



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

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



9:55 PM - 6 Nov 2017

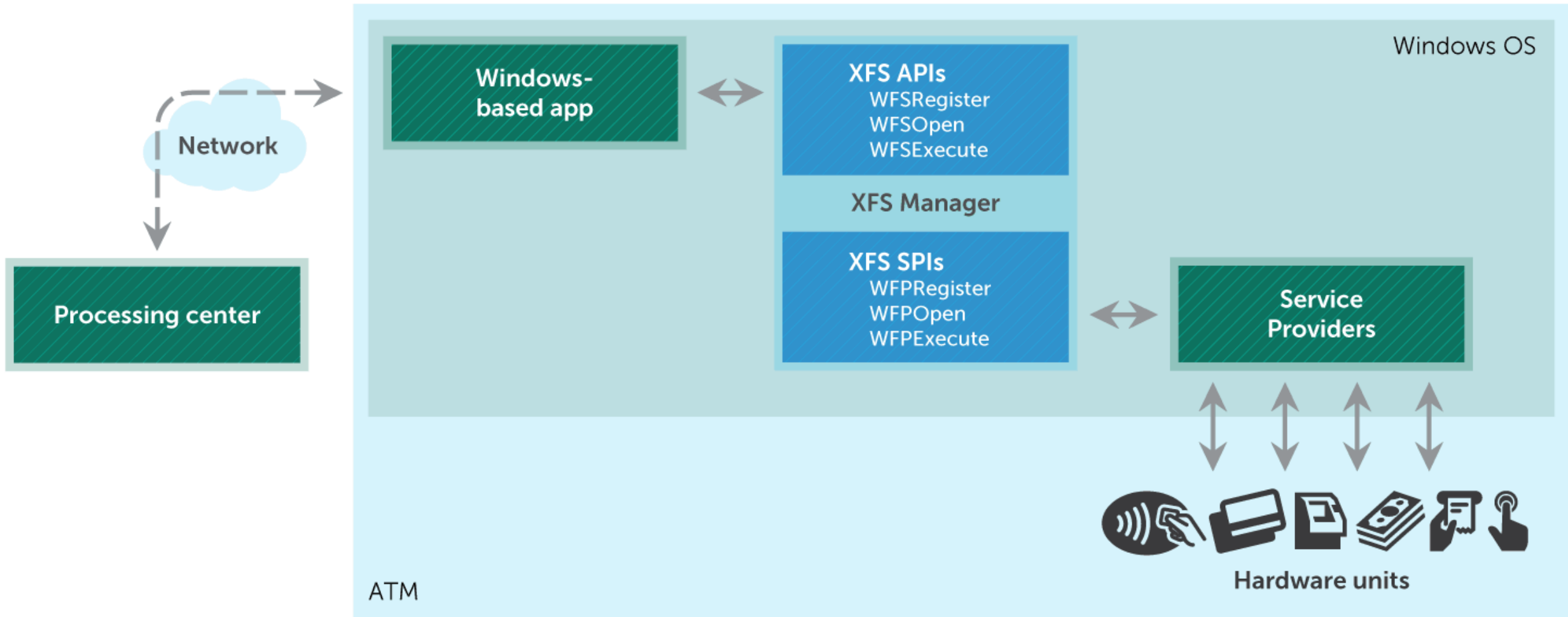
3,115 Retweets 6,082 Likes



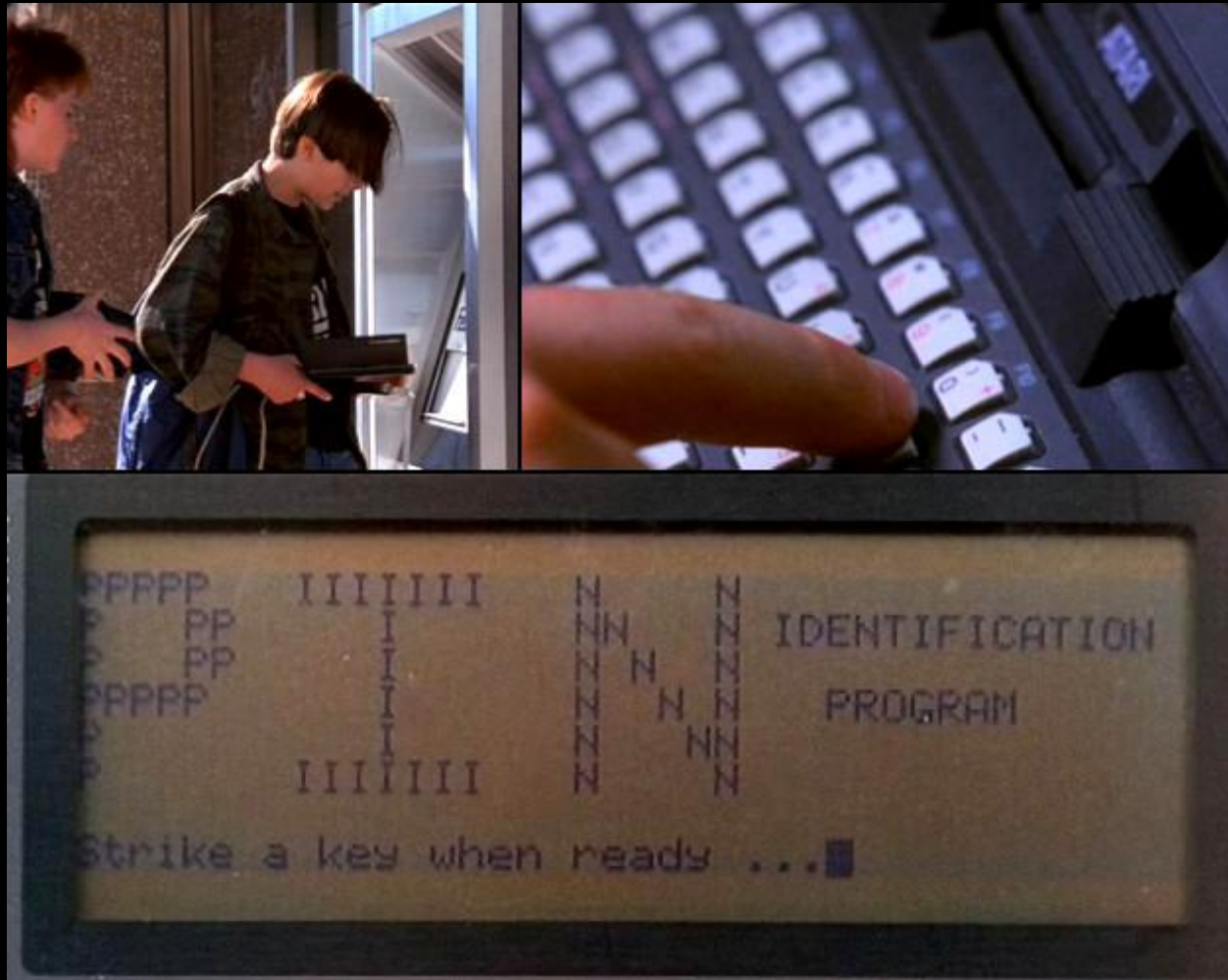
ARE YOU KIDDING ME?



