



# SECURITE DES APPLICATIONS MOBILES CRITIQUES



- 1. Introduction : la pièce manquante de votre sécurité**
- 2. Exemples d'attaque ciblant les applications mobiles bancaires**
- 3. Point de situation sur les menaces mobiles**
- 4. La réponse de sécurité à déployer**
- 5. Synthèse et bénéfices**

Publication sur  
le store public

Le chaînon  
manquant

## Phase de développement et de test

### Les contrôles de sécurité :

- Analyse du code source
- Analyse statique et dynamique
- Test de vulnérabilité
- Test de pénétration
- Analyse comportementale
- ...

FAIT !  
ou  
presque

## Phase d'utilisation sur les mobiles des utilisateurs

### Intégrer la sécurité de l'environnement :

- Contrôle de sécurité du terminal
- Contrôle des Apps tierces et détection des Apps malveillantes
- Analyse des communications

Reste  
à faire !

1. Introduction : la pièce manquante de votre sécurité
2. Exemples d'attaque ciblant les applications mobiles bancaires
3. Point de situation sur les menaces mobiles
4. La réponse de sécurité à déployer
5. Synthèse et bénéfices

1

Des usages et des permissions déclarées ...

Accès aux contacts



Accès au réseau



Accès aux données



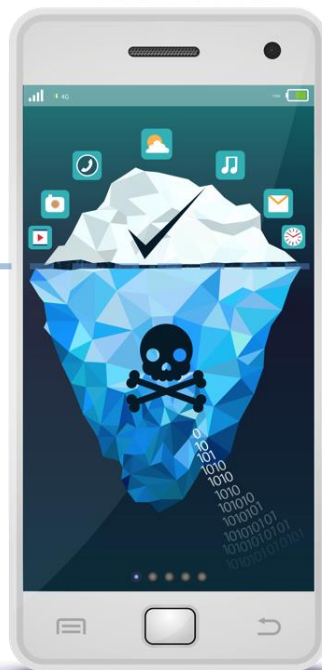
Accès aux messages



Accès à la localisation



...et davantage



Récupération de données personnelles



Connection à des serveurs non sécurisés

Appel automatique

SMS/MMS automatique et invisible



... Mais bien davantage encore de comportements et processus cachés

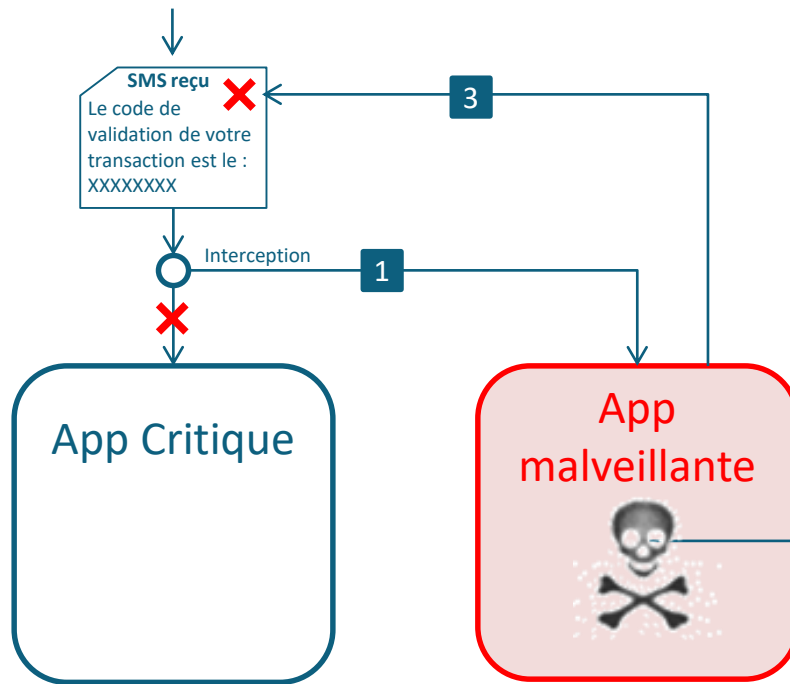
2

- **Keylogger**
- **Screenlogger**
- **Intercepteur OTP**
- **Cheval de Troie récupérateur de données**
- **Attack overlay**
- **Clone ... fonctionnel ou non**

