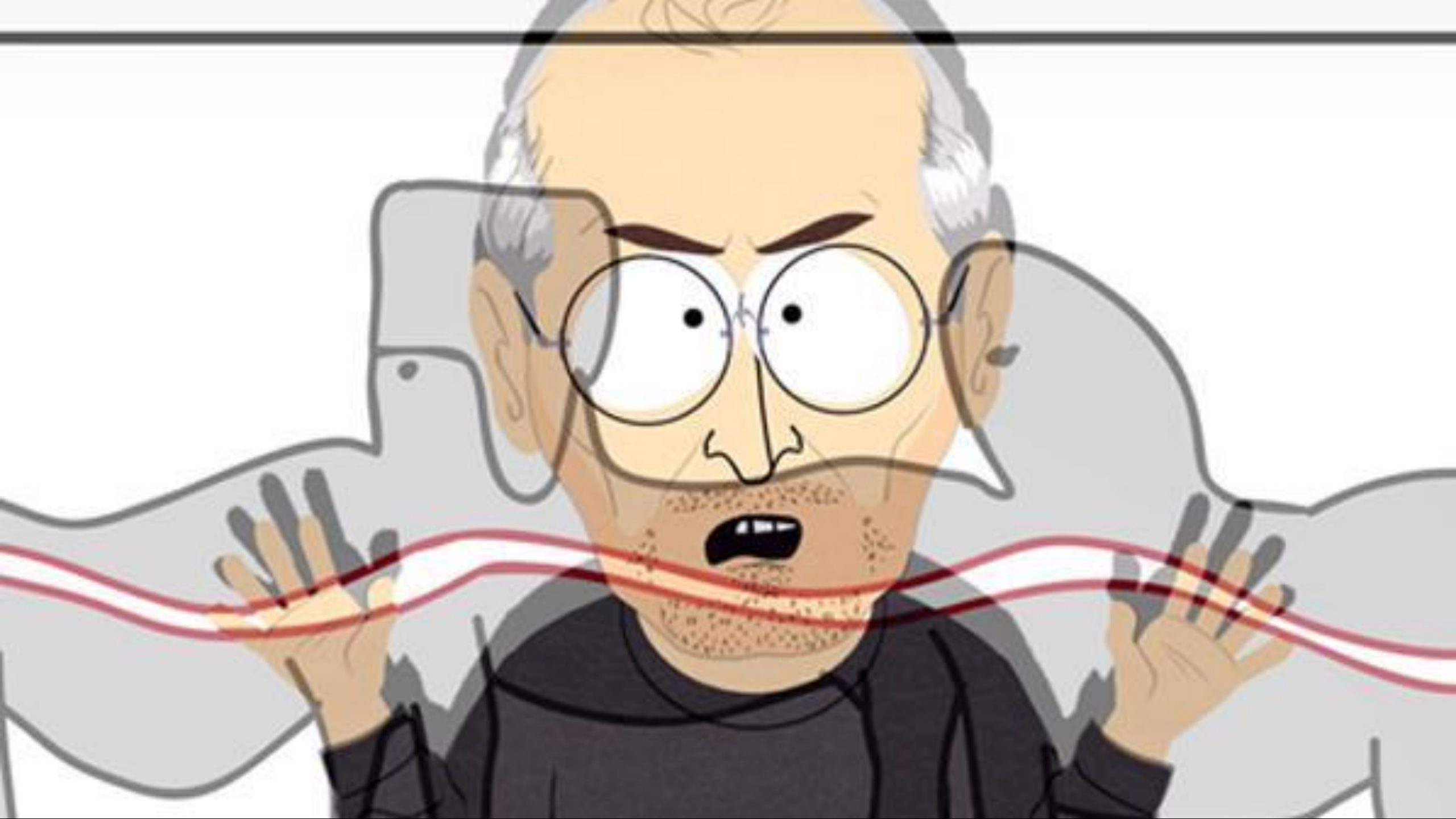
- PHYSICAL
- HARDWARE
- SOFTWARE
- NETWORK

COUNTERMEASURE TO SAVE TREASURE

CASHCONTROLCENTIPEDE



DefCamp#8
Where Hacking & Security Collide



CASH

THEY DON'T BREAK IT. THEY STEAL.

TREASURE CHEST

DON'T BREAK THE LOCK
BREAK THE CHAIN

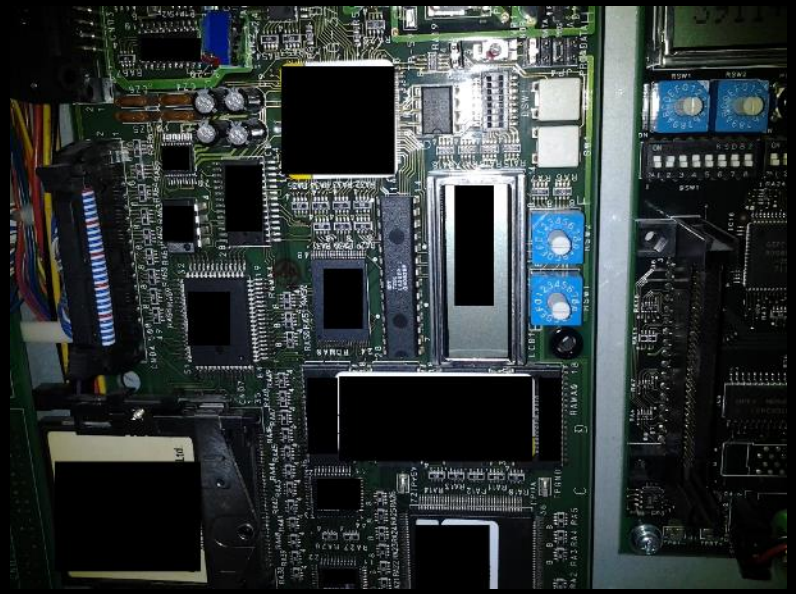
DefCamp#8
Where Hacking & Security Collide