HOW IT WORKS?



THINGS FROM THE 1990S



ATTACK TECHNIQUES

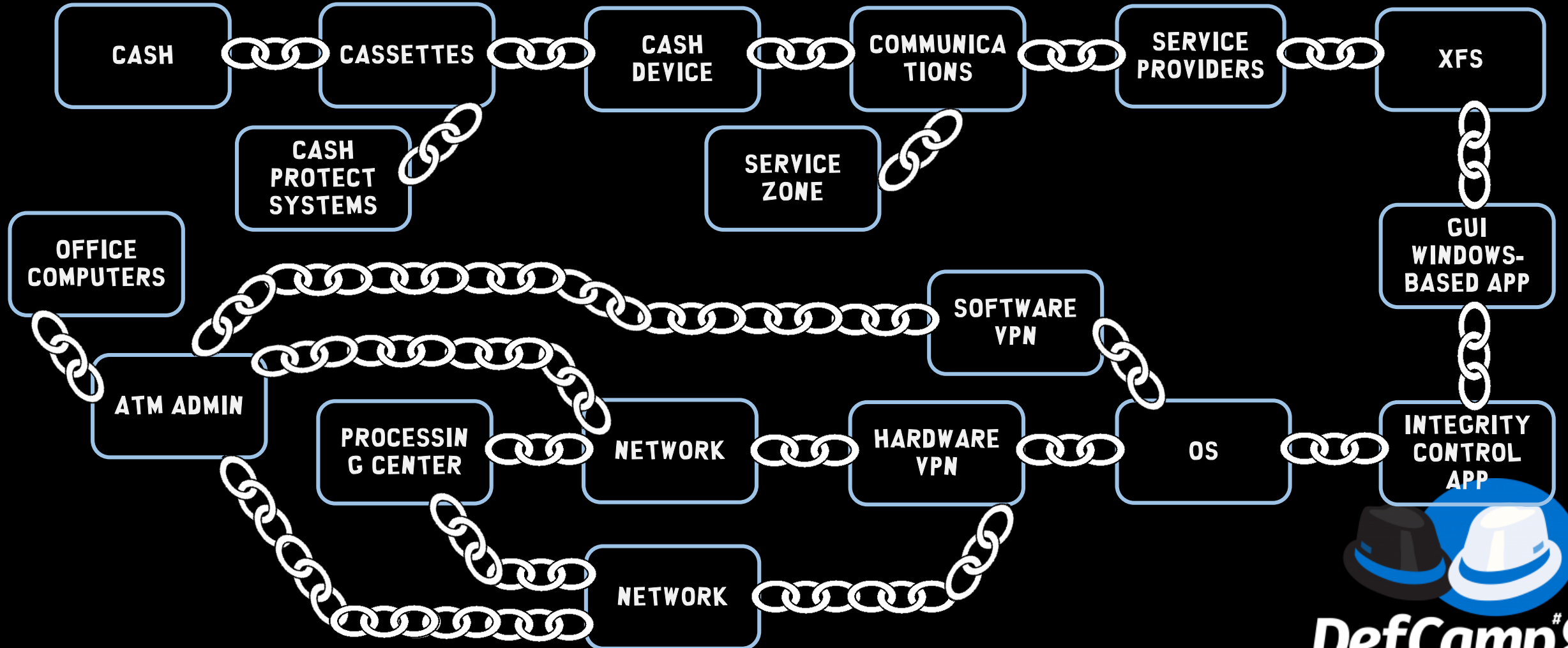
- PHYSICAL
- HARDWARE
- SOFTWARE
- NETWORK

