F-Secure | LABS

BSides Athens

CLICK HERE FOR FREE TV!

Chaining bugs to takeover Wind Vision accounts

Leonidas Tsaousis

Security BSides Athens – June 2021

LABS

OUTLINE

1. Introductions
2. Analysis
3. Disclosure
4. Conclusion



LABS

WHOAMI

- security consultant at F-Secure (ex-MWR)
- OSEP / OSCP
- rookie speaker
- mobsec afficionado
- @laripping

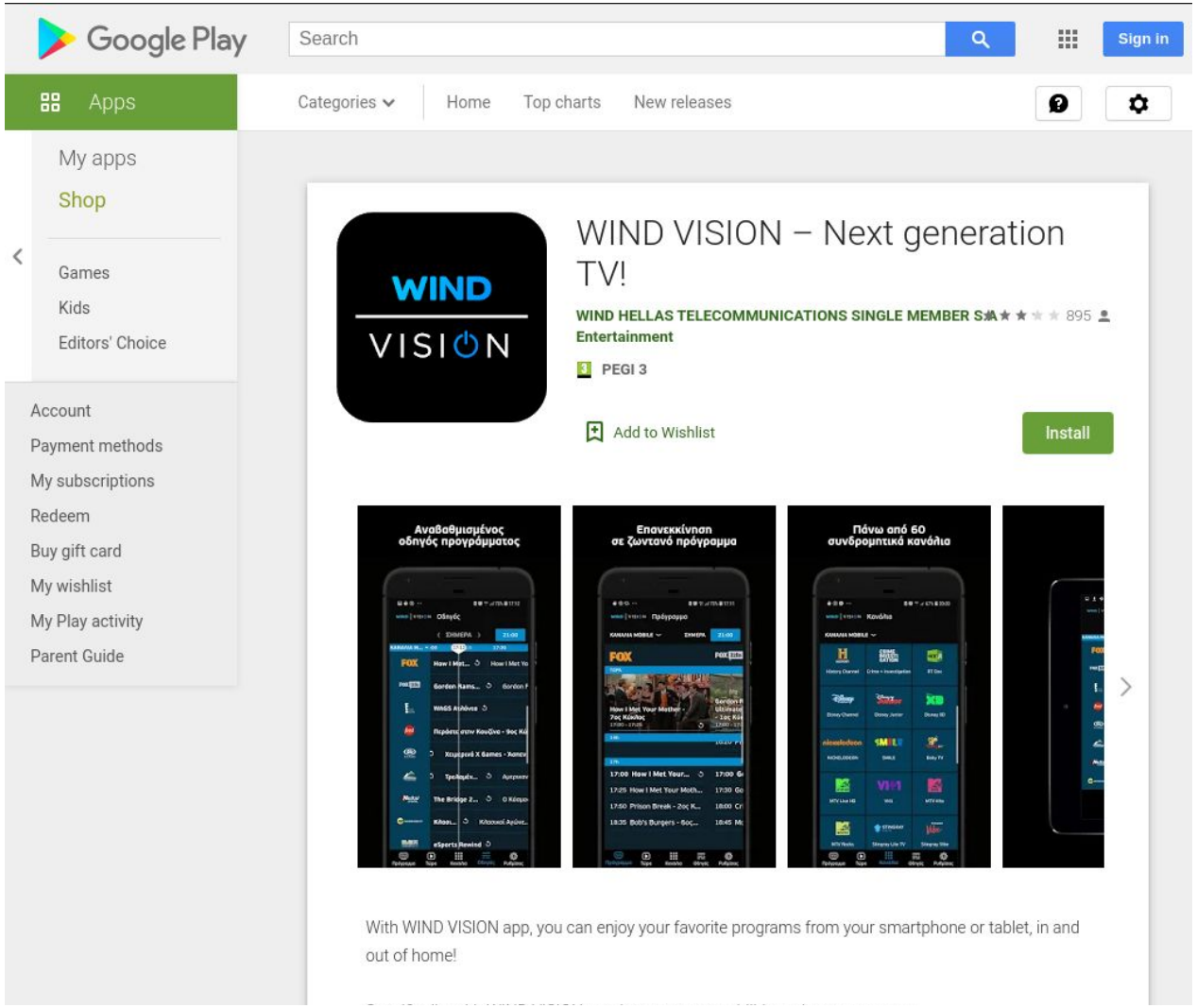
WIND WHO?