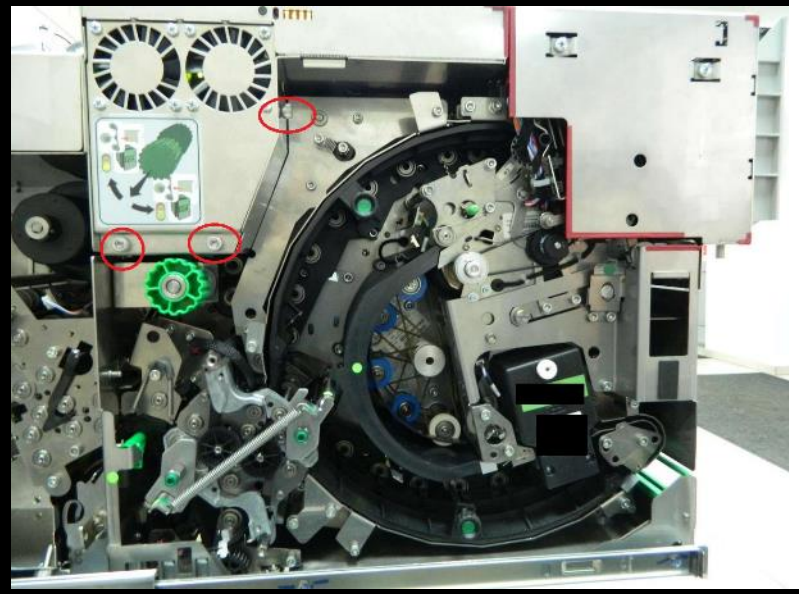
CASH DEVICES

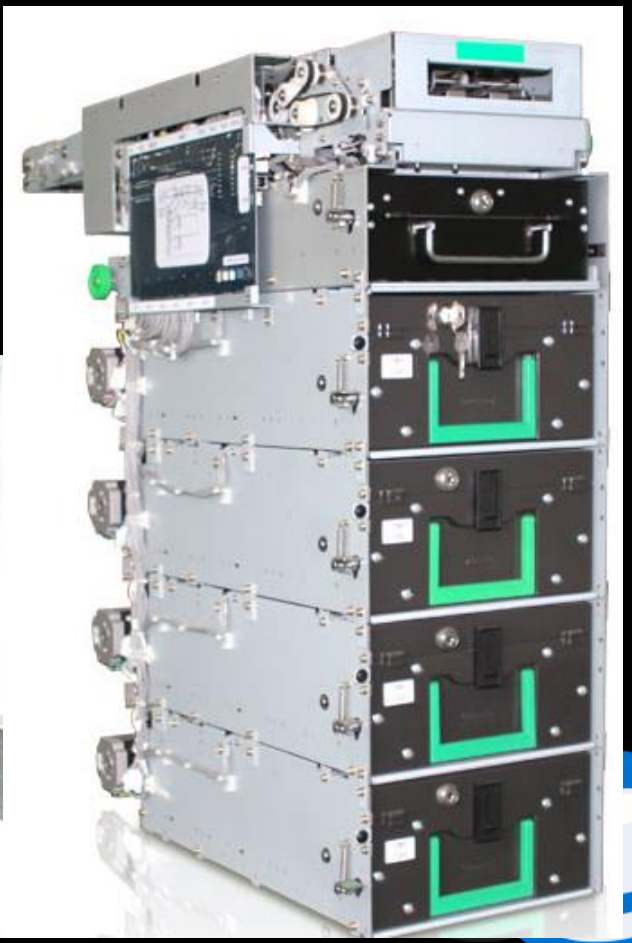
IS IN THE SAFE. SO WHAT?