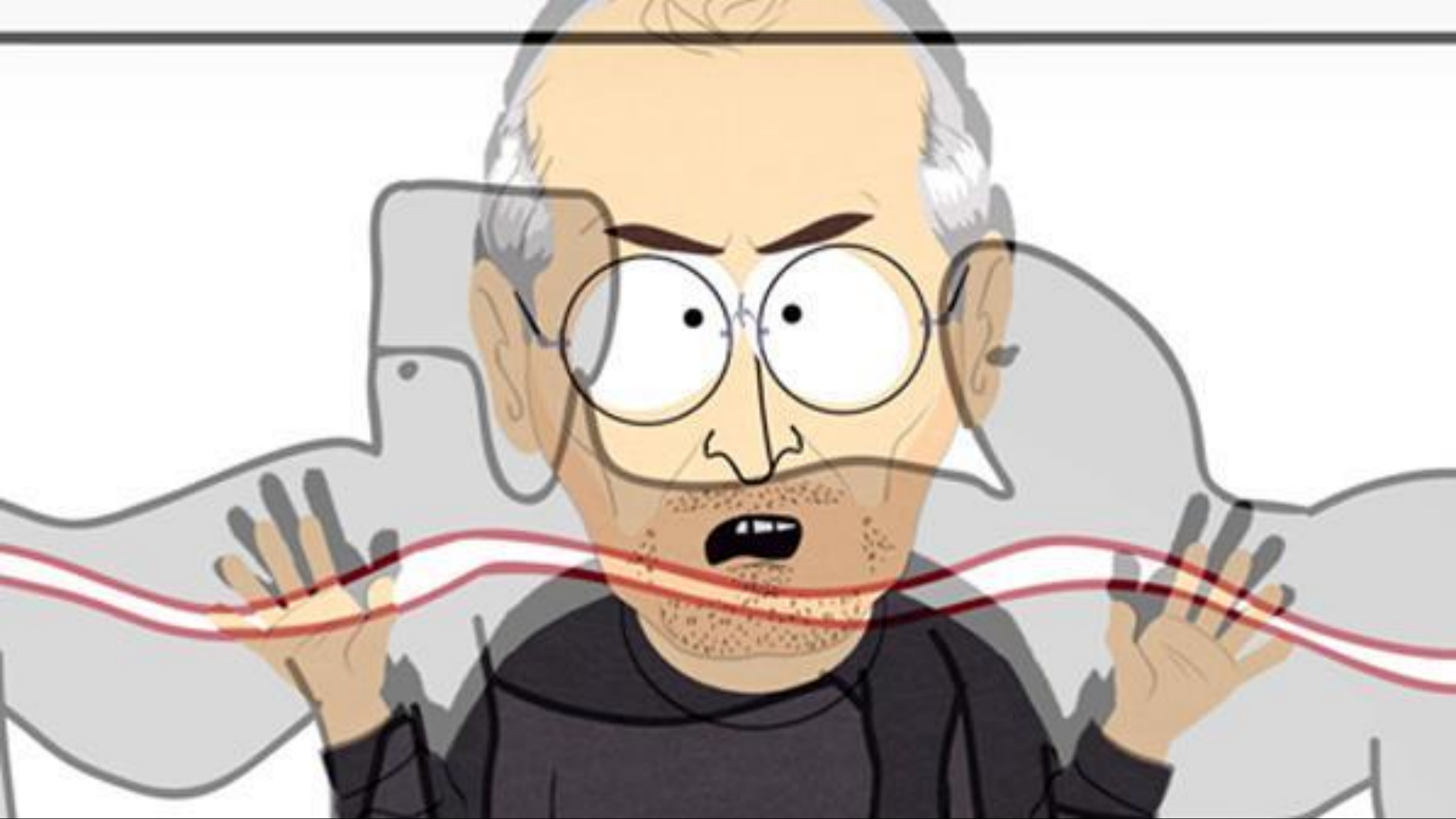


COUNTERMEASURE TO SAVE TREASURE



CASHCONTROLCENTIPEDE





CASH

THEY DON'T BREAK IT. THEY STEAL.