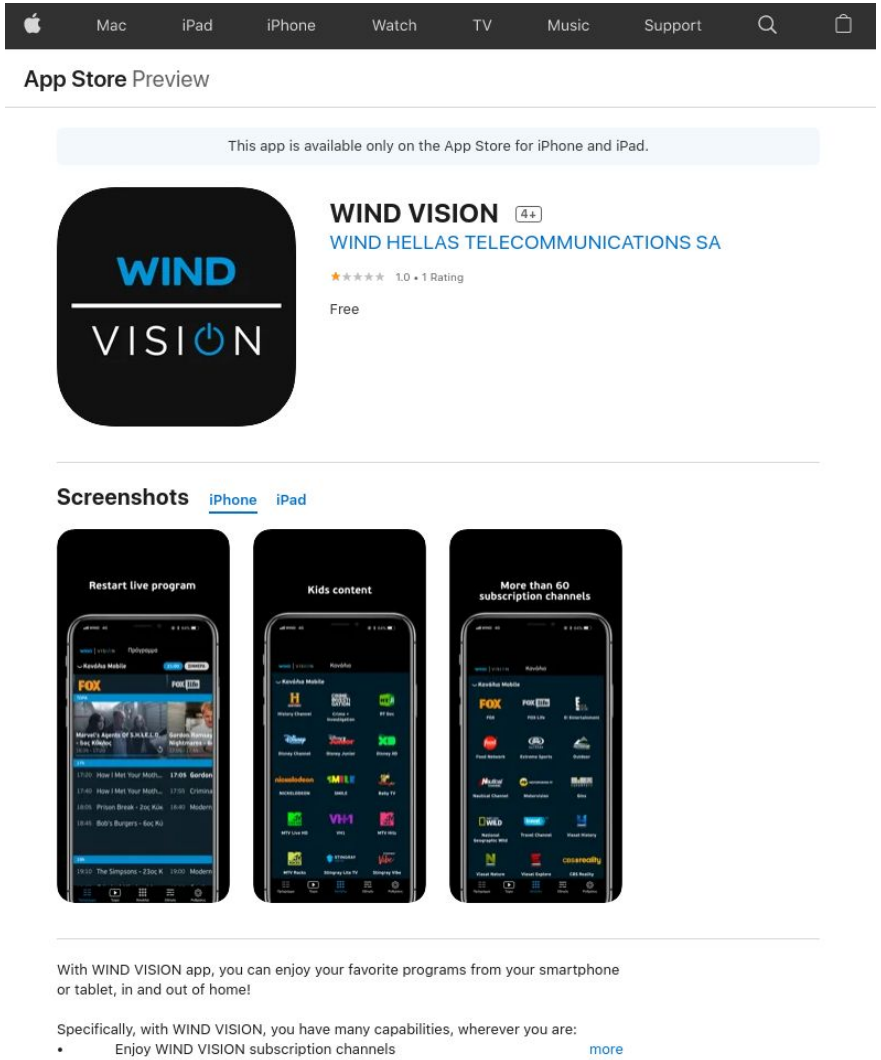
LABS



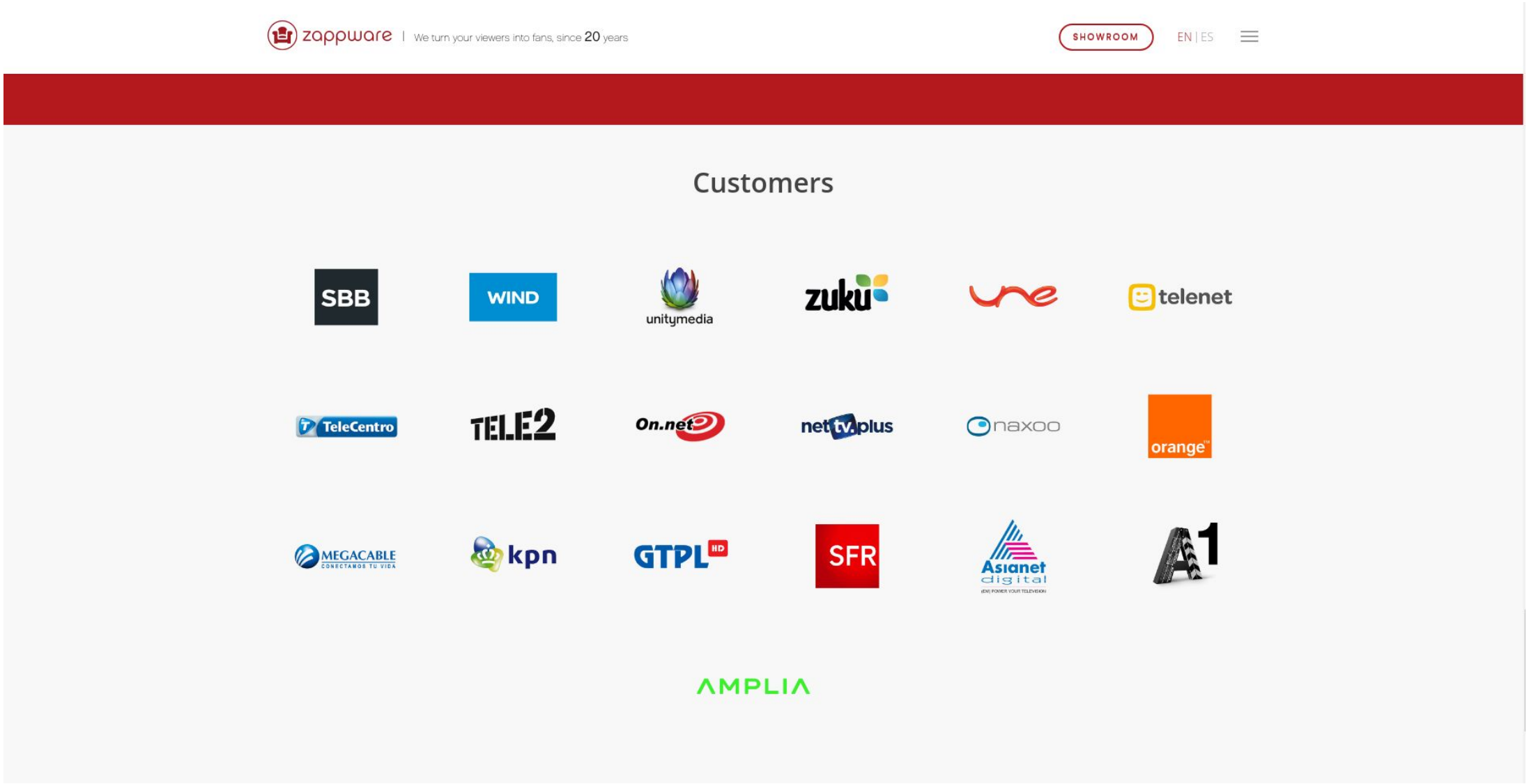
LABS

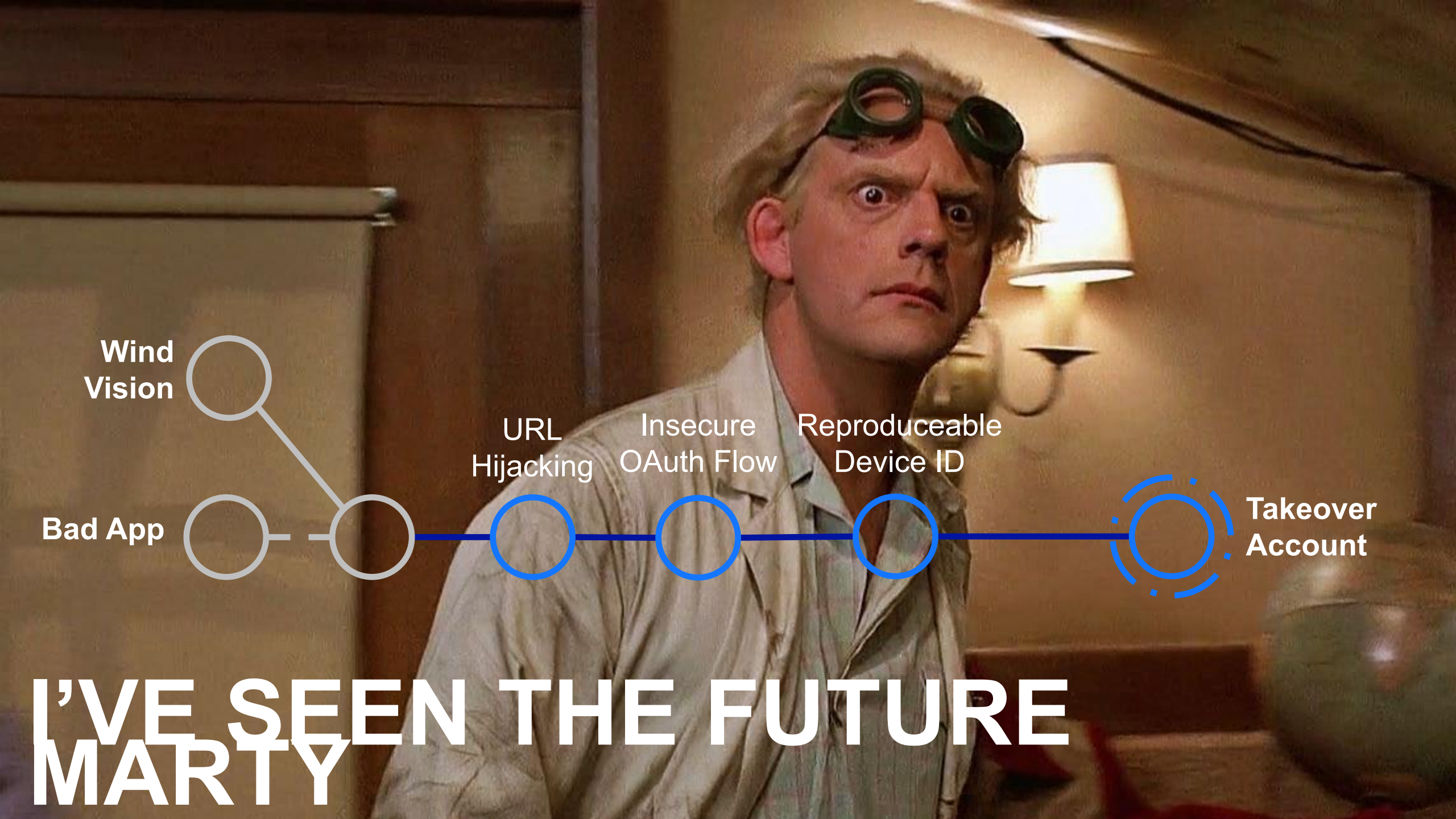
WIND WHO?





ZAPP-WHAT?

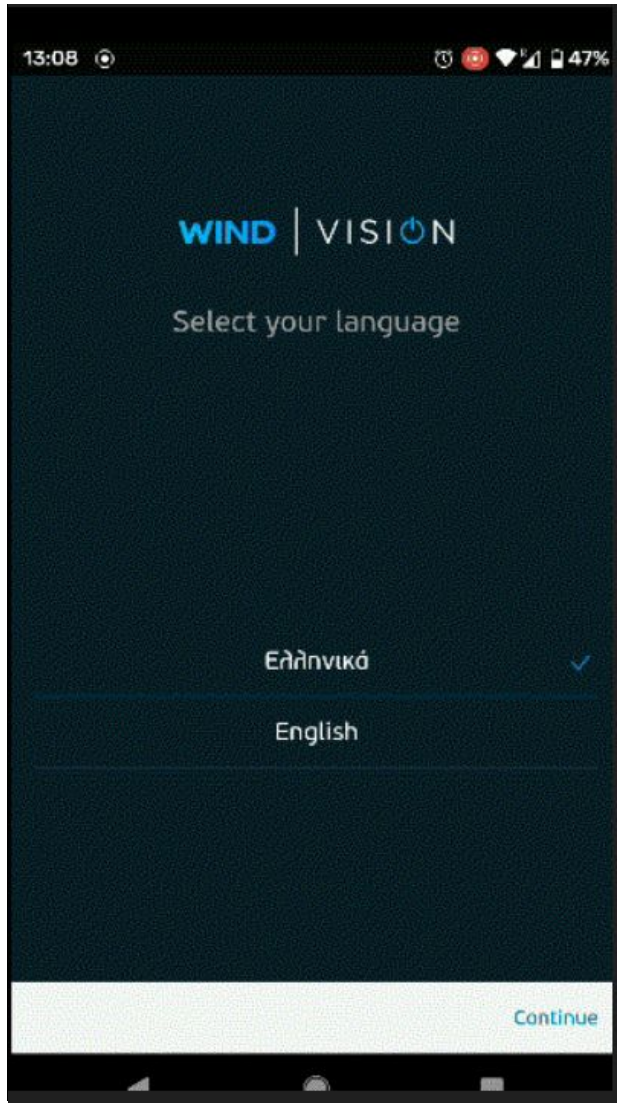

zappware | We turn your viewers into fans, since 20 years
SHOWROOM
EN | ES
Customers
SBB
WIND
unitymedia
zuku
telenet
TeleCentro
TELE2
On.net
net tv plus
naxoo
orange
MEGACABLE
kpn
GTPL HD
SFR
Asianet digital
A1
AMPLIA

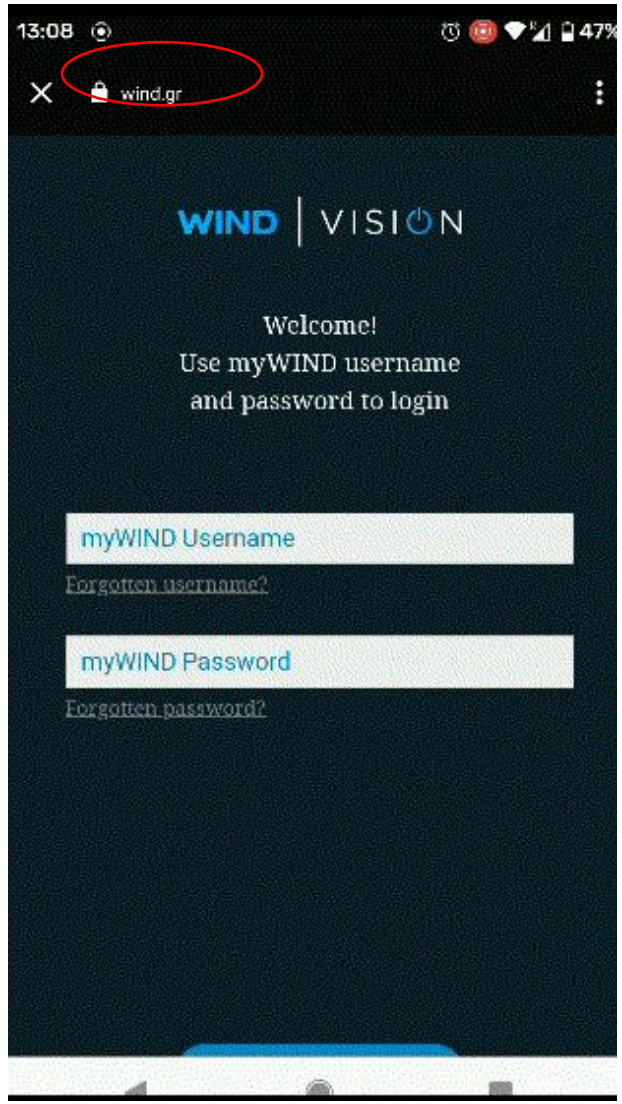

Wind Vision
Bad App
URL Hijacking
Insecure OAuth Flow
Reproduceable Device ID
Takeover Account
I'VE SEEN THE FUTURE MARTY

ANALYSIS

LABS

IN AND OUT OF CHROME…





…USING LINKS

```
<activity
    android:name=".MainActivity"
    android:label="Complete Login"
    <intent-filter>
        <action android:name="android.intent.action.VIEW" />
        <category android:name="android.intent.category.DEFAULT" />
        <category android:name="android.intent.category.BROWSABLE" />
        <data
            android:host="pridp.wind.gr"
            android:path="/AuthCallback"
            android:scheme="nexx4" />
```

nexx4://pridp.wind.gr/AuthCallback?code=8bd470fa1631afe325c409ff2098b768b613a4f513d0bc2b6c710af660527281

LABS

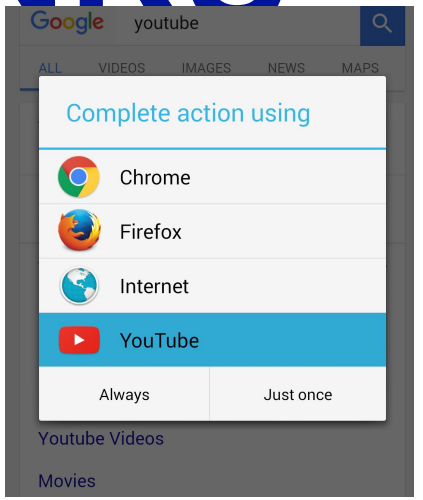
…DEEP LINKS

```
<activity
    android:name=".MainActivity"
    android:label="Complete Login"
    <intent-filter>
        <action android:name="android.intent.action.VIEW" />
        <category android:name="android.intent.category.DEFAULT" />
        <category android:name="android.intent.category.BROWSABLE" />
        <data
            android:host="pridp.wind.gr"
            android:path="/AuthCallback"
            android:scheme="nexx4" />
```

nexx4://pridp.wind.gr/AuthCallback?code=8bd470fa1631afe325c409ff2098b768b613a4f513d0bc2b6c710af660527281

LABS

DEEP LINKS VS APP LINKS



https://www.youtube.com/.

