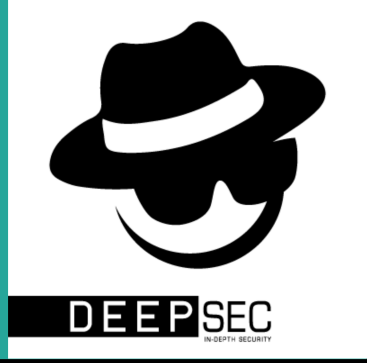


Everything Is Connected: How To Hack Bank Account Using Instagram

Aleksandr Kolchanov

About me

- Now I'm an independent security researcher
- Ex russian bank security researcher
- Ex aircompany security consultant

Interests

- Mobile operators security
- Banks security
- Uncommon attacks
- Social networks threats

Plan for this talk

1. Let’s just search a cards
2. Security of call centers of banks
3. Which information is required to spoof an identity when call
4. People publish all necessary information in social networks
5. Use photo of plane ticket to hack bank? Is it real? Practical case
6. And some perspectives

An unexpected question: is it easy to find information about valid bank card on the Internet?

But people do it

Just use some tags in Instagram

[redacted]

21 отметок "Нравится"

19 ДЕКАБРЯ 2017 Г.

Войдите, чтобы поставить «Нравится» или прокомментировать.

[redacted]

10 отметок "Нравится"

27 ИЮНЯ

Войдите, чтобы поставить «Нравится» или прокомментировать.

45 отметок "Нравится"

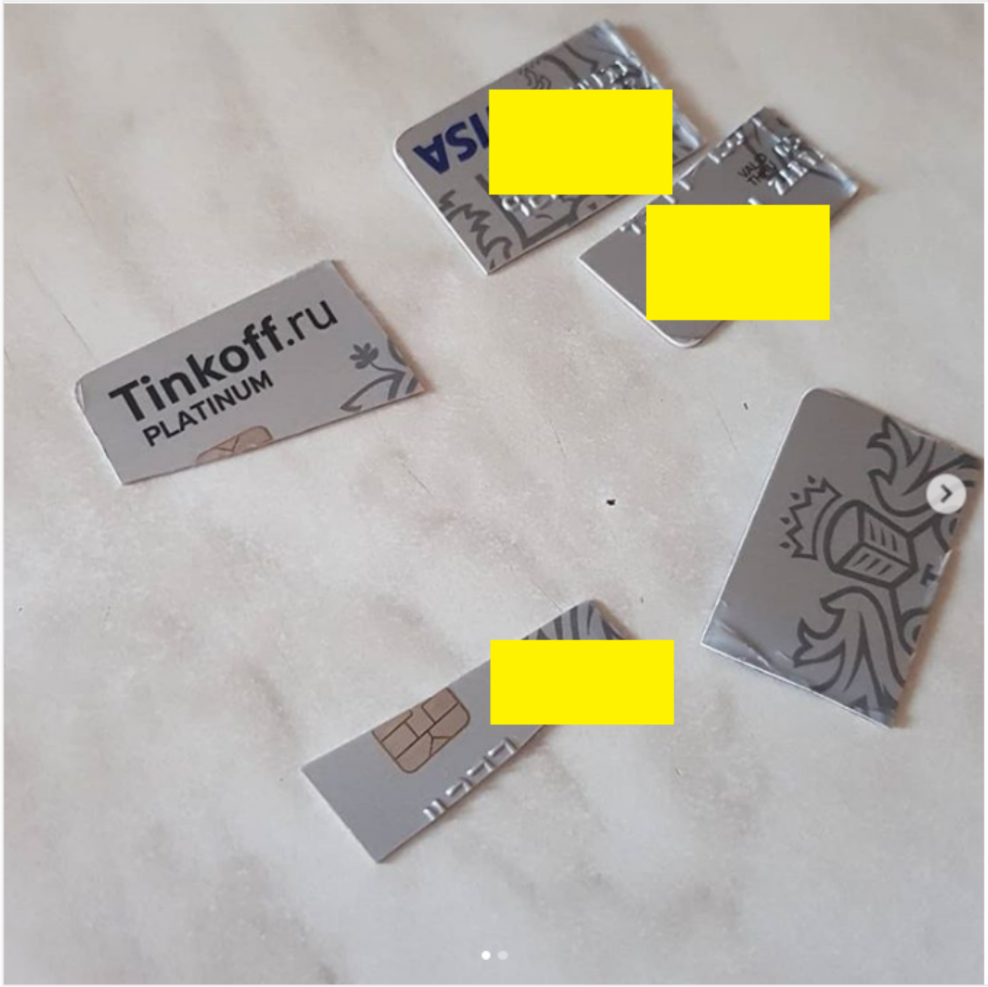
3 ДЕКАБРЯ 2016 Г.