TREASURE CHEST



DON'T BREAK THE LOCK BREAK THE CHAIN



DefCamp8
Where Hacking & Security Collide



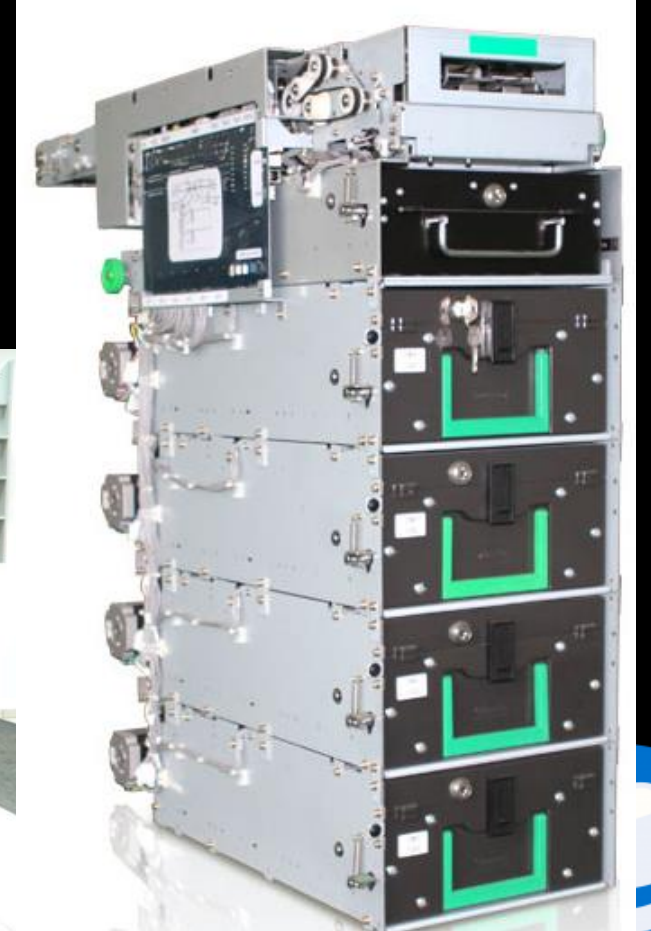
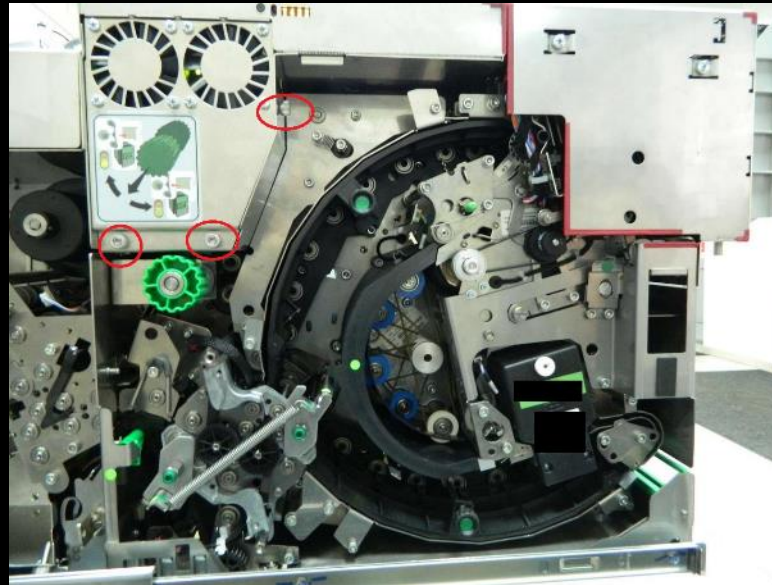
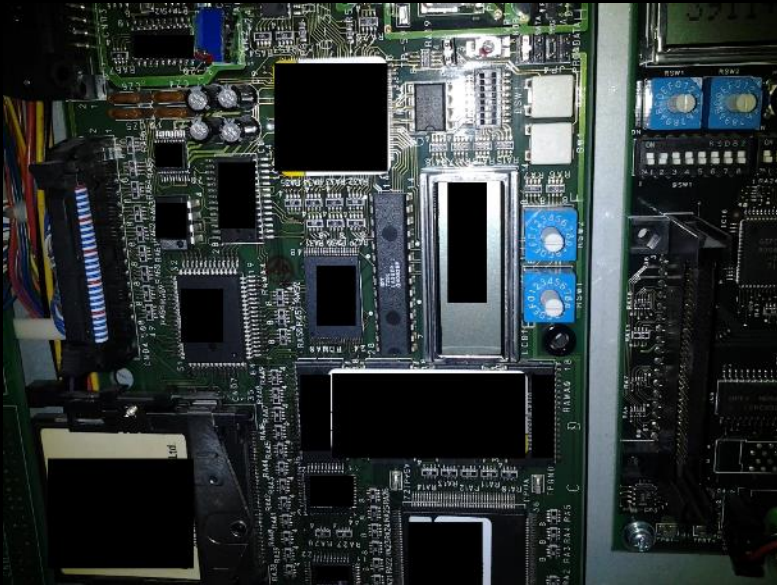
CASH DEVICES

IS IN THE SAFE. SO WHAT?