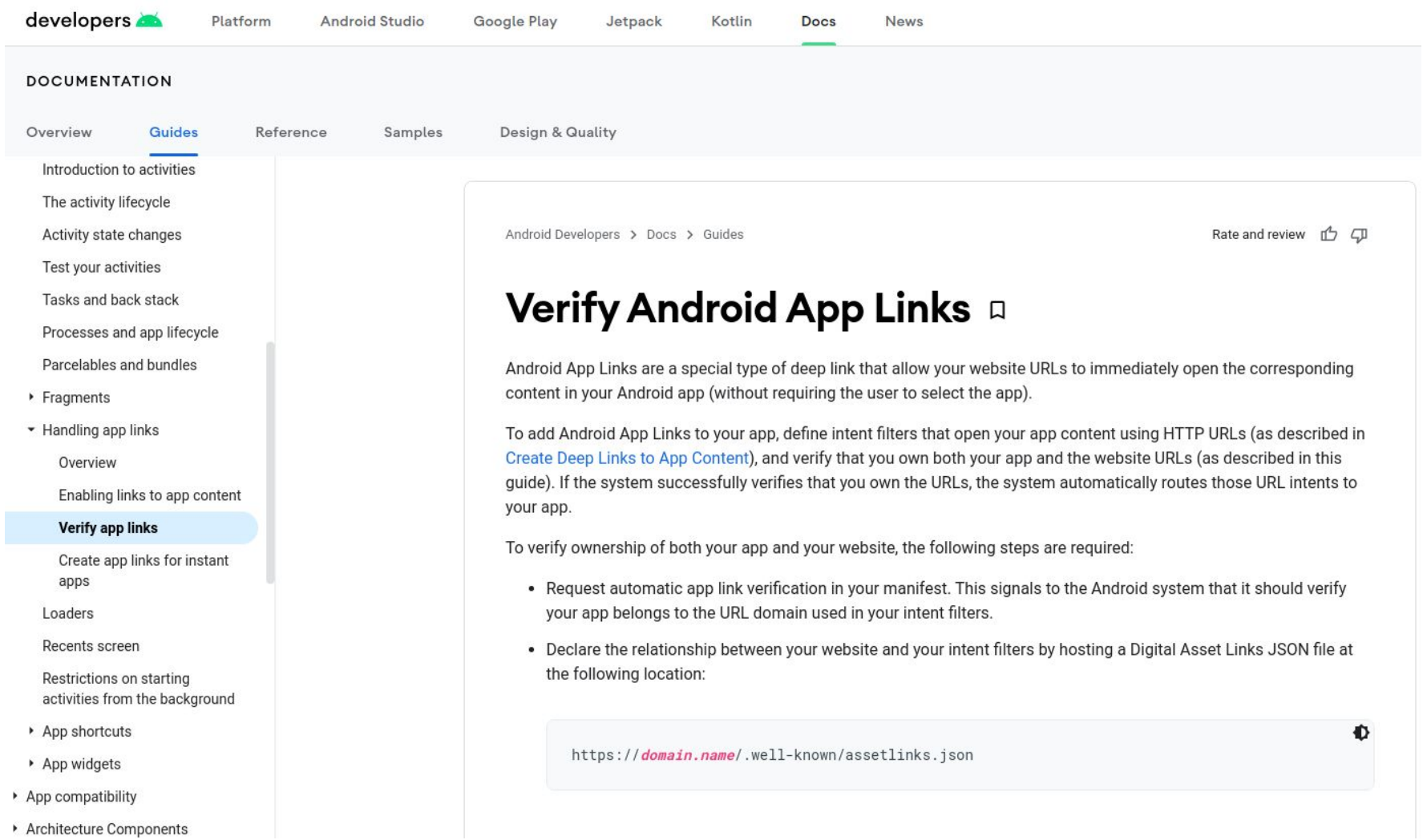
<intent-filter>

<intent-filter android:autoVerify=true>*



* + Digital Asset Link (DAL)
JSON

DAL VERIFICATION




OKAAAAY, MOVING ON
LABS

LABS

WEB TRAFFIC ANALYSIS







Request

Pretty | Raw | \n | Actions | Select extension...

```
POST /secure/v1/graphql/ HTTP/1.1
Host: client.tvclient.wind.gr
User-Agent: android phone
Authorization: AWS4-HMAC-SHA256 Credential=ASIAUN3BNO3K7P2F6JP6
Device-Id: R2pNREh7R2FWdE1tUGhTUW1ua2d5cFlZaWFmZHhEWQA99
Content-Type: application/json; charset=utf-8

{
  "query":"query User {  me {  __typename  id  firstName  guestMode  household {  __typename  ...
    __typename  id  items {  __typename  ...vodAssetEntitlementFragment  product {  __typename  ...vo
    } } community {  __typename  ...communityInfo } devices {  __typename  ...deviceCatalogFragment }
  e {  __typename  id  name  kind  pincode  permissions {  __typename  parentalRating {  __typename  ..
    registrationTime  removable  removableFrom  deviceType  previewModeEnabled  deviceEnablementPolicies {  __typ
  t {  __typename  ...vodProductEntitlementFragment }}fragment vodProductEntitlementFragment on ProductEntitle
  "operationName":"User",
  "variables":{
  }
}
```

Response

Pretty | Raw | Render | \n | Actions

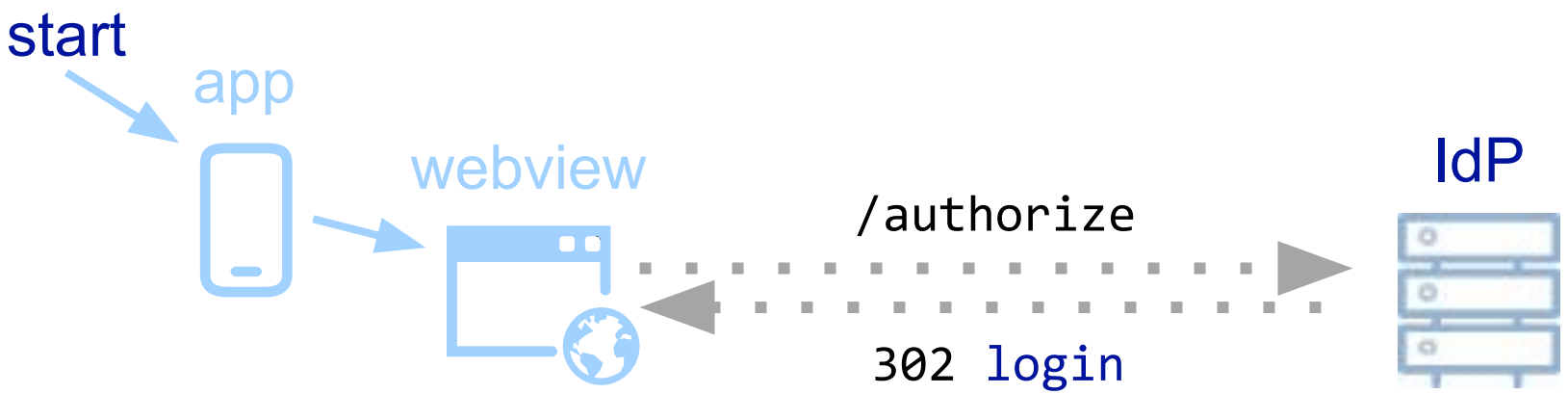
```
HTTP/1.1 200 OK
Content-Type: application/json;charset=utf-8
Content-Length: 4575
Connection: close
Date: Sun, 13 Sep 2020 21:09:23 GMT
x-amzn-RequestId: 5b280f75-ec55-40e9-bfd2-ccb1de23a517
x-amzn-Remapped-Connection: keep-alive
x-amz-apigw-id: S0qUfE8IDoEFU7w=
Vary: Origin
x-amzn-Remapped-Server: nginx/1.13.8
Access-Control-Expose-Headers: Access-Control-Allow-Methods,Access-Control-
x-amzn-Remapped-Date: Sun, 13 Sep 2020 21:09:23 GMT
Access-Control-Allow-Credentials: true
X-Cache: Miss from cloudfront
Via: 1.1 71ac5938fae2311667bfbb1e1df1d673.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: LHR62-C4
X-Amz-Cf-Id: bbzlRJB1JDTwxBmLmdXRXXgSlTOJw8Y9KMd6CGz9ip9Hk9tA5p-UEA==

{
  "data":{
    "me":{
      "__typename":"User",
      "id":"NDEwNjQ1MjQzMVIycE5SRWg3UjJGV2RFMXRVR2hUVVcxdWEyZDVjRmxaYVdGbVp
      "firstName":null,
```

LABS

THE AUTH FLOW (1/5)

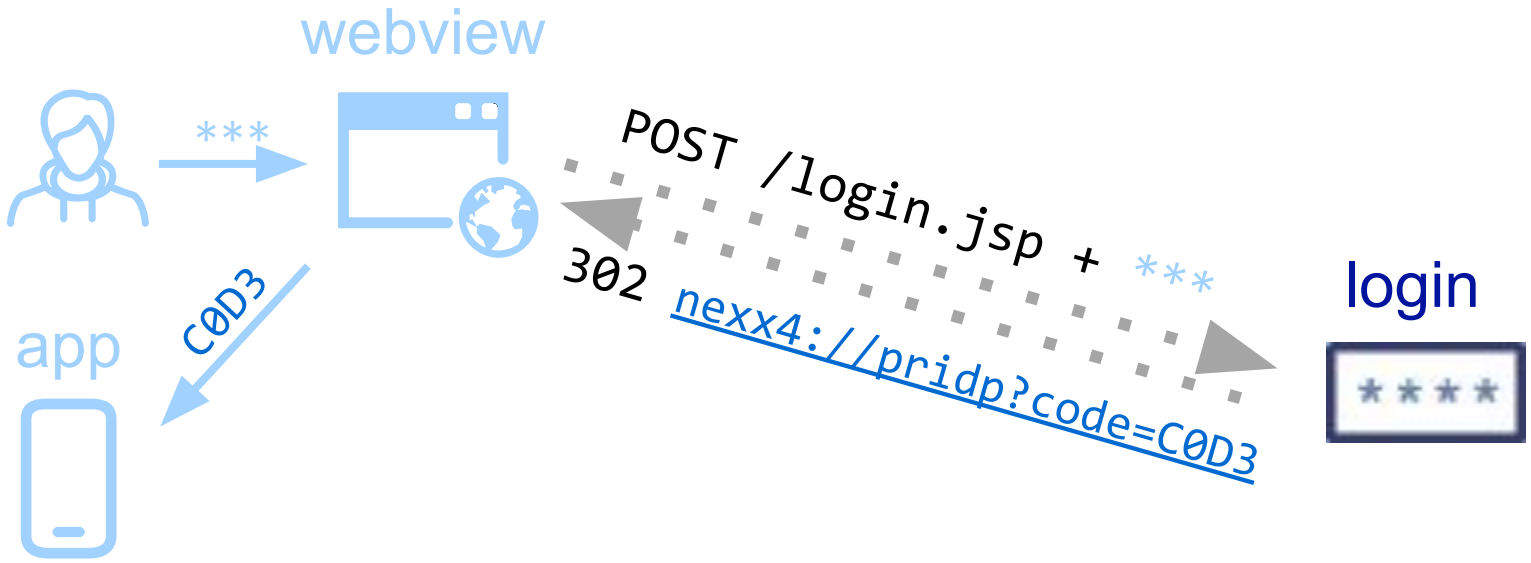
1. Authorization



LABS

THE AUTH FLOW (2/5)

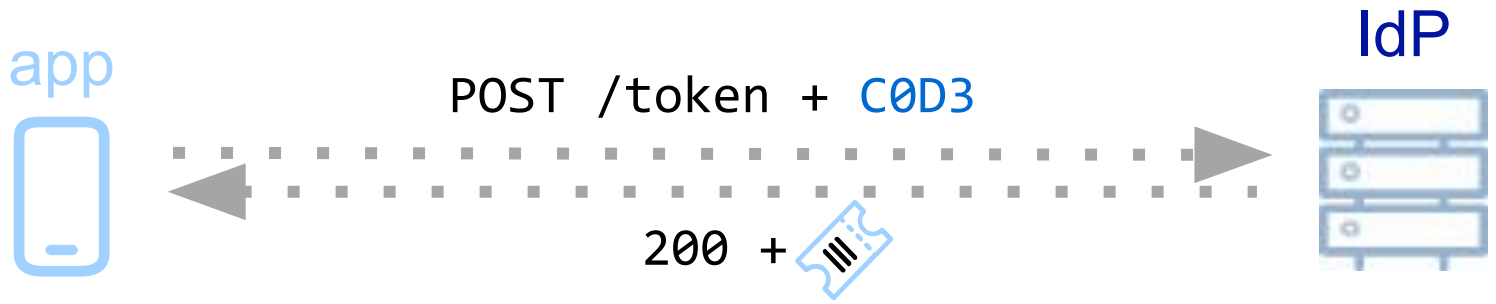
1. Authorization
2. Password for Code



THE AUTH FLOW (3/5)