WHAT IS THE HOOK

- MICROCONTROLLER
- FIRMWARE

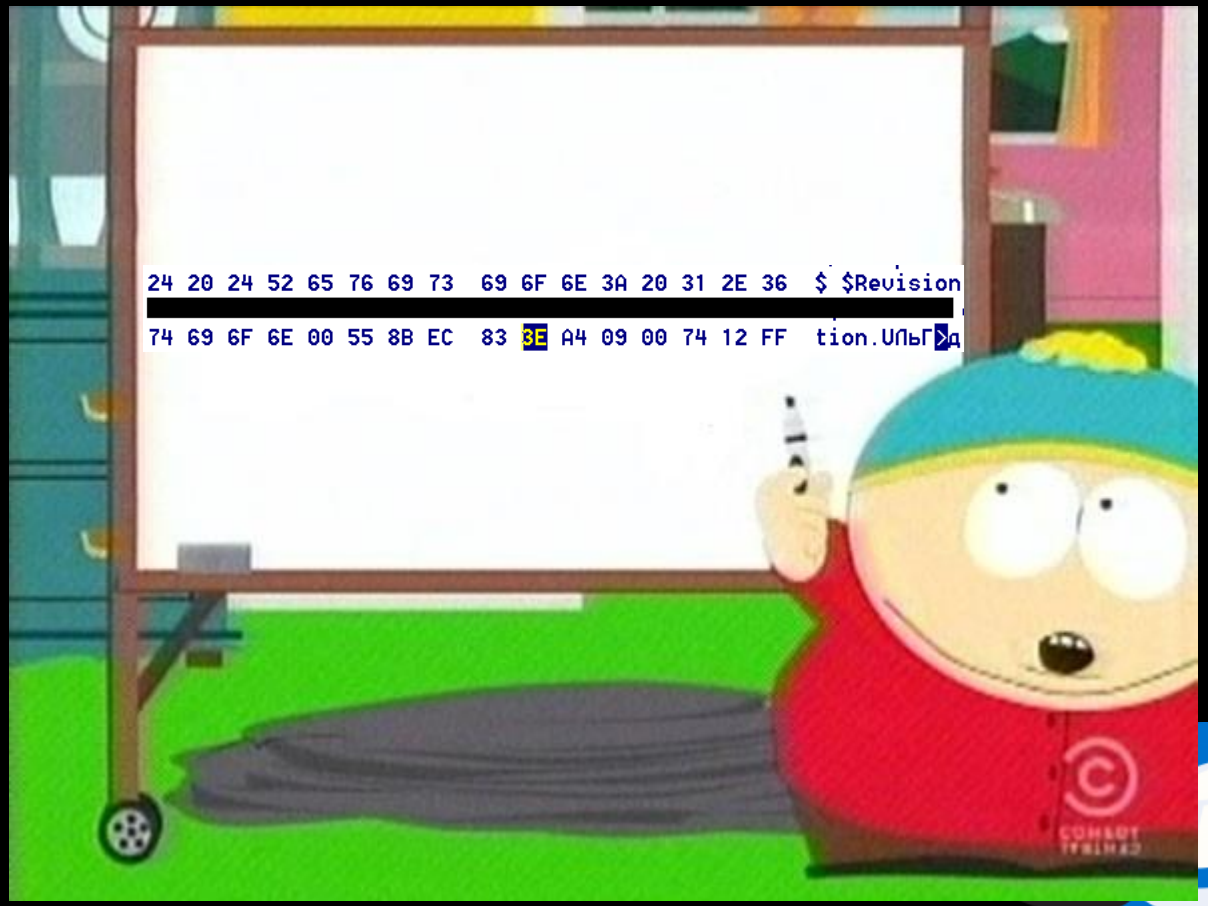






SUPER ADVANCED PERSISTENT THREAT

- FIRMWARE
  - MODIFY
  - UPDATE
- CASH DEVICE
  - CONTROL
  - TOTAL CONTROL



DefCamp#8
Where Hacking & Security Collide

CARD READER

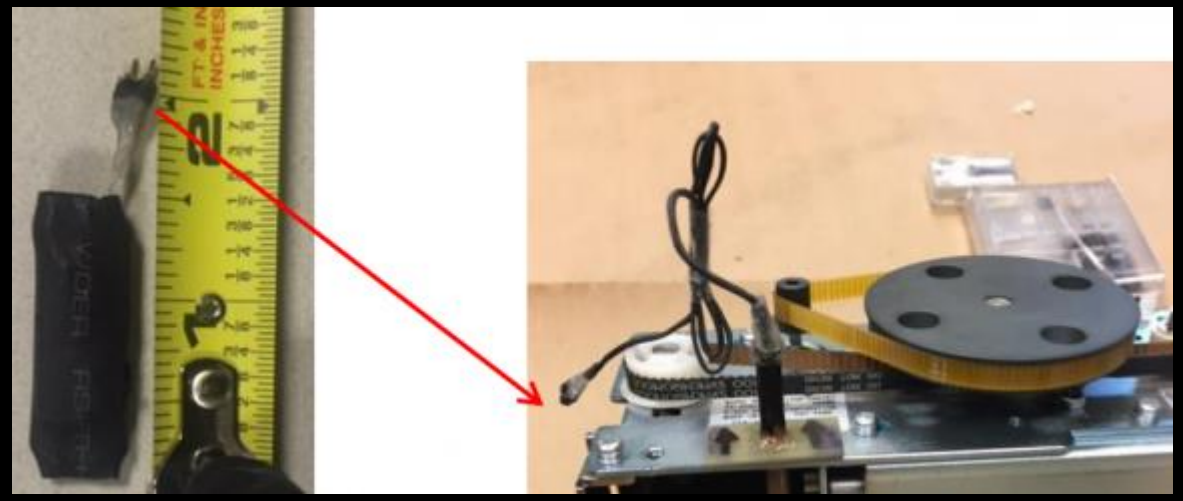
NOT CASH, BUT ... CASH

DefCamp#8

Where Hacking & Security Collide

CARD READER EXPLOITATION

- SENSITIVE DATA IN PLAIN TEXT
- HARDWARE SNIFFER



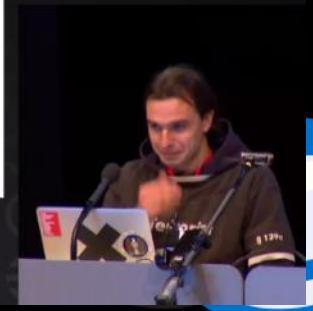
YOU ARE NOT YOU ANYMORE

können diese Augen lügen?