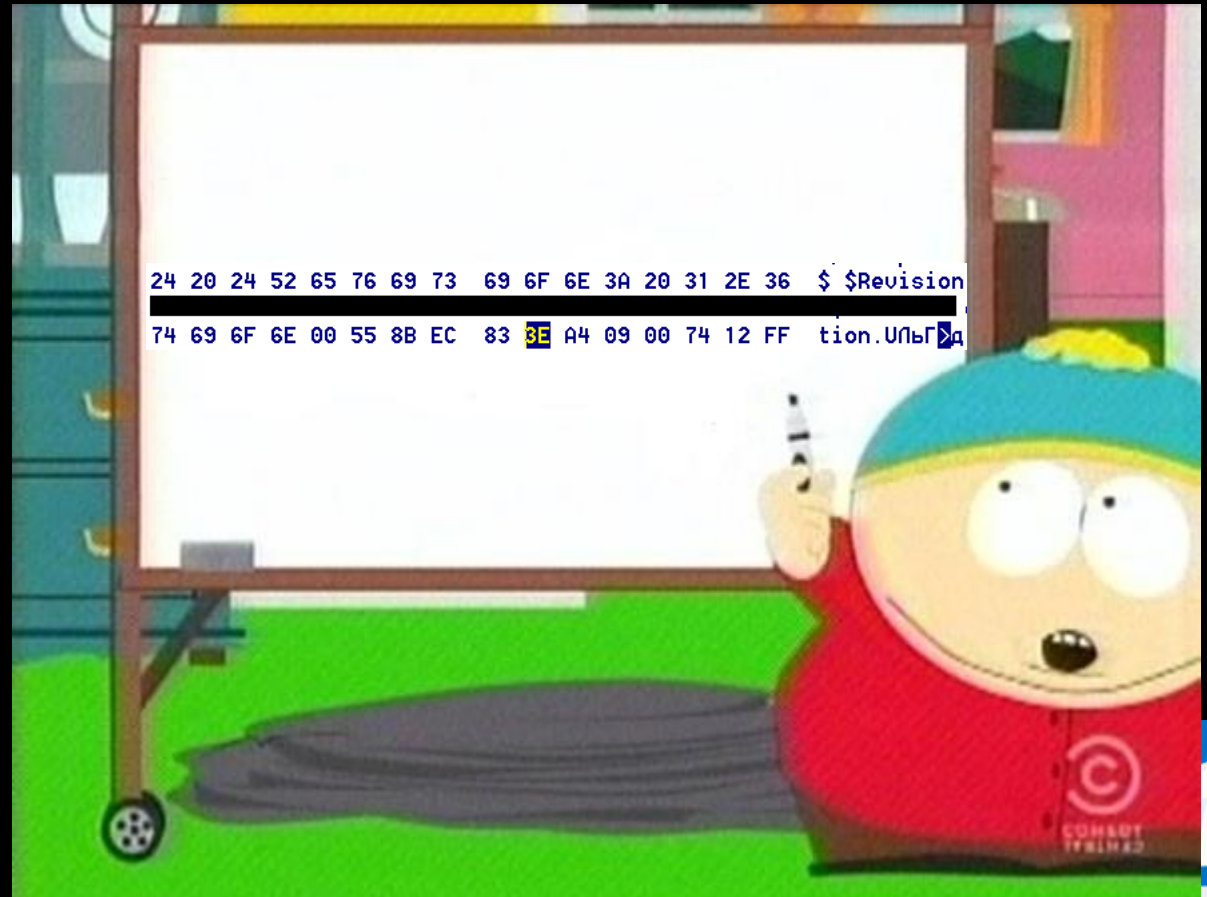
WHAT IS THE HOOK

- MICROCONTROLLER
- FIRMWARE



SUPER ADVANCED PERSISTENT THREAT

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



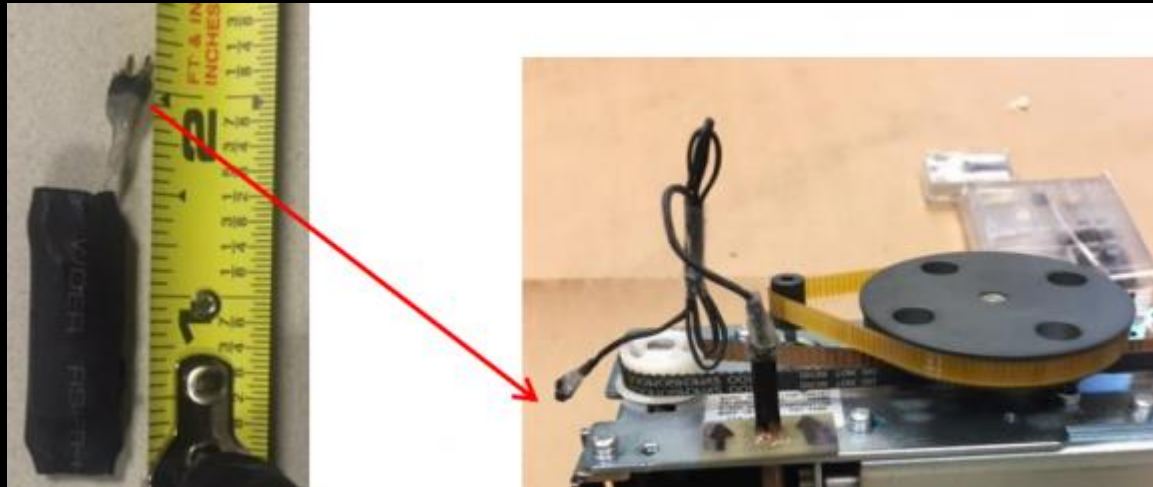
CARD READER

NOT CASH, BUT ... CASH



CARD READER EXPLOITATION

- SENSITIVE DATA IN PLAIN TEXT
- HARDWARE SNIFFER

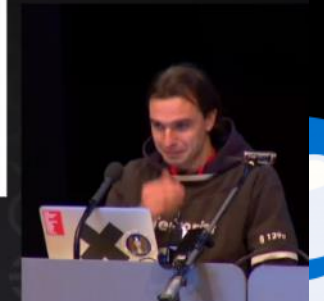


YOU ARE NOT YOU ANYMORE

können diese Augen lügen?



guten Tag, mein Name ist
Dr. von der Leyen



SOURCE: [HTTPS://MEDIA.CCC.DE/V/31C3-6450](https://media.ccc.de/v/31c3-6450) - DE - SAAL 1 -
201412272030 - ICH SEHE ALSO BIN ICH DU - STARBUG#VIDEO

COMMUNICATIONS



ANALYZE THIS

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



TYPICAL FLAVOURS



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

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

HACKER STUFF



DefCamp8
Where Hacking & Security Collide

VIDEO - NEWLY EVIL USB (BLACKBOX)

[HTTPS://YOUTU.BE/3HYA0MVIZPM](https://youtu.be/3HYA0MVIZPM)