LABS

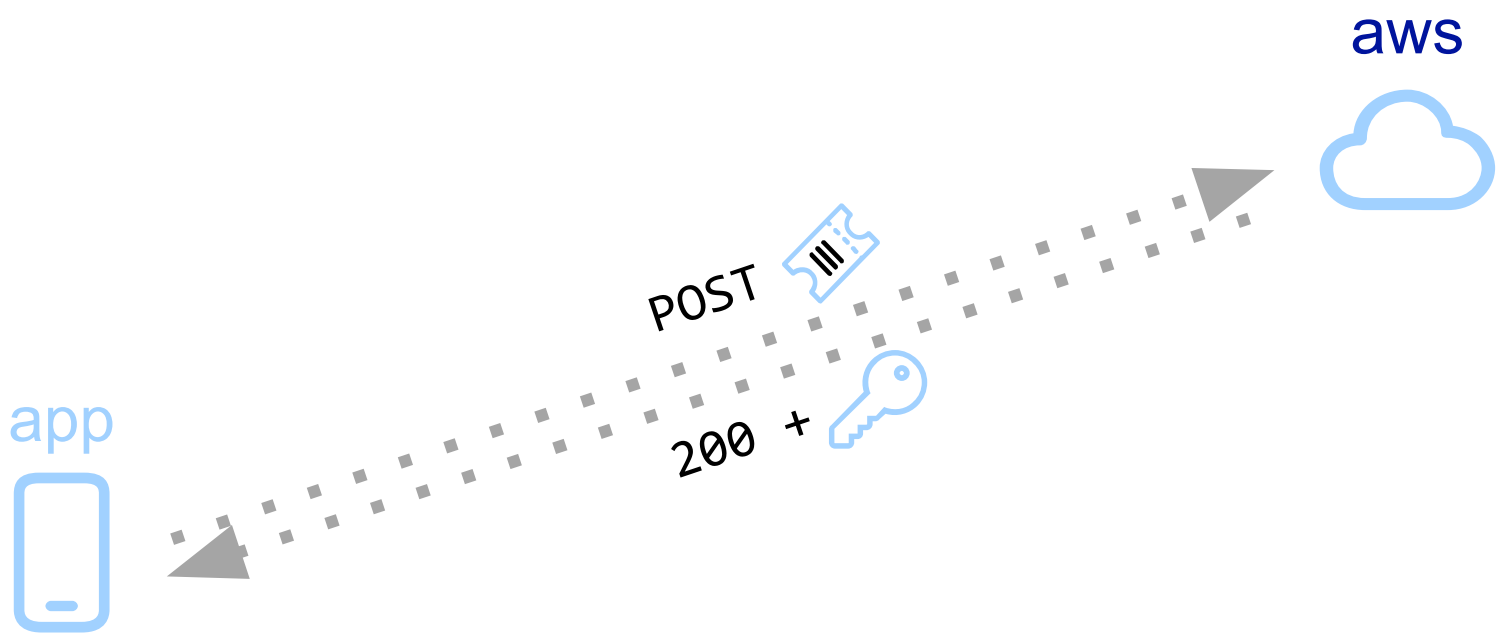
1. Authorization
2. Password for Code
3. Code for Token



THE AUTH FLOW (4/5)

LABS

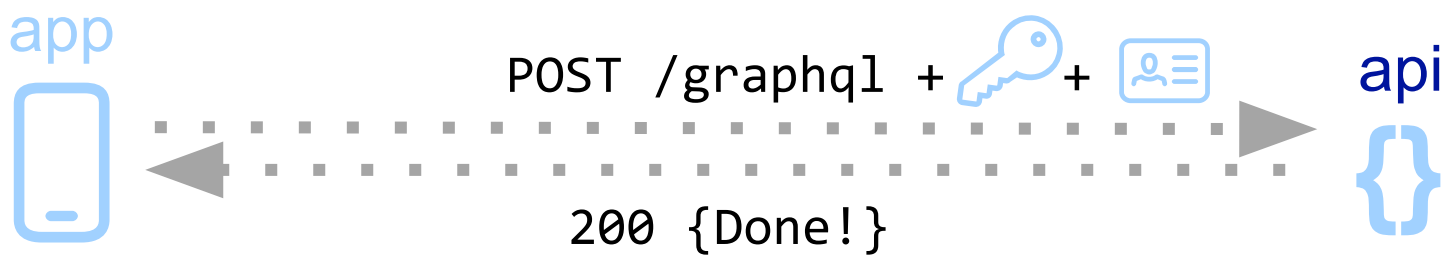
1. Authorization
2. Password for Code
3. Code for Token
4. Token for Key



THE AUTH FLOW (5/5)

LABS

1. Authorization
2. Password for Code
3. Code for Token
4. Token for Key
5. API request

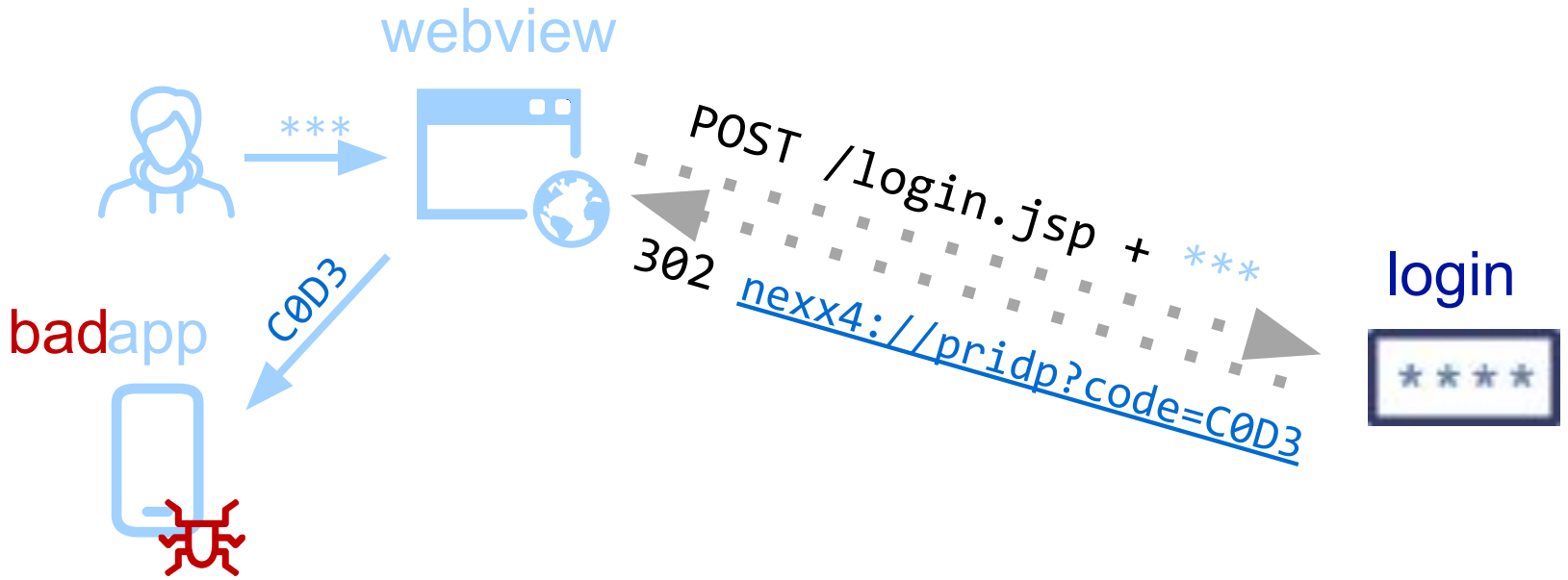


THE AUTH FLOW (2/5)

LABS

1. Authorization
2. Password for Code
3. Code for Token
4. Token for Key
5. API request

Assumed URL hijack

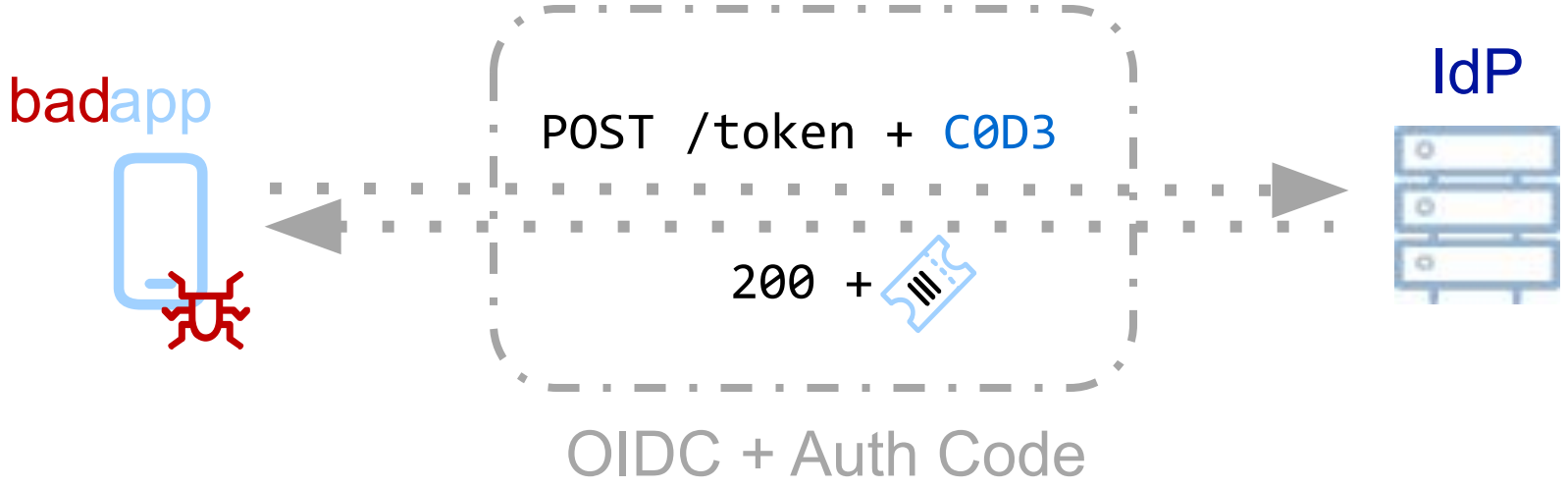


LABS

THE AUTH FLOW (3/5)