ƎICƎ
a new dawn

guten Tag, mein Name ist
Dr. von der Leyen

ƎICƎ
a new dawn



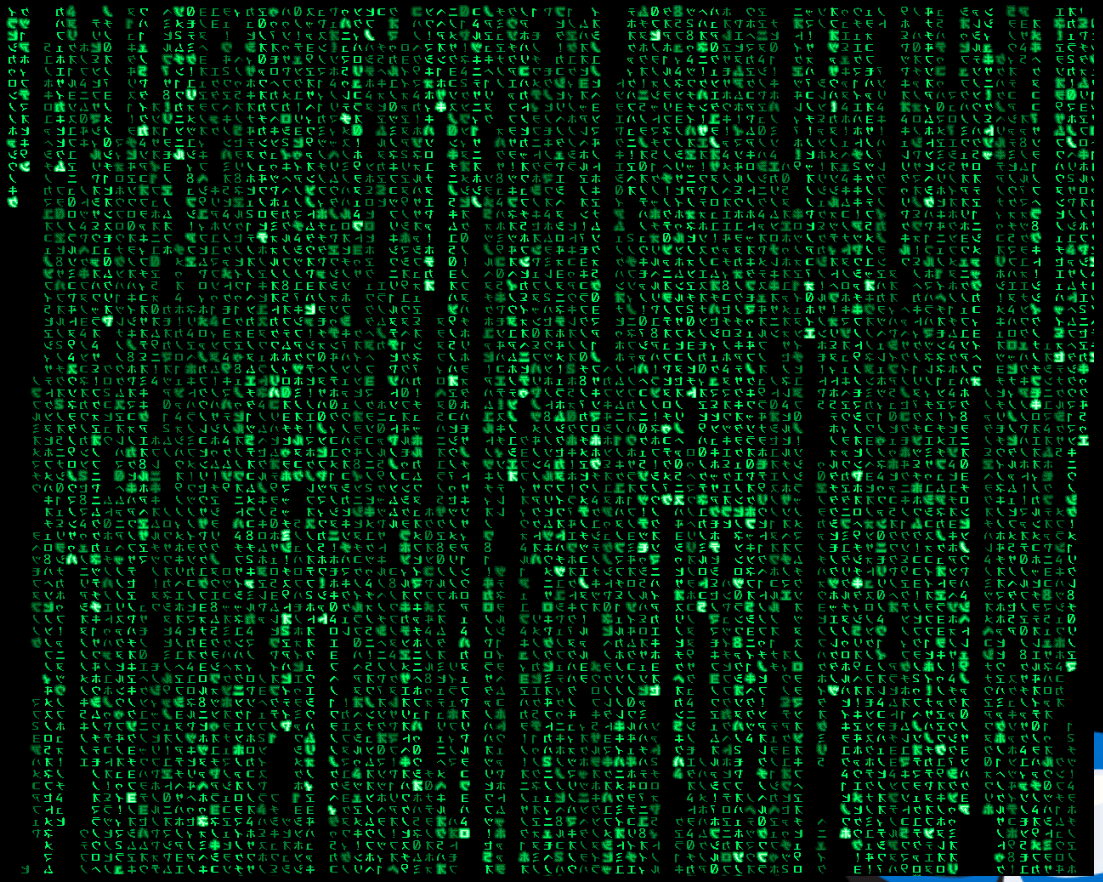
SOURCE: HTTPS://MEDIA.CCC.DE/V/31C3_-_6450_-_DE_-_SAAL_1_-_201412272030_-_ICH_SEHE_ALSO_BIN_ICH_DU_-_STARBUG#VIDEO

DefCamp#8
Where Hacking & Security Collide

COMMUNICATIONS

ANALYZE THIS

- RS... (E.G. 232, 485)
- SDC
- USB



TYPICAL FLAVOURS

- ASCII-BASED
- BINARY
- ~~ENCRYPTED~~ OBFUSCATED

02 30	XX XX	X X	01 01 02 00 03 00 04 00 05 00 06 00	10 03	42

DefCamp#8
Where Hacking & Security Collide

HACKER STUFF

DefCamp#8
Where Hacking & Security Collide

VIDEO - NEWLY EVIL USB (BLACKBOX)

HTTPS://YOUTU.BE/3HYAOMVIZPM

SERVICE ZONE

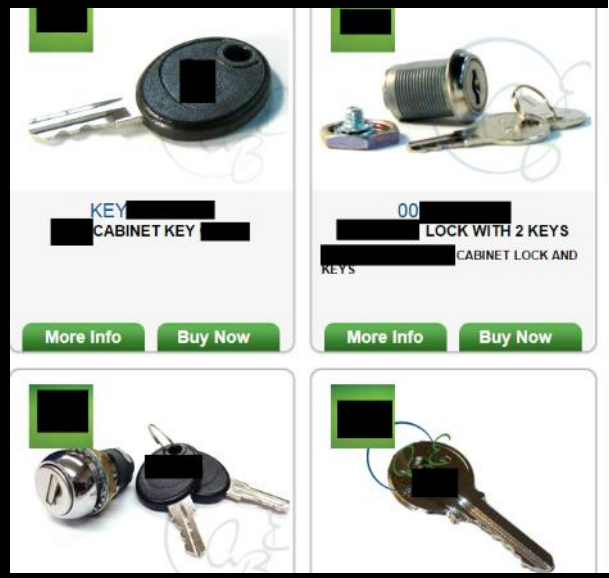
THERE IS NO CASH. REALLY?