**Des outils à la  
disposition des  
pirates**

## Attaque OTP

- 1 Une application tierce écoute les SMS entrants sur le mobile de l'utilisateur
- 2 Elle récupère de manière sélective les contenus qui l'intéresse
- 3 Elle efface automatiquement les contenus récupérés pour ne laisser aucune trace sur le mobile de l'utilisateur.



**Site pirate**  
<http://interception-demo.pradeo.net/>

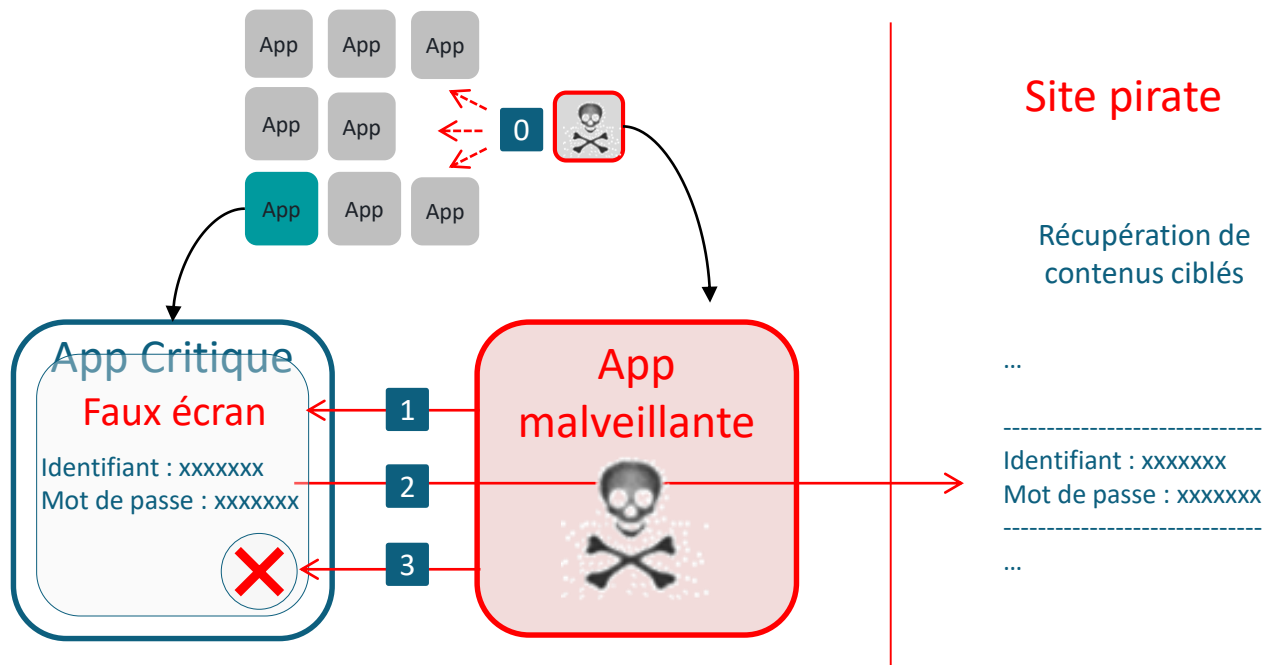
**Envoyez vos SMS  
au 06 66 68 68 84**

Récupération du  
contenu des SMS reçus

...  
-----  
Le code de validation de  
votre transaction est le :  
XXXXXXXX  
-----  
...

- 0 Une application tierce surveille les applications lancées sur le mobile de l'utilisateur
- 1 Pendant l'exécution de l'application « cible », elle présente à l'utilisateur un « écran-bis » calqué sur celui de l'application attaquée
- 2 L'interface-bis collecte les informations sensibles recherchée
- 3 Puis rend la main à l'application cible (par exemple en prétextant une erreur de saisie ...)