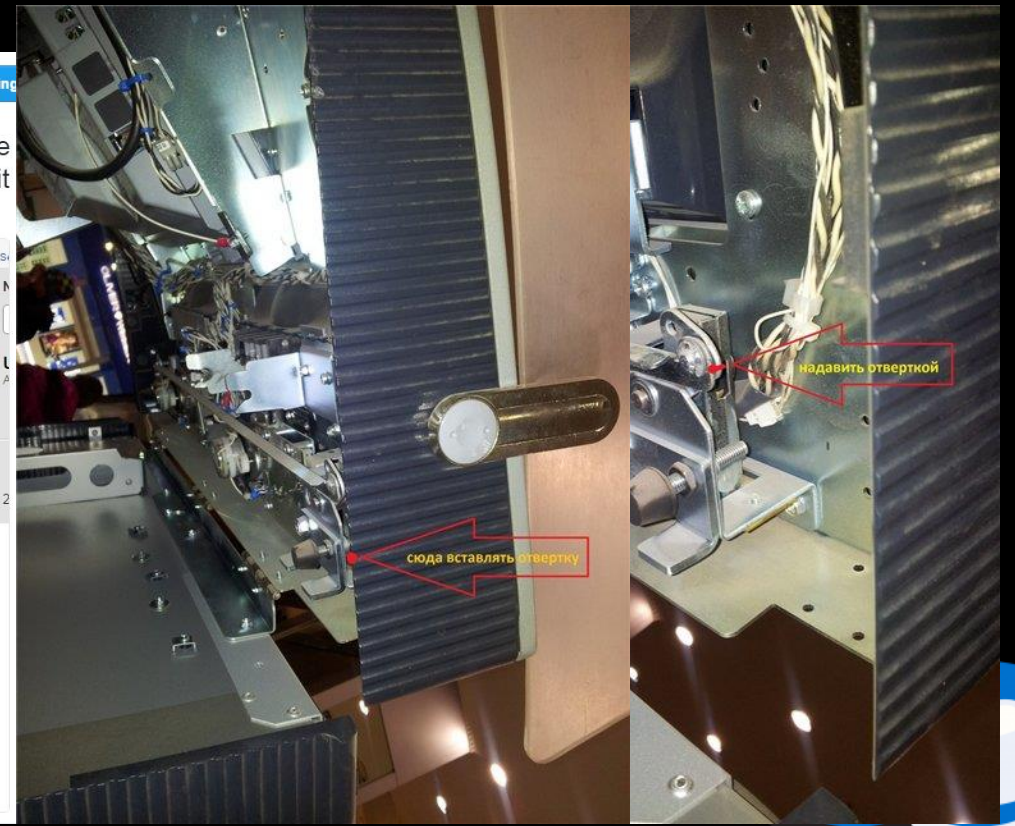
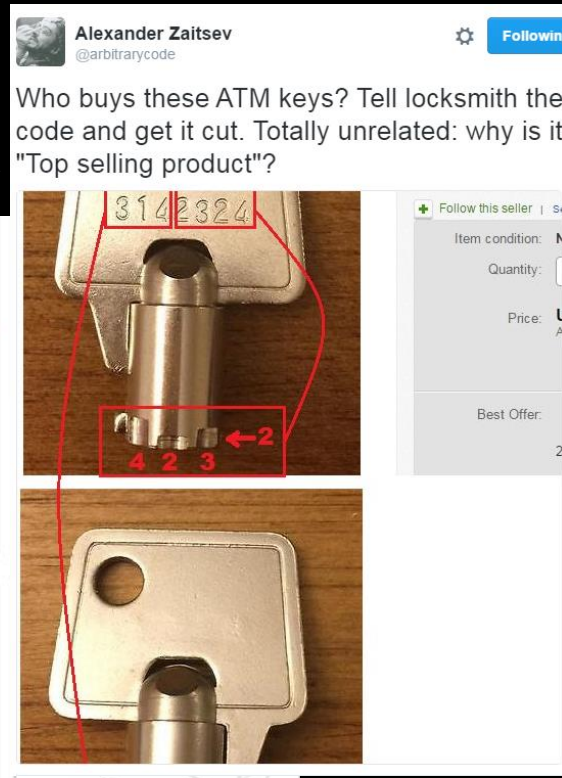
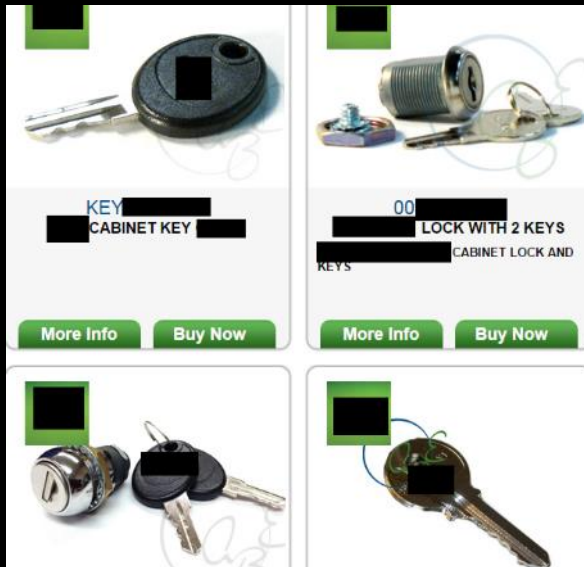
SERVICE ZONE

THERE IS NO CASH. REALLY?



HOW TO GET IN

- “MASTER KEY”
- SCREWDRIVER
- “SPECIAL” TOOL



VIDEO - HOW TO GET IN

[HTTPS://YOUTU.BE/KIJZHUTLJU](https://youtu.be/KIJZHUTLJU)



OUR SERVICE ZONE IS SECURED ©



SHOULD WE?