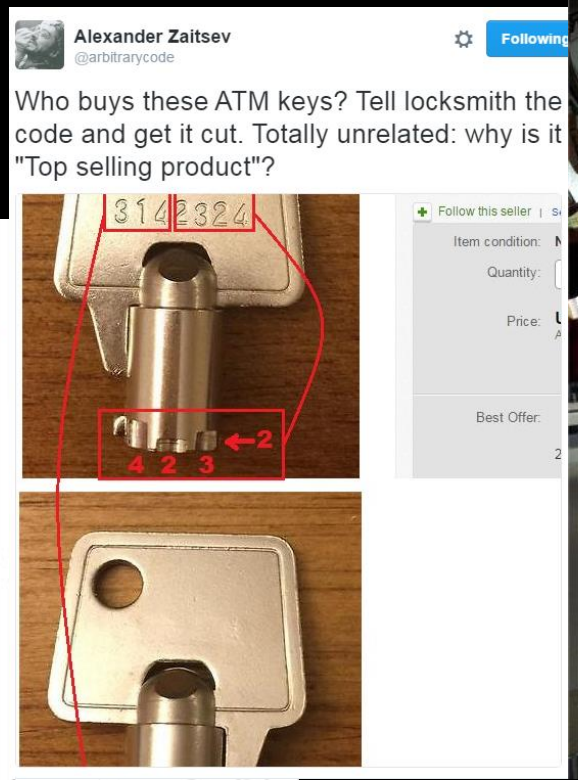
DefCamp#8

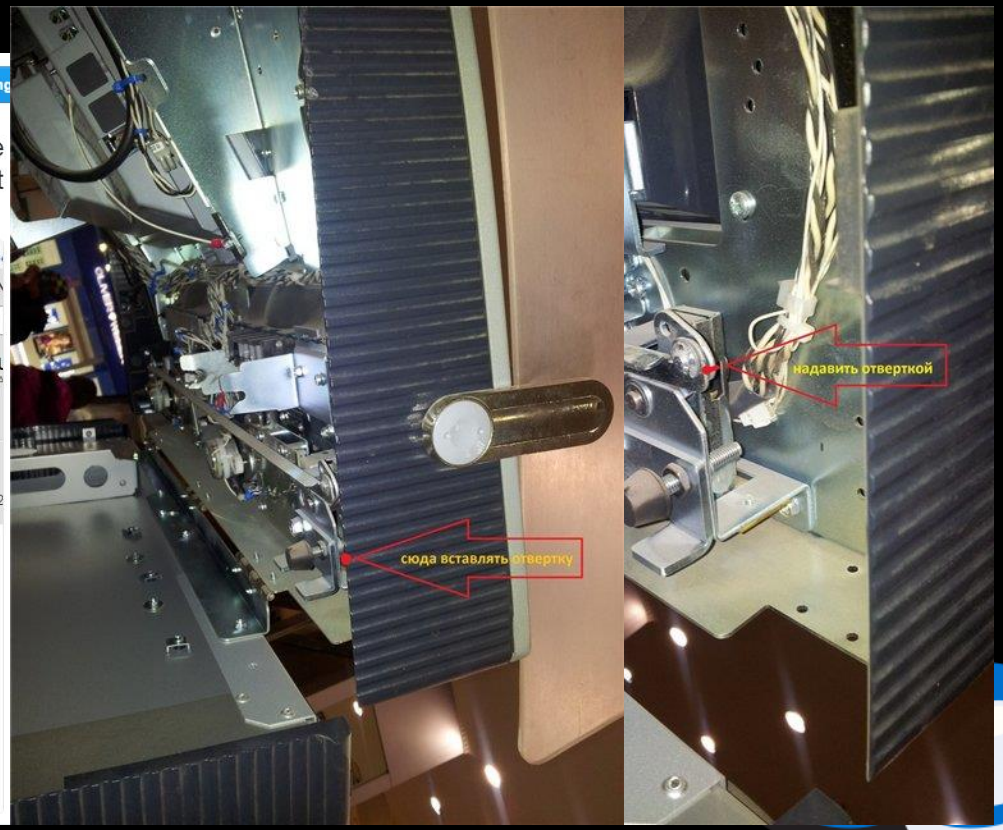
Where Hacking & Security Collide

HOW TO GET IN

- "MASTER KEY"
- SCREWDRIVER
- "SPECIAL" TOOL







DefCamp#8
Where Hacking & Security Collide

VIDEO - HOW TO GET IN

HTTPS://YOUTU.BE/KIJIZHUTLJU

OUR SERVICE ZONE IS SECURED ©

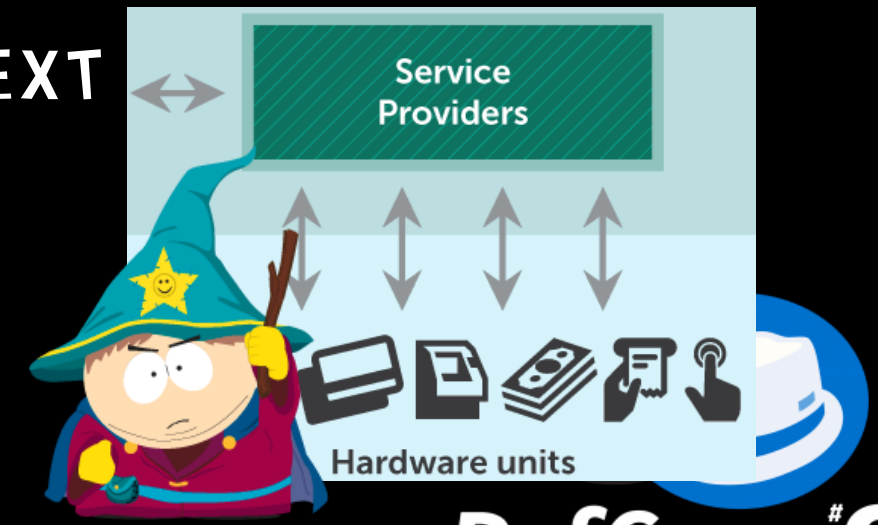
SHOULD WE?

SERVICE PROVIDERS

DefCamp#8
Where Hacking & Security Collide

MALWARE: NEXT GENERATION

- ATTACKER BYPASSES INTERACTION WITH XFS MANAGER
- HOOKS ALL FUNCTIONS USED BY SPECIFIC ATM VENDOR SOFTWARE
- GIVES HIGHEST INFORMATION TO ATTACKER COMPARED TO XFS BASED MALWARE:
  - INTERCEPT NETWORK DATA IN CLEAR TEXT
  - INTERCEPT EMV TRANSACTIONS
  - INTERCEPT USB/COM COMMUNICATION



FRIDA

OVERVIEW DOCS NEWS CODE CONTACT

All News

Frida Releases

Recent Releases

Version 8.0

Frida 8.0 Released

RELEASE 04 Oct 2016  oleavr

It is time to level up to the next major version.