Assumed URL hijack

1. Authorization
2. Password for Code
3. Code for Token
4. Token for Key
5. API request



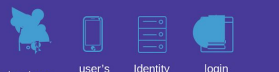
LABS


Sponsored By
okta
Protecting Mobile Apps with PKCE
17
The Proof Key for Code Exchange (PKCE, pronounced pixie) extension describes a technique for public clients to mitigate the threat of having the authorization code intercepted. The technique involves the client first creating a secret, and then using that secret again when exchanging the authorization code for an access token. This way if the code is intercepted, it will not be useful since the token request relies on the initial secret.
The full spec is available as RFC7636. We'll cover a summary of the protocol below.
Authorization Request
Authorization Code Exchange
home
security fundamentals
security guidelines
improve this document
discover firefox
mon abbreviations & definitions
Full and related names
Description
Login
The act of verifying a user identity, i.e. they say they are.
role, groups, attributes, access control list, scopes
OpenID Connect
Open standard for access delegation.
Egor Homakov
Security consulting: Sakurity Twitter: @homakov. homakov@gmail.com
Tuesday, July 3, 2012
The Most Common OAuth2 Vulnerability
HN discussion
TL;DR
If website uses OAuth multi-logins there is an easy way to log into somebody's account, protection is almost never implemented and people don't take into account that OAuth is also used for authentication.
OAuth2 is an authorization framework. Apparently it's very popular now. Disregards its popularity a lot of people don't understand it deeply enough to write proper and secure implementation.
OAuth1.a and OAuth2 are incompatible, some services use former(twitter, wtf, come on!), some latter, some of them have insufficient and poor documentation(in terms of security) etc. It took me a few hours to read OAuth2 draft thoroughly and I found a few interesting vectors. One of them I am exposing in this post.
It's really dangerous but very common vulnerability for multi-login OAuth websites.
A little bit of theory:
response_type = code is server-side auth flow, should be used when possible, more secure than response_type = token. Provider returns 'code' with User's user-agent and Client sends along with client's credentials the code to obtain 'access_token'. Callback when user is redirected looks like site.com/oauth/callback?code=AQCOtAVov1Cu316rpqPfs-8nDb-jJEiF7aex9n05e2dq3oiXlDwubVoC8VEGNq10rSkyyFb3wKbtZh6xpgG59FsAMMSjlAr613Ly1usZ47jPgADzbDyVuotFaRiQux3g6Ut84nmAf9j-KEvsX0bEPH_aCekLNJ1QAnjpls0SL9ZSK-yw1wPQWQsBhbfMPNJ_Lql
I remind you, OAuth is all about authorization, not authentication. What's the difference
THE GOOD
THE BAD
and THE UGLY

IT’S SO EASY WITH PKCE

LABS

OAuth2 with PKCE



0. Registration



Registers client with Identity Provider (IDP)

The IDP will assign a **client_id** for the app (e.g. 123)

Developer registers **redirect_uri** with the IDP (e.g. myapp://auth)

AUTH FLOW

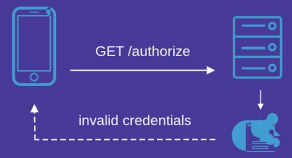
1. Before auth



Generates **state** and **code_verifier**

These are both random strings that are kept in-memory on the device

2. App starts the auth request



/authorize URL parameters:

response_type = code
client_id = 123
redirect_uri = myapp://auth
scope = email
state = **state**
code_challenge = sha256(**code_verifier**)
code_challenge_method = sha256

3. IDP links back to the app with the auth code



Deep link looks something like this:

myapp://auth?code= **code**&state= **state**

A new **code** is generated by the IDP for each auth session

PKCE STEP

4. Token Exchange



/post data:

grant_type = authorization_code
code = **code**
redirect_uri = myapp://auth
client_id = 123
code_verifier = **code_verifier**

PKCE

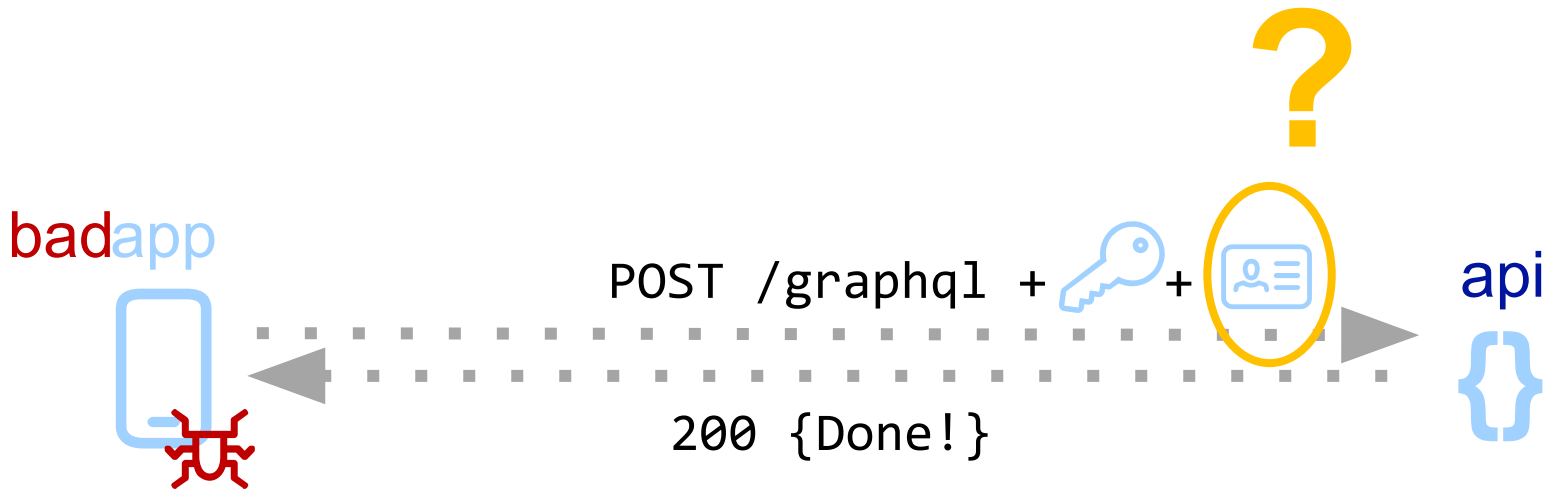
IDP checks that sha256(**code_verifier**) = **code_challenge** before returning the JWT

Icons from Flaticon flaticon.com/authors/freepik

LABS

URL HIJACK + NO PKCE =FULL TAKEOVER?

1. Authorization
2. Password for Code
3. Code for Token
4. Token for Key
5. API request?



WE’RE STUCK

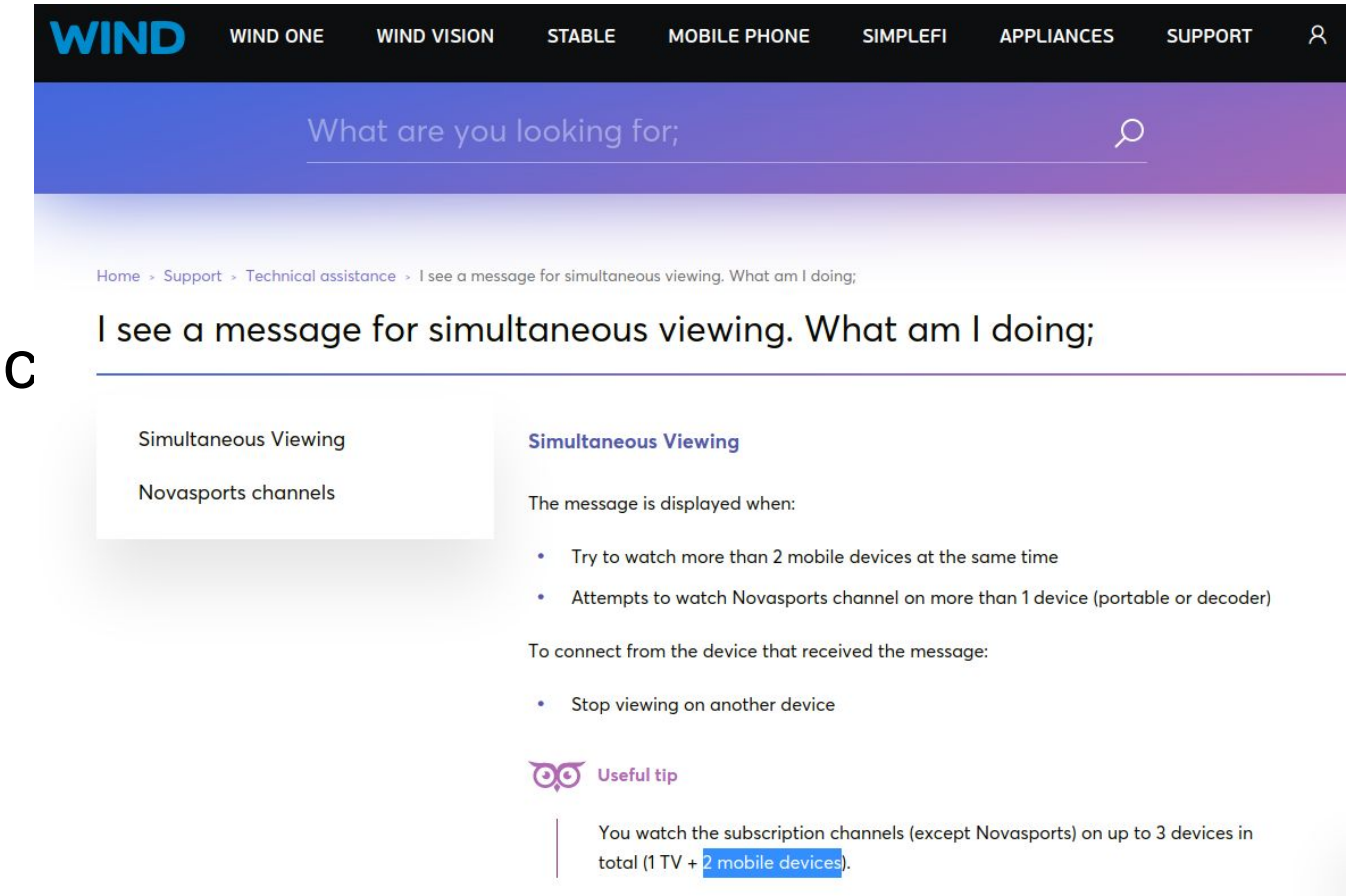


DEVICE-ID?

"A valid `Device-ID` is one that has been previously uploaded to the server, generated locally after the registration of a new device"

A bad app can either:

- Register a new Device-ID
  - potentially clearing existing devic
- Guess an existing Device-ID



DEVICE-ID GENERATION



LABS

DEVICEID RE-GENERATION

```
private void calculateDeviceId() {
    UUID UUID = new UUID(-1301668207276963122L, -6645017420763422227L);
    byte[] deviceUniqueID = new byte[0];
    deviceUniqueID = new MediaDrm(UUID)
            .getPropertyByteArray(MediaDrm.PROPERTY_DEVICE_UNIQUE_ID);
    String id = Base64.encodeToString(deviceUniqueID, 2)
            .replaceAll("=", "99")
            .replaceAll("/", "88")
            .replaceAll("\\+", "77");
    if (id.length() >= 100) {
        id = id.substring(0, 99);
    }
    Log.d("DLA", "ID calculated is: "+id);
}
```

random?

MediaDrm — Added in API level 18

```
public MediaDrm (UUID uuid)
```

Instantiate a MediaDrm object

Parameters	
uuid	UUID: The UUID of the crypto scheme. This value cannot be null.