Войдите, чтобы поставить «Нравится» или прокомментировать.

12 отметок "Нравится"

19 АВГУСТА

Войдите, чтобы поставить «Нравится» или прокомментировать.



52 отметок "Нравится"

29 ИЮНЯ

Войдите, чтобы поставить «Нравится» или прокомментировать.

Popular tags in different languages

- Card
- Creditcard
- Newcard
- [bank title]
- Bank
- Money
- Salary

Bank call center

Call to the bank
Use IVR (Interactive Voice Menu) or ask a employee
Sign in (with code, password or card data, or something else)
Get information about account or do something (like money transfer)

- Card balance
- List of payments
- Information about deposits and credits
- Send money or refill phone
- Change phone number

How to attack IVR system?

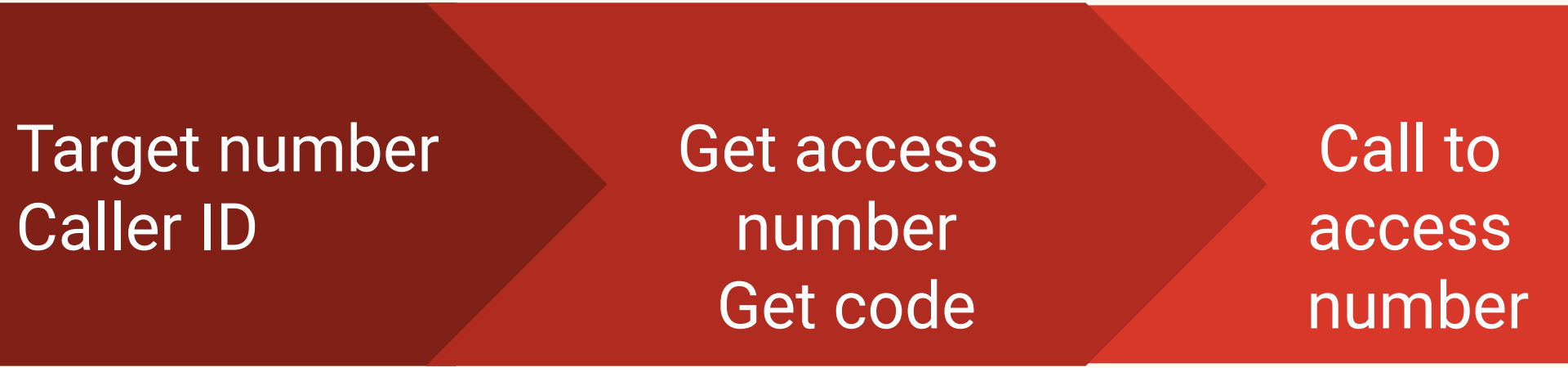
Basic idea

Call to the bank with spoofed Caller ID (phone number)
Bypass an authentication
Do some actions or get information

Authentication

- Only caller ID (phone number)
- Card information
- Passport or ID information
- Code word
- SMS-code
- Biometric

How to make a call with spoofed Caller ID?



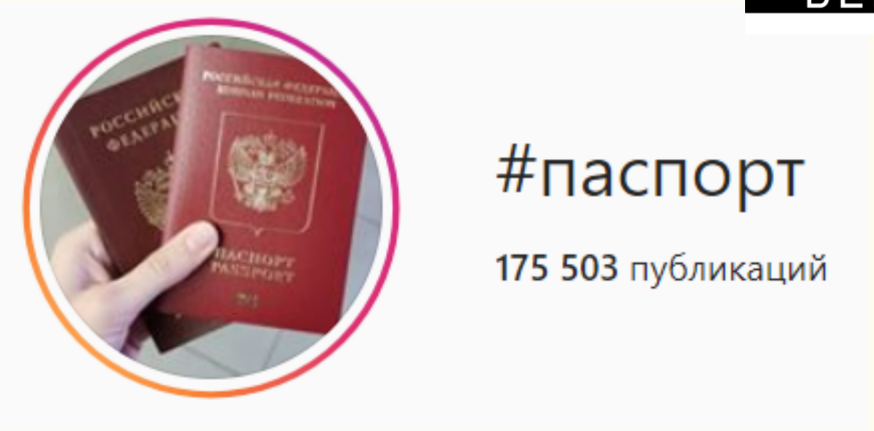
We already know, how attacker can find card information

But what about passports and IDs?