Quick-start Instructions

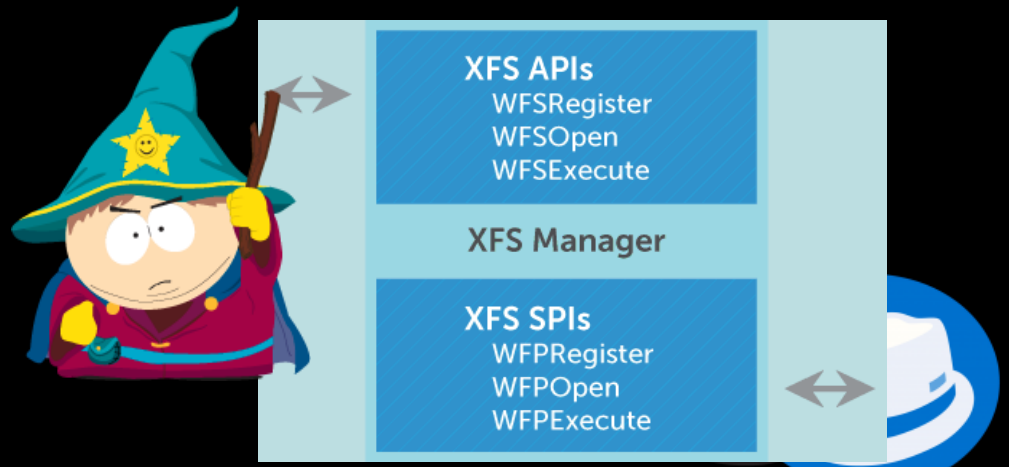
```
~ $ sudo pip install frida
~ $ frida-trace -i "*dispens*" service_provider
```

VIDEO – MALWARE NG

HTTPS://YOUTU.BE/XOKG7HNVT20

MALWARE: XFS BASED

- EVERY WINDOWS EXECUTED CAN ISSUE COMMANDS TO XFS MANAGER
- MALWARE CAN WORK ON MOST ATMS
- EVERYONE INVOLVED IN ATM SECURITY IS PRETTY MUCH FAMILIAR WITH IT



DEVOPSSECHUMANCATERPILLAR

- BUFFER OVERFLOW
- KIOSK MODE BYPASS
- SENSITIVE DATA DISCLOSURE

THIRD-PARTY SECURITY SOFTWARE ONE MORE DOOR

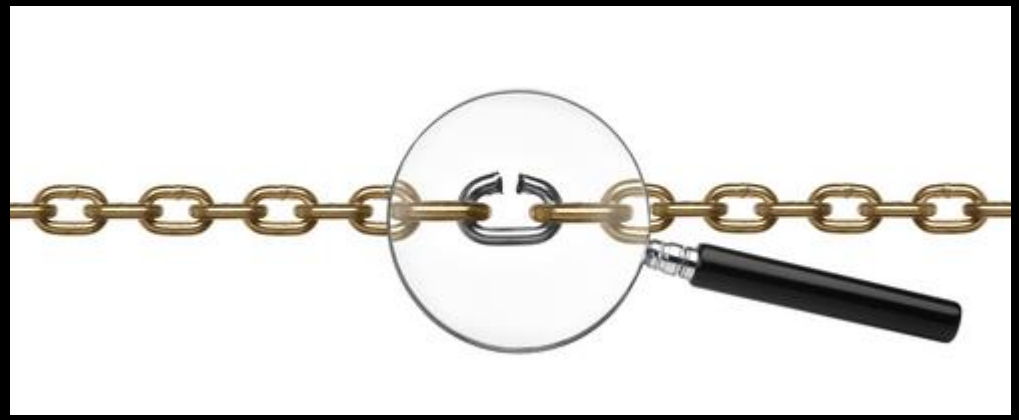
- BUFFER OVERFLOW
- KIOSK MODE BYPASS
- SENSITIVE DATA DISCLOSURE
- REMOTE CONTROL