PROPERTY_DEVICE_UNIQUE_ID — Added in API level 18

```
public static final String PROPERTY_DEVICE_UNIQUE_ID
```

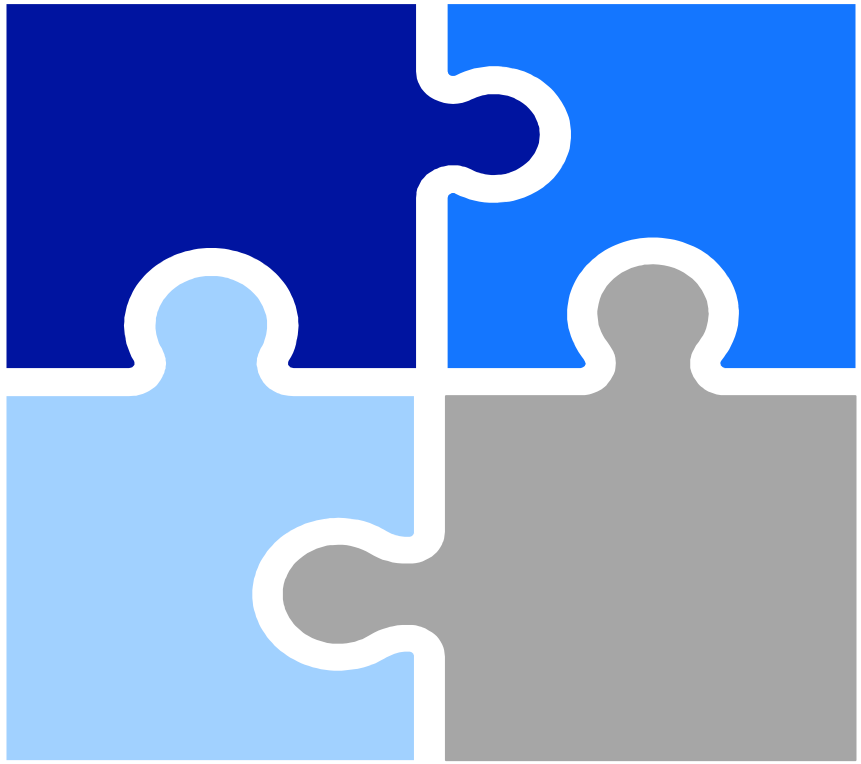
Byte array property name: the device unique identifier is established during device provisioning and provides a means of uniquely identifying each device.

Constant Value: "deviceUniqueId"

LABS

PUTTING IT ALL TOGETHER

Insecure Auth Flow



Reproduceable Device ID

URL Scheme Hijack

API request?

LABS

ANY JUICY API REQUESTS?



Response

Pretty | Raw | Render | \n | Actions


```
1  HTTP/1.1 200 OK
2  Access-Control-Allow-Credentials: true
3  Access-Control-Expose-Headers: Access-Control-Allow-Methods,A
4  Content-Type: application/json
5  Date: Wed, 26 May 2021 17:52:41 GMT
6  Server: nginx/1.13.8
7  vary: Accept-Encoding, User-Agent
8  Connection: Close
9  Content-Length: 387
10
11 {
     "data":{
       "me":{
         "__typename":"User",
         "id":"NDEwNjQ1MjQzMVIycE5SRWg3UjJGV2RFMXRVR2hUVVcxdWEyZ
         "firstName":null,
         "guestMode":false,
         "household":{
           "__typename":"Household",
           "masterPincode":"0000",
           "trackViewingBehaviour":false,
           "agreedToTermsAndConditions":false,
           "maxNumberOfConfirmedReplayChannels":null,
           "previewModeAllowed":false,
           "canMoveOperatorChannelLists":true
         }
       }
     }
```

WIND ONE WIND VISION STABLE MOBILE PHONE SIMPLEFI APPLIANCES SUPPORT

MASTER PIN CODE

Home › Support › Starting at WIND › Apart from the TV, how many other devices can I watch WIND VISION?

Apart from the TV, how many other devices can I watch WIND VISION?

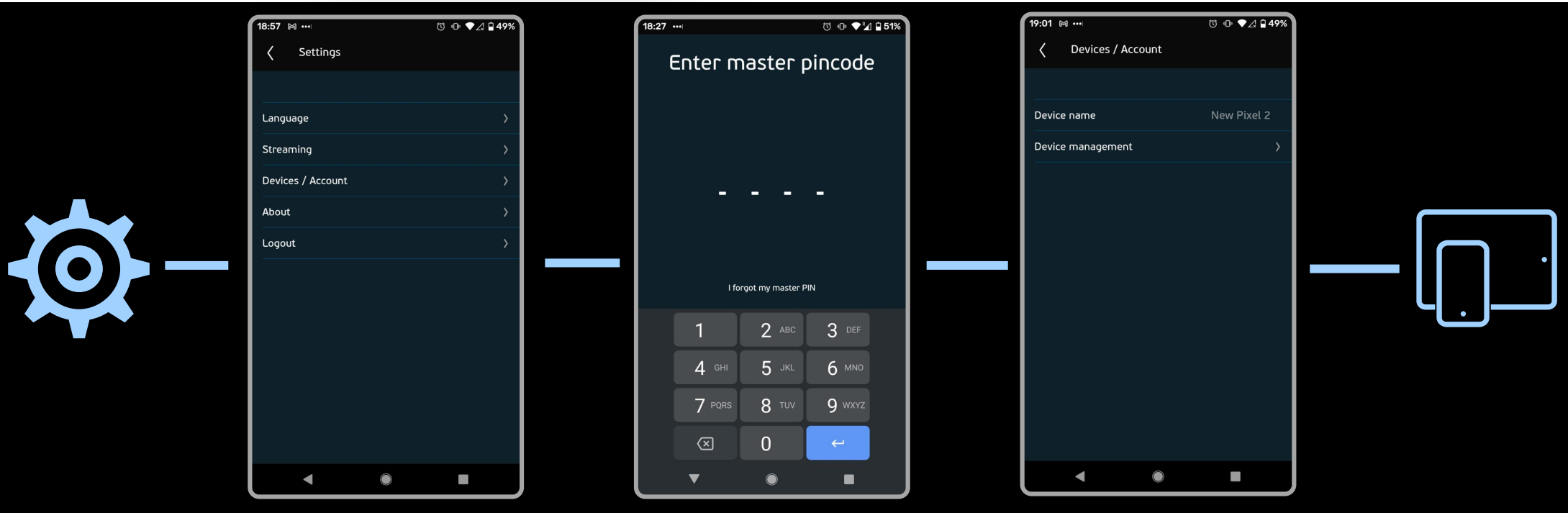
Additional devices

View on another device

Additional devices

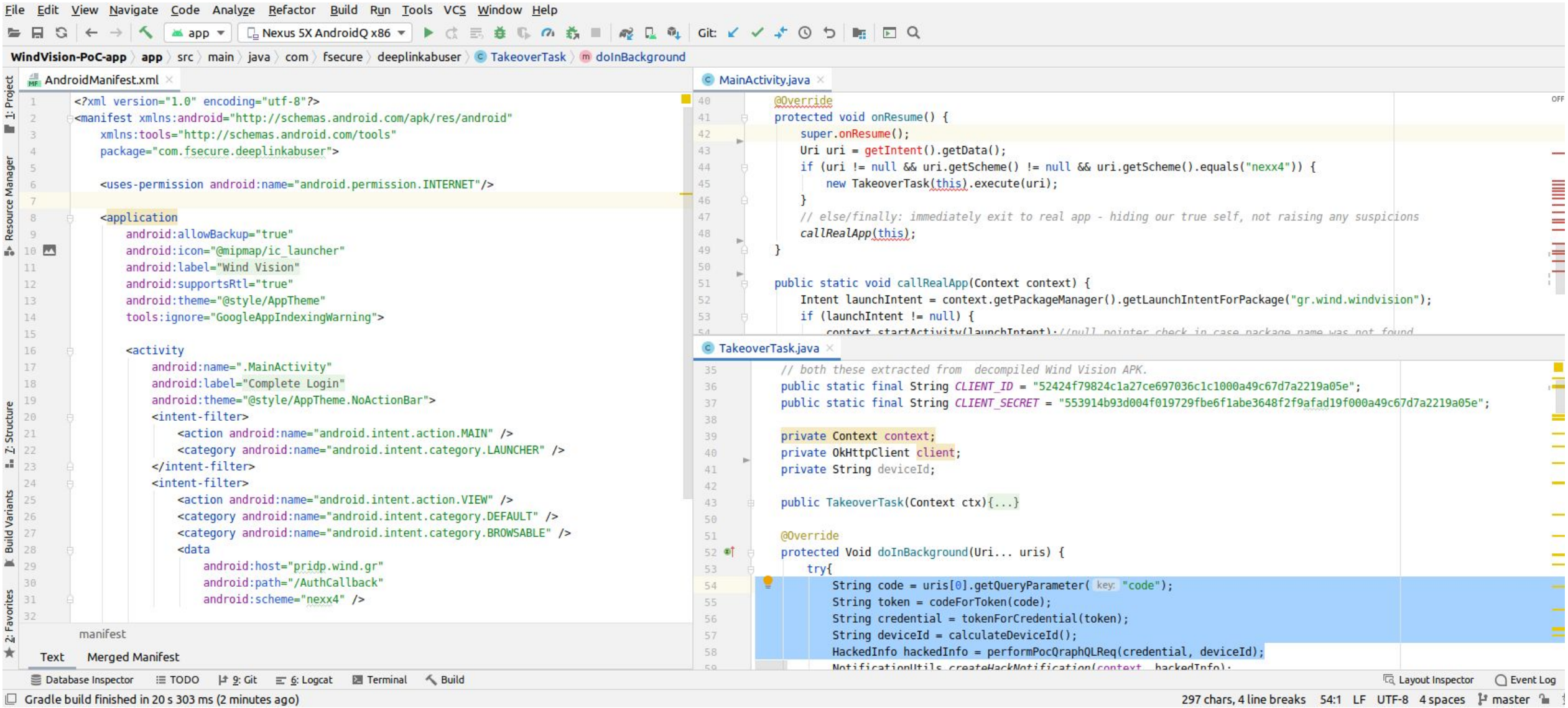
WIND VISION channels are available on **4 additional devices**, excluding the TV.

Simultaneous playback of content can be done on **up to 3 devices** .