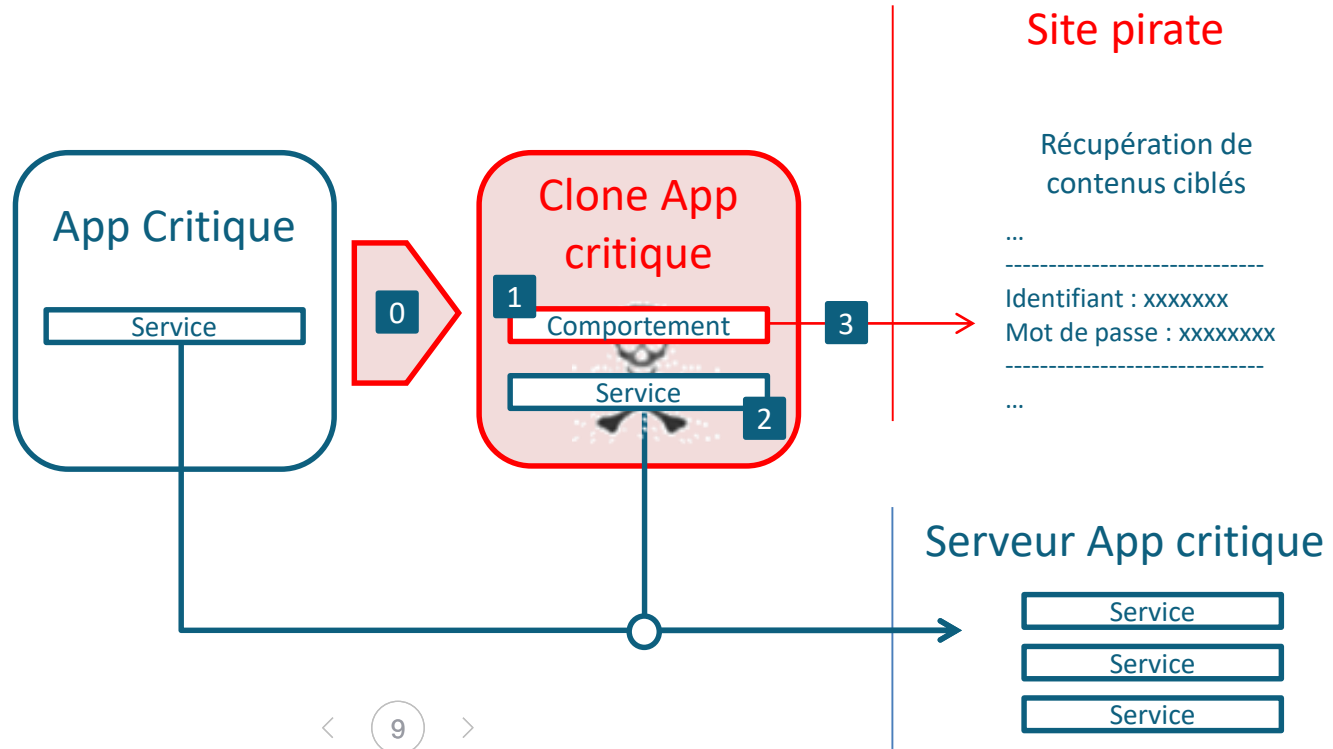
## Attaque Overlay





- 0 La version officielle de l'application critique est clonée dans sa globalité
- 1 Des comportements malveillants sont ajoutés dans le clone
- 2 L'utilisateur qui télécharge le clone ne réalise pas que l'application officielles est détournée car les fonctions sont opérationnelles (le clone est branché sur les mêmes services coté serveur)
- 3 Les données sensibles sont collectées à son insu