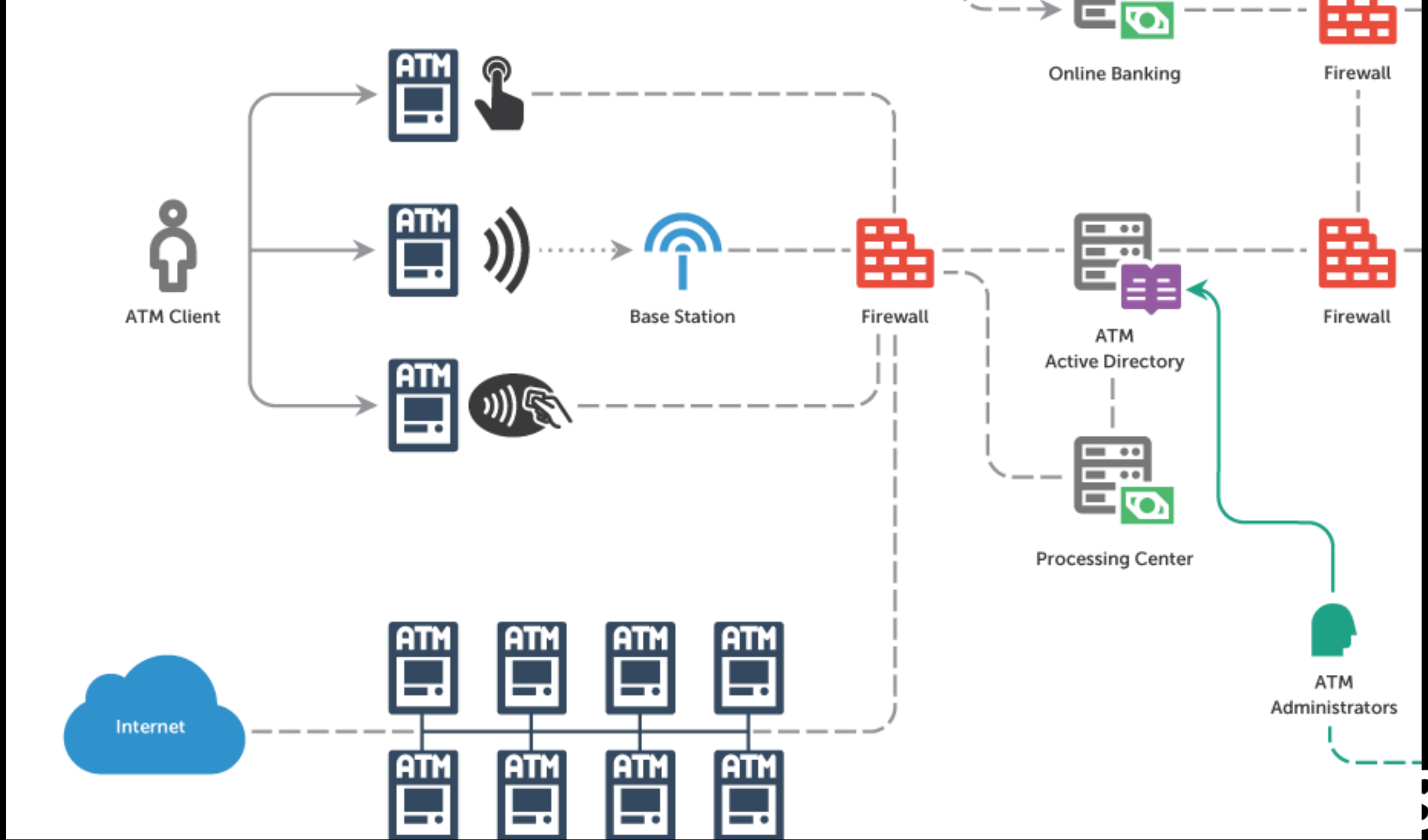
OPERATING SYSTEM

MS08-067 STRIKES AGAIN

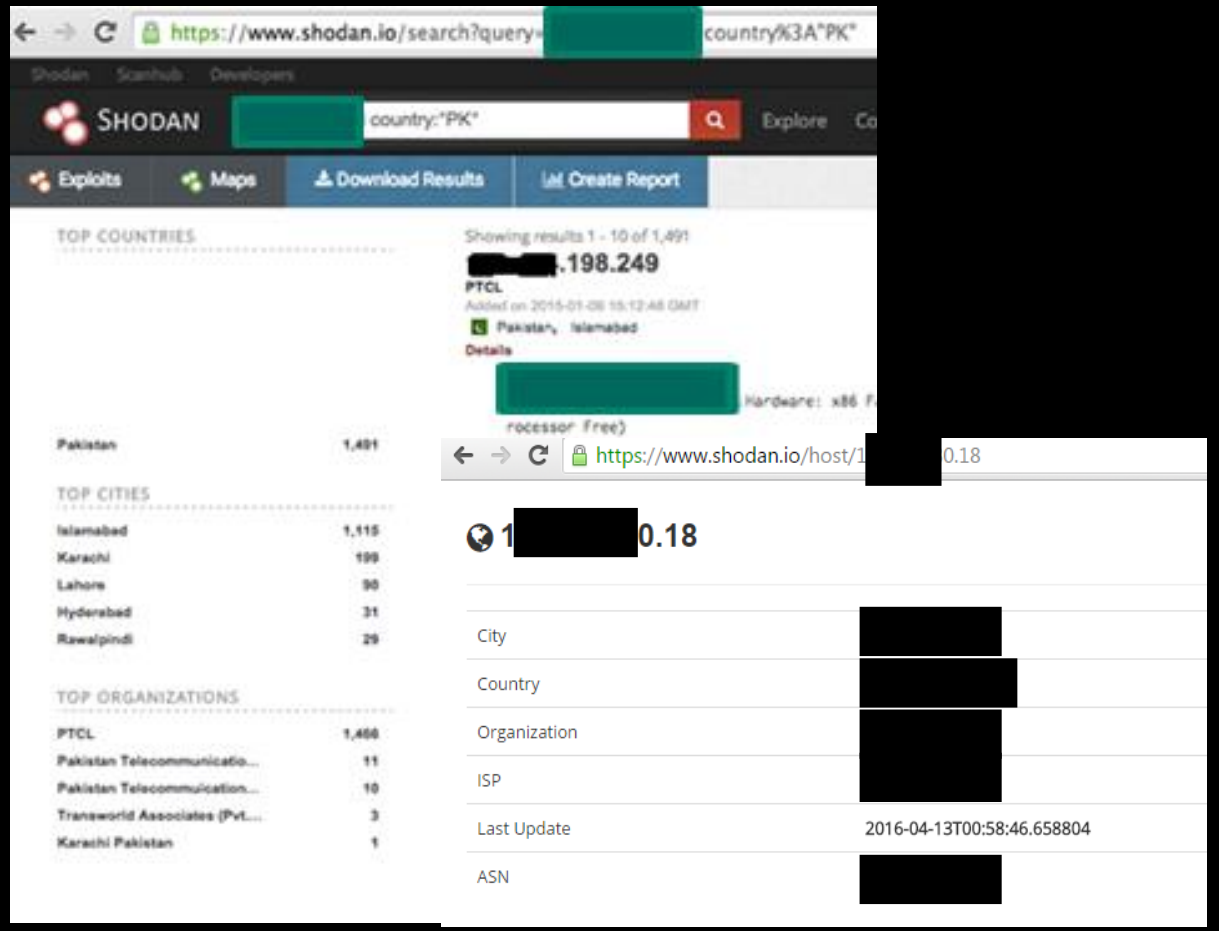
JUST AHEAD

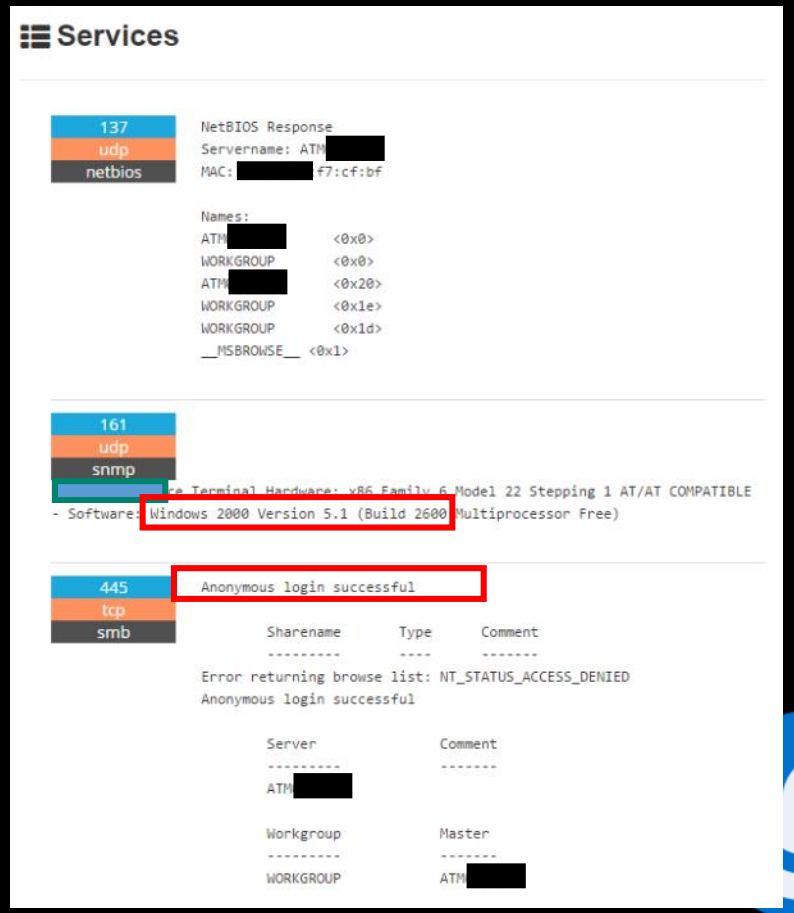
- OLD VERSIONS
- NOT UPDATED
- VULNERABILITIES
- STANDARD SERVICES




Online Banking
Firewall
ATM
ATM
ATM
ATM Client
Base Station
Firewall
Firewall
ATM
Active Directory
Processing Center
ATM
Administrators
Internet
ATM
ATM
ATM
ATM
ATM
ATM
ATM
ATM

LET'S HAVE FUN WITH SHODAN



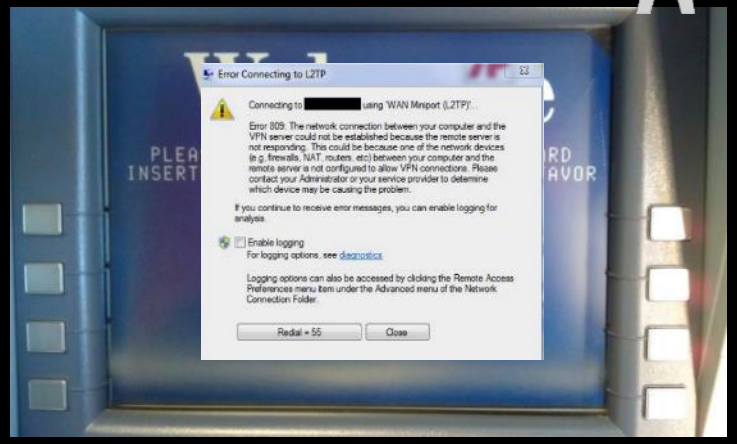


DefCamp#8
Where Hacking & Security Collide

VIDEO – OBEY THE NET

HTTPS://YOUTU.BE/N9DJTYO-COO

WHY VPN IS NOT GOOD SOMETIMES



- SOFTWARE
  - WITH ACCESS TO OS CAN BE DISABLED
  - NOT ALWAYS PROVIDE FIREWALLING FUNCTIONALITY
  - IF VPN-CONNECTION IS INTERRUPTED IT IS COMMON, THAT ALL DATA FROM THIS MOMENT WILL BE TRANSMITTED IN CLEAR-TEXT
- HARDWARE
  - DOESN'T PROTECT AGAINST PHYSICAL ACCESS
  - WORKS REGARDLESS OF HOST COMPUTER
  - IT'S PEACE OF METAL/PLASTIC, YOU CAN GRAB IT WITH HAND

PROCESSING CENTER

TWO-EDGED SWORD

- ROGUE PROCESSING CENTER (ATTACKING ATM)