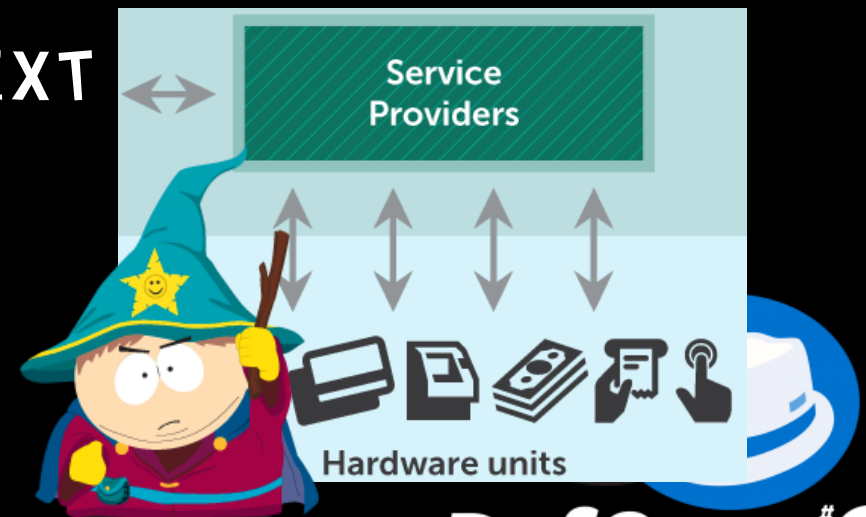


SERVICE PROVIDERS



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**



[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

```
1 $ sudo pip install frida
1 $ frida-trace -i "*dispens*" service_provider
```

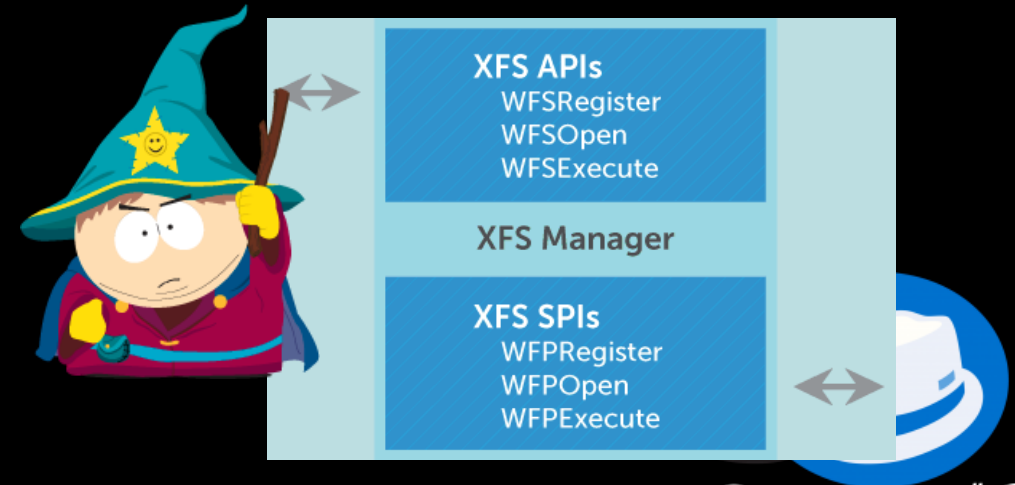
VIDEO – MALWARE NG

[HTTPS://YOUTU.BE/XOKG7HNVT20](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