Just use Instagram again

Popular tags in different languages

- Passport
- 14years
- NewPasport
- Road
- PriorityPass



Also, you can find some interesting flashmobs

Where else attacker can gain access to the necessary passport data?

Aircompany!

Just hack personal accounts, they are not usually so secure
GDS systems
Bruteforce “Check booking” services
Visit airport and search for boarding pass and luggage tags
Find tickets at the social networks

- Passport Data
- Phone number
- Part of card data
- Data of other passengers

GDS

- PNR (passenger name record)
- Last name


الإتحاد
ETIHAD
AIRWAYS
ECONOMY
GUEST KOLCHANOV/ALEKSANDR
FLIGHT NO EY 280
DATE 030CT
DEPARTS 2135
FROM ABU DHABI INTL
ARRIVES 0310
TO KOCHI
GATE 37
BOARD TIME 2035
ZONE 4
SEAT 21B
PNR N
SEQ 023
AGT DMEGIZ
PW

S7 Airlines

Посадочный талон Boarding pass

ETK:4212[redacted]

ИМЯ ПАССАЖИРА/PASSENGER NAME
KOLCHANOV/ALEKSANDR

N РЕГ/SEQ 67

ОТ/FROM ST. PETERSBURG LED
ДО/TO DOMODEDOVO-MOSC DME

РЕЙС/FLIGHT КЛАСС CLASS МЕСТО SEAT
S7 0038 Q 9F

ДАТА/DATE ВРЕМЯ/TIME
03OCT 05:20

ВЫХОД GATE ПОСАДКА ДО BOARD.TILL
D01 04:50

BAG NO SNR NO

2173 Д СПТ

Посадочный талон
Boarding pass

N РЕГ/SEQ 67
KOLCHANOV/ALEKSANDR
ОТ/FROM ST. PETERSBURG
ДО/TO DOMODEDOVO-MOS
РЕЙС КЛАСС ДАТА ВРЕМЯ
FLIGHT CLASS DATE TIME
0038 Q 03OCT 0520
ВЫХОД ПОСАДКА ДО МЕСТО
GATE BOARD TILL SEAT
D01 04:50 9F

ETK:42[redacted]

Passengers

Refund the ticket

Mr Kolchanov Aleksandr Adult

Ticket number 42[redacted]

Date of birth 06 January 1997

Document number 72[redacted]

☐ Add FFP card to receive miles for your flight

Contact

Email: pyrk1@mail.ru

Telephone number 792[redacted]

Payment history

02 October 2018

Paid [redacted] RUB

Visa [redacted] **** **** [redacted]

ALEKSANDR KOLCHANOV

Flight [redacted] RUB

St Petersburg (LED) – Moscow (DME) 03 October 2018

1 adult [redacted] RUB

Taxes [redacted] RUB

Service fee 100 RUB

GDS

Check with different GDS systems
Check with the aircompany systems

- Boarding Pass
- Luggage tag
- Passport data at the Boarding Pass
- Call to ticket company and ask for PNR

Practical case with Privatbank

- Use international number +38-056-716-11-31
- Spoof any Caller ID
- Information about deposits and credits will be available without any additional authorisation

Practical case with Privatbank 2

Hacker can use last 4 digits of card number to:

- Gain access to balance information
- Block card
- Change PIN to random

Practical case with Privatbank 1

They don’t ask any information to confirm phone refill

Just “If you want to refill from card *07 press 1”

Practical case with Privatbank

There are some additional things, hacker can do via IVR

And...

Practical case with Privatbank

This is not 0-day vulnerability

This is 438-day accepted risk

I sent this problem to BugBounty without any results

Practical case with Privatbank !

Anybody can gain access to information about all clients of the largest commercial bank in Ukraine

¯_(ッ)_/¯

Any questions?

Aleksandr Kolchanov - pyrk1@yandex.ru