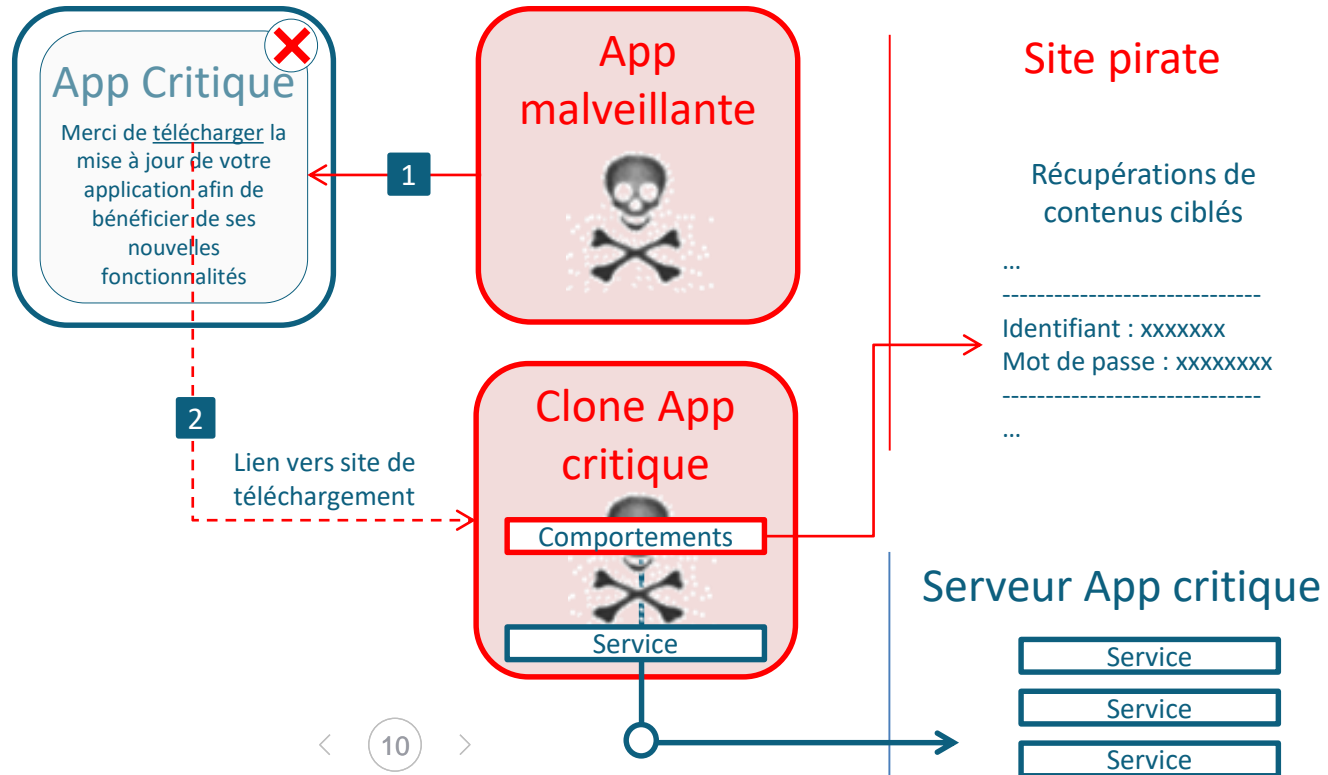
## Attaque via un clone



## Variante : attaque overlay + clone

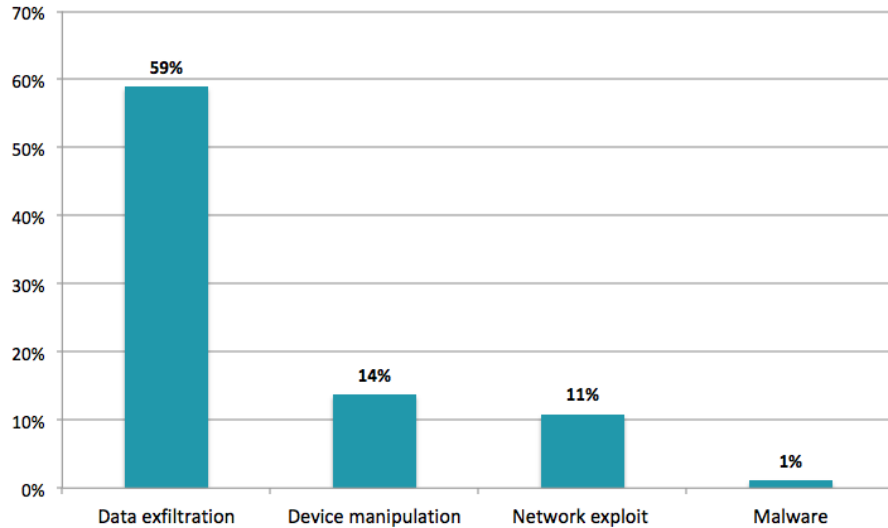
1 Phase 1 : Une application tierce prend la main sur l'application officielle via une attaque Overlay et force l'installation du clone et la désinstallation de l'application officielle

2 Phase 2 : le clone s'installe et délivre un service identique à l'application officielle ... mais avec les comportements malveillants en plus



1. Introduction : la pièce manquante de votre sécurité
2. Exemples d'attaque ciblant les applications mobiles bancaires
3. Point de situation sur les menaces mobiles
4. La réponse de sécurité à déployer
5. Synthèse et bénéfices

## TOP DES MENACES LIÉES AUX APPLICATIONS - 2018



## MENACES

- Applications grises