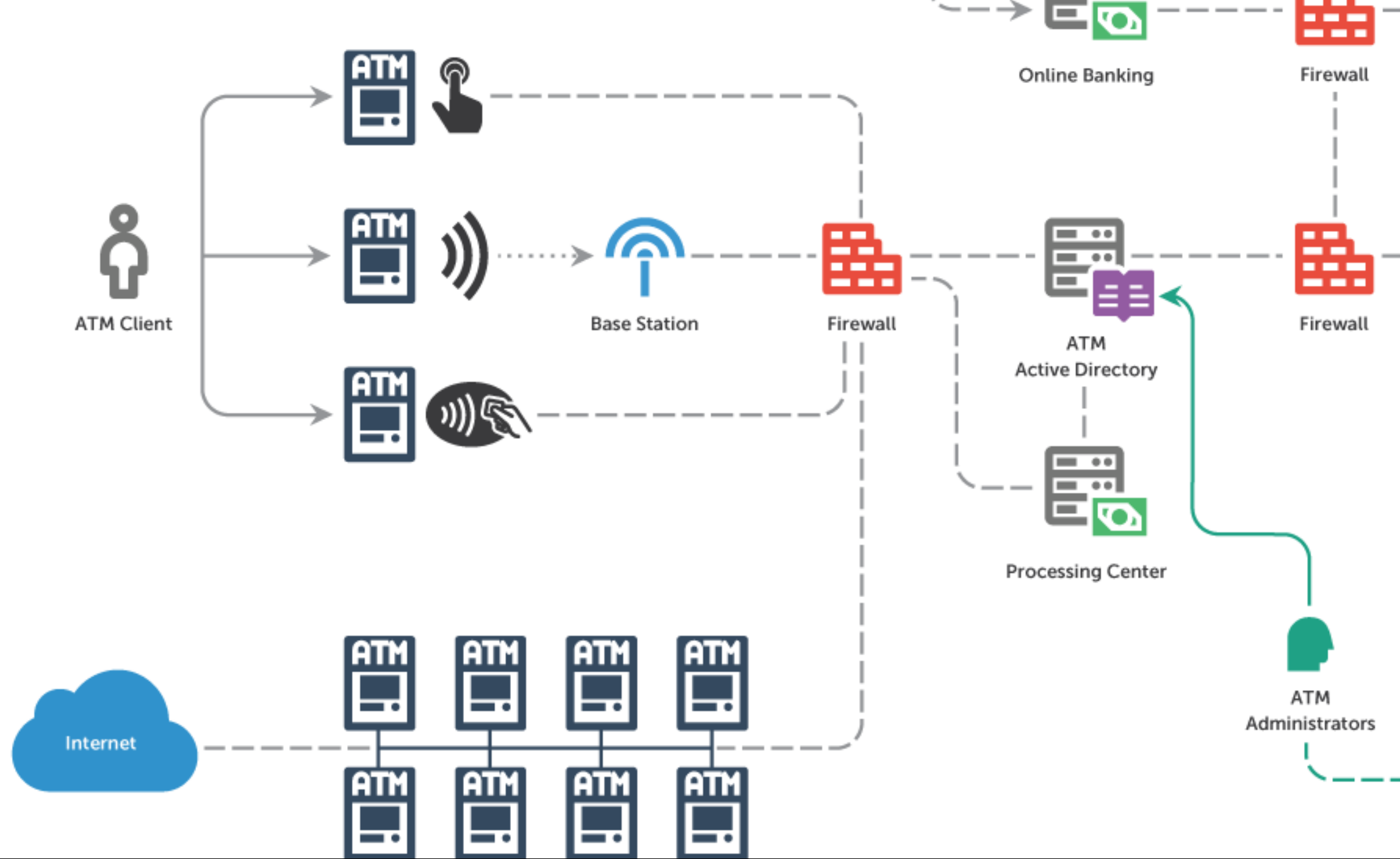
MS08-067 STRIKES AGAIN



JUST AHEAD

- OLD VERSIONS
- NOT UPDATED
- VULNERABILITIES
- STANDARD SERVICES





LET'S HAVE FUN WITH SHODAN

The screenshot shows the Shodan search results for the query 'country:PK'. The page displays a list of results, with the first result highlighted. The highlighted result is for a host with IP address 198.249.1.18, identified as PTCL. The result was added on 2015-01-06 15:12:48 GMT. The location is Pakistan, Islamabad. The hardware is x86 Family 6 Model 22 Stepping 1 AT/AT COMPATIBLE. The software is Windows 2000 Version 5.1 (Build 2600) Multiprocessor Free. The page also shows a sidebar with 'TOP COUNTRIES' and 'TOP CITIES'.

Showing results 1 - 10 of 1,491

198.249.1.18
PTCL
Added on 2015-01-06 15:12:48 GMT
Pakistan, Islamabad
Details

Hardware: x86 Family 6 Model 22 Stepping 1 AT/AT COMPATIBLE
Software: Windows 2000 Version 5.1 (Build 2600) Multiprocessor Free

TOP COUNTRIES

Country	Count
Pakistan	1,491

TOP CITIES

City	Count
Islamabad	1,115
Karachi	199
Lahore	90
Hyderabad	31
Rawalpindi	29

TOP ORGANIZATIONS

Organization	Count
PTCL	1,466
Pakistan Telecommunication Corporation	11
Pakistan Telecommunication Corporation	10
Transworld Associates (Pvt.) Ltd.	3
Karachi Pakistan	1

City: [REDACTED]
Country: [REDACTED]
Organization: [REDACTED]
ISP: [REDACTED]
Last Update: 2016-04-13T00:58:46.658804
ASN: [REDACTED]

The screenshot shows the Shodan Services page for the host 198.249.1.18. The page displays a list of services, with the first service highlighted. The highlighted service is NetBIOS Response, which shows the server name as ATN and the MAC address as f7:cf:bf. The service is also listed as 161, udp, and snmp. The hardware is x86 Family 6 Model 22 Stepping 1 AT/AT COMPATIBLE. The software is Windows 2000 Version 5.1 (Build 2600) Multiprocessor Free. The page also shows a sidebar with 'Services'.

Services

137
udp
netbios

NetBIOS Response
Servername: ATN
MAC: f7:cf:bf

Names:
ATN <0x0>
WORKGROUP <0x0>
ATN <0x20>
WORKGROUP <0x1e>
WORKGROUP <0x1d>
__MSBROWSE__ <0x1>

161
udp
snmp

Hardware: x86 Family 6 Model 22 Stepping 1 AT/AT COMPATIBLE
Software: Windows 2000 Version 5.1 (Build 2600) Multiprocessor Free

445
tcp
smb

Anonymous login successful

Sharename	Type	Comment
Error returning browse list: NT_STATUS_ACCESS_DENIED		
Anonymous login successful		
Server	Comment	
ATN		
Workgroup	Master	
WORKGROUP	ATN	

VIDEO – OBEY THE NET

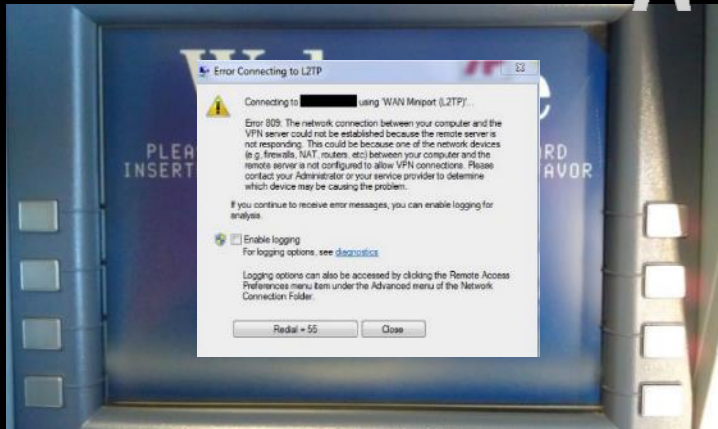
[HTTPS://YOUTU.BE/N9DJTY0-C00](https://youtu.be/N9DJTY0-C00)



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/NRBQBLBLLS](https://youtu.be/NRBQBLBLLS)



HACK THE BANK

HOW TO



WHAT TO BREACH

- **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



RULES

- READ FULL VERSION HERE [HTTPS://DEF.CAMP/HACK-THE-BANK/](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 ^_^





HAVE FUN STAY SAFE

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

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



DefCamp8
Where Hacking & Security Collide