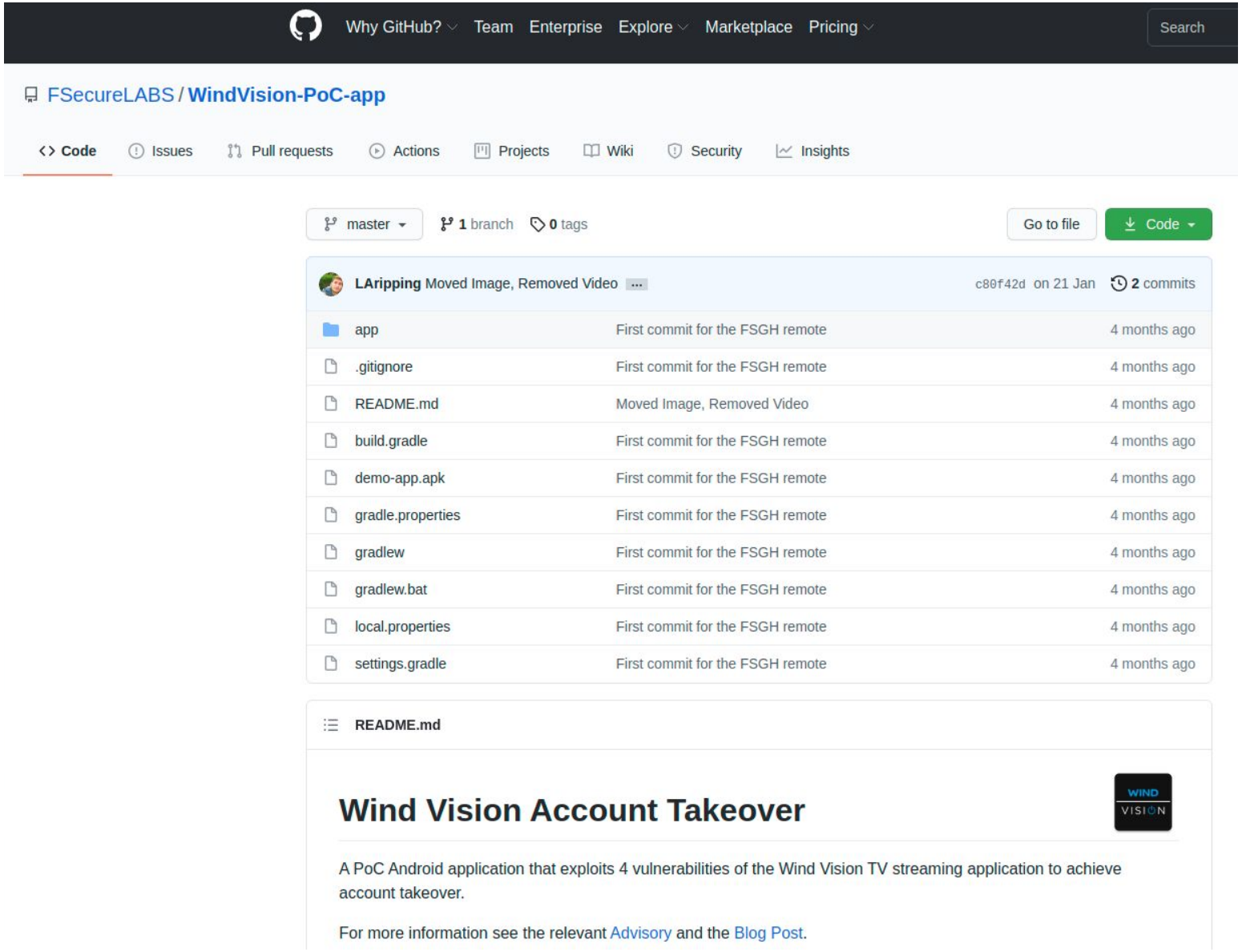
CODING TIME!

LABS



CODING TIME!

LABS




LABS
THAT'S NOT REALISTIC
Bad App?
In Play Store??
Wrong Click???

MAL
STO

LABS

threatpost

Google Play Harbo
Delivering Spy Tro



Author:
Tara Seals
March 9, 2021 / 11:44 am
3:30 minute read
Write a comment
Share this article:

A never-before-s
and MRAT malwa
users.

A malware dropper t
phones has been spr
according to researc

The malware is part
also allows eventual

The dropper, dubbed

Gizchina
CHINESE GADGET REVIEW

NEWS TECH

MALWARE FO
HAS INFECTE

EFE UDIN NOVEMB



This
Accor
infec
end

ZDNet

MENU

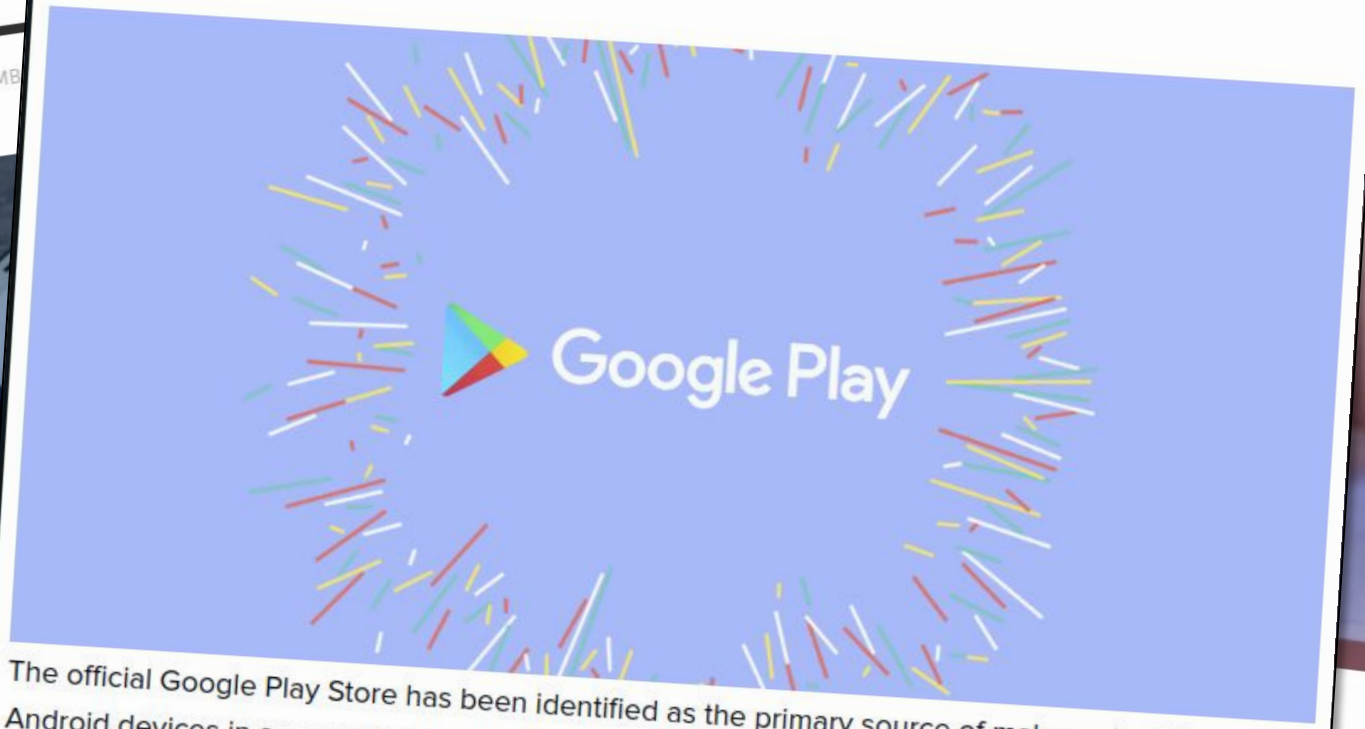
UK

Play Store identified as main distribution vector for most Android malware

Mammoth research project using Symantec (now NortonLifeLock) telemetry confirms what everyone suspected.



By Catalin Cimpanu for Zero Day | November 11, 2020 -- 15:50 GMT (15:50 GMT) | Topic: Security



The official Google Play Store has been identified as the primary source of malware installs on Android devices in a recent academic study — considered the largest one of its kind carried out to date.

Using telemetry data provided by NortonLifeLock (formerly Symantec), researchers analyzed the
installations on more than 12 million Android devices for a four-month period between
ember 2019.

Cookie Settings

OOP

SNC

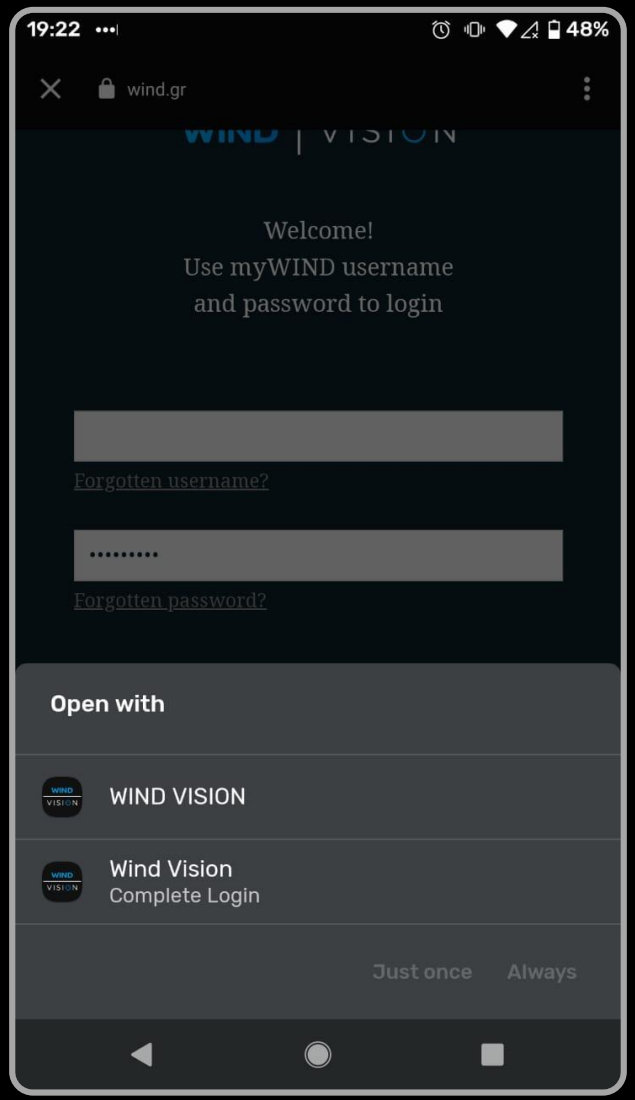
Google Play
re after years
chers say



le
ng

WHICH WOULD YOU CHOOSE?

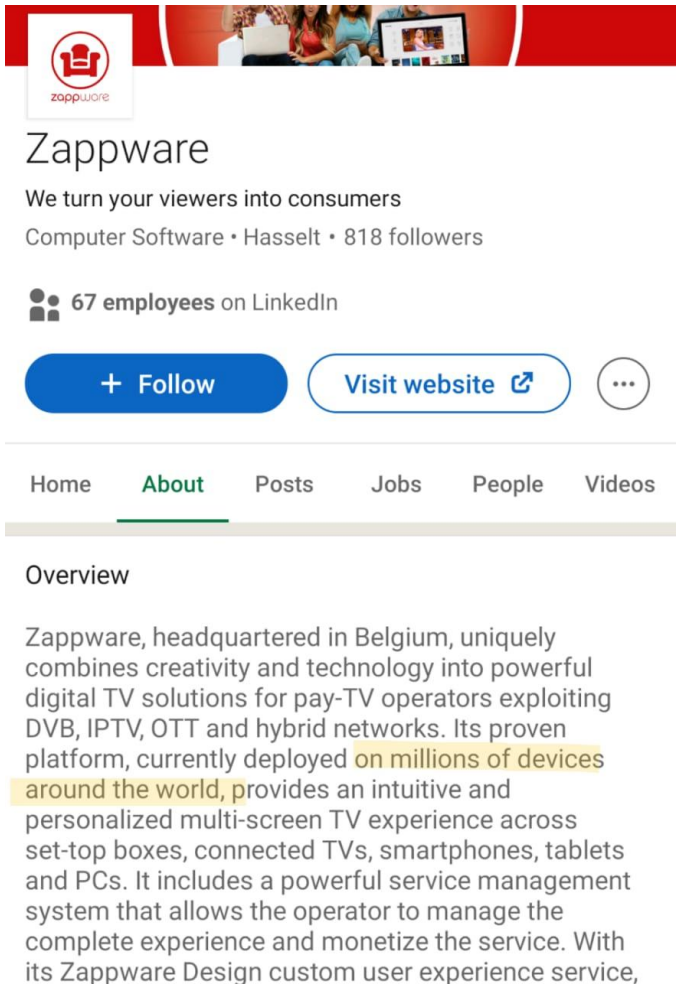
LABS



DISCLOSURE


PATIENCE, YOU MUST HAVE

USER BASE?