- Malwares

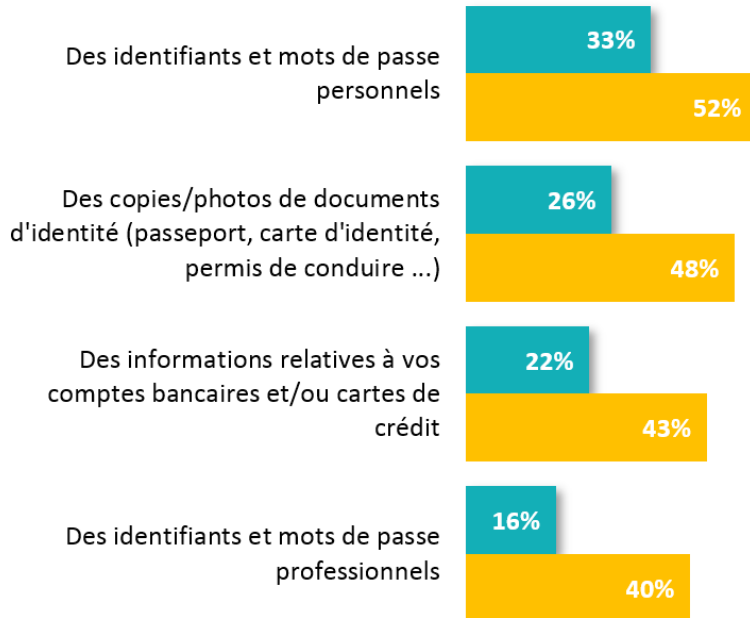


## Comportements à risque des consommateurs ...




1066  
personnes

Q : Vous est-il déjà arrivé d'enregistrer sur votre Smartphone ou votre tablette les informations suivantes vous concernant ?



*Sous-Total des réponses : « Oui et elles y sont encore enregistrées » et « Oui, mais je les ai effacées depuis »*



Utilisateurs Smartphones et/ou tablettes - 1066 personnes



Utilisateurs professionnels de Smartphone - 222 personnes

Enquête  
« opinionway »

## TOP DES MENACES LIÉES AU RÉSEAU - 2018

1

Attaque au travers des réseaux WIFI publics

2

Phishing

3

Man-in-the-Middle

## MENACES



Scan SMS



WiFi à risque / interdit



Man-In-The-Middle



Réseau cellulaire suspect



Proxy



Bluetooth



VPN



NFC



Géolocalisation

## TOP DES