  - CASH WITHDRAWAL
- ROGUE ATM (ATTACKING PROCESSING CENTER)
  - FAKE CASH DEPOSIT
  - BANK CARD ACCOUNT COMPROMISE
  - PAYMENT SERVICES/SYSTEMS ATTACKS

VIDEO – ROGUE PROCESSING

HTTPS://YOUTU.BE/NRBQBLBLLLS

HACK THE BANK

HOW TO

WHAT TO ~~B~~REACH

- GOALS
  - SENSITIVE DATA DISCLOSURE
  - UNAUTHORIZED CASH WITHDRAWAL
- WAYS
  - NETWORK
  - COMMUNICATIONS LINES
- POINTS
  - BASED ON THE COMPLEXITY OF THE FINDINGS
  - ATTACKS OVER USB BRING YOU EXTRA POINTS

DefCamp#8
Where Hacking & Security Collide

RULES

- READ FULL VERSION HERE HTTPS://DEF.CAMP/HACK-THE-BANK/
- HACK THE BANK CAREFULLY - DISRESPECTING ANY OF THESE RULES AS WELL AS ANY OFFENSIVE ACTION TAKEN AGAINST ANY OTHER PARTICIPANTS WILL RESULT IN IMMEDIATE DISQUALIFICATION

- P.S. MODERATORS ARE ALWAYS RIGHT ^_^

DefCamp#8
Where Hacking & Security Collide

KASPERSKY lab

HAVE FUN
STAY SAFE

OLGA KOCHETOVA,
OLGA.KOCHETOVA@KASPERSKY.COM,
@_ENDLESS_QUEST_

ALEXEY OSIPOV,
ALEXEY.OSIPOV@KASPERSKY.COM,
@GIFTSUNGIVEN

DefCamp#8
Where Hacking & Security Collide