Zappware

We turn your viewers into consumers

Computer Software • Hasselt • 818 followers

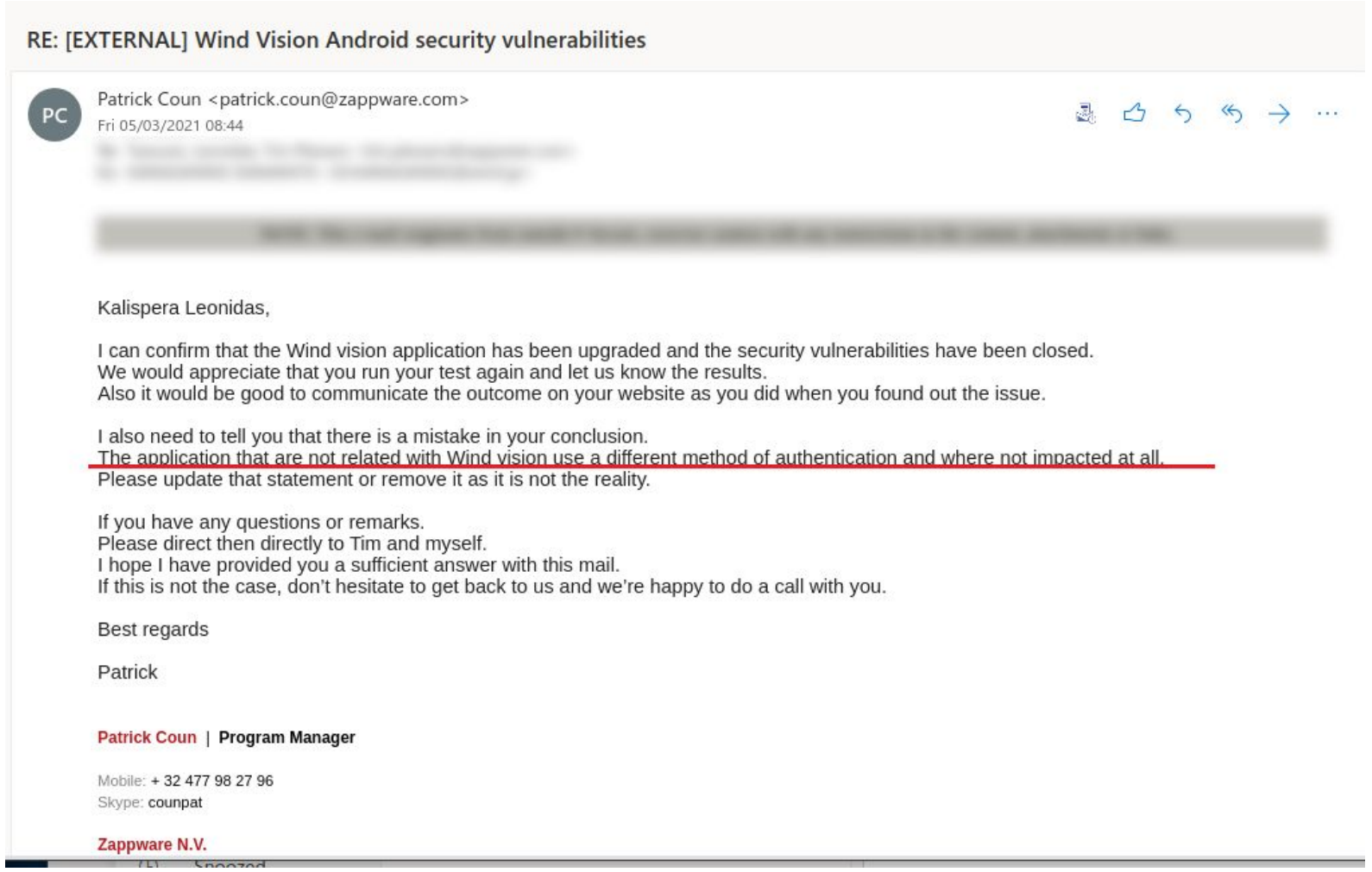
67 employees on LinkedIn

+ Follow | Visit website | ...

Home | About | Posts | Jobs | People | Videos

Overview

Zappware, headquartered in Belgium, uniquely combines creativity and technology into powerful digital TV solutions for pay-TV operators exploiting DVB, IPTV, OTT and hybrid networks. Its proven platform, currently deployed on millions of devices around the world, provides an intuitive and personalized multi-screen TV experience across set-top boxes, connected TVs, smartphones, tablets and PCs. It includes a powerful service management system that allows the operator to manage the complete experience and monetize the service. With its Zappware Design custom user experience service,



RE: [EXTERNAL] Wind Vision Android security vulnerabilities

PC

Patrick Coun <patrick.coun@zappware.com>

Fri 05/03/2021 08:44

Kalispera Leonidas,

I can confirm that the Wind vision application has been upgraded and the security vulnerabilities have been closed.
We would appreciate that you run your test again and let us know the results.
Also it would be good to communicate the outcome on your website as you did when you found out the issue.

I also need to tell you that there is a mistake in your conclusion.
The application that are not related with Wind vision use a different method of authentication and where not impacted at all.
Please update that statement or remove it as it is not the reality.

If you have any questions or remarks.
Please direct then directly to Tim and myself.
I hope I have provided you a sufficient answer with this mail.
If this is not the case, don't hesitate to get back to us and we're happy to do a call with you.

Best regards

Patrick

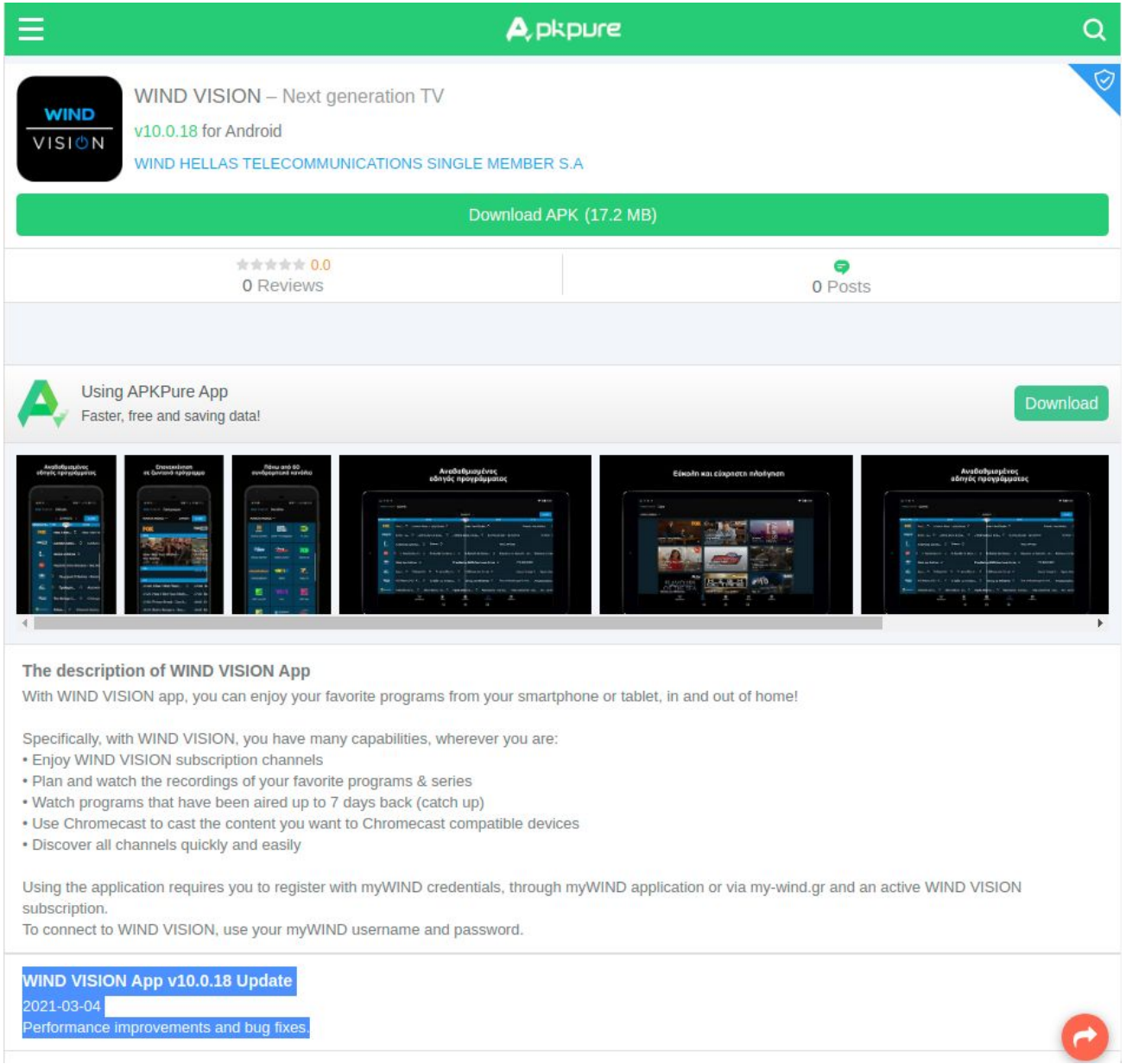
Patrick Coun | Program Manager

Mobile: + 32 477 98 27 96
Skype: counpat

Zappware N.V.

PATCHES?

- Insecure Authentication (CVE-2021-22268)
- PIN Code Leakage (CVE-2021-22269)
- URL Hijacking (CVE-2021-22269)
- Reproduceable Device ID (CVE-2021-22271)



MEDIA COVERAGE

LABS

INVESTIGATIONS

Wind Vision Android App: Customer data at risk from hackers!

By **Hack Sticks** 15 February 2021, 15:45

Wind Vision Android App: Customer data at risk from hackers! ***Security vulnerabilities are found in Wind Vision Android Application a service from telecommunications provider Wind Hellas. Security errors in the application allow the violation of legitimate user accounts as well as the theft of passwords and other accounts.***

According to confidential information from a SecNews user who sent an anonymous message with anonymity, **the implementation of Wind Hellas is a danger for hundreds of Greek citizens** who have the subscription service and use it on their personal devices. **Four (4) critical vulnerabilities have already been identified in the application and while as of November 14, 2020, Wind Hellas became aware, there was no official response / announcement or information if and when the security issue was resolved.**



LIVE NEWS


How to turn off smart reply & edit features in Gmail
May 24, 2021, 17:56


All three Hermès AirTag products are not available to order
May 24, 2021, 17:26



FBI: Connects Conti ransomware with 16 attacks on major US agencies
May 24, 2021, 17:07


Upcoming Honor phones will have Google apps pre-installed
May 24, 2021, 16:37



Pixel 6 / Pixel 6 Pro: What do we know about Google's upcoming smartphones?
May 24, 2021, 16:16


COVID-19: Singapore approves breath test - result in 1 minute
May 24, 2021, 15:57


Tesla is guilty of an update that reduced the charging speed
May 24, 2021, 15:12



An FBI analyst is accused of stealing anti-terrorism documents
May 24, 2021, 14:34

TIPS (FOR HACKERS)

- Do tinker with apps you use everyday
- Be thorough, follow your checklist
- Chain bugs for maximum impact!



TIPS (FOR DEVS)

- Pick the Secure Oauth scheme
- Secure URL schemes
- (truly) Random IDs
- Don’t exchange PINs



CREDITS

- Oliver Simonnet
- Riaan Naudé
- James Stevenson & Robert Sherry
- Ken Gannon
- <test account provider>



F-Secure | LABS

THANK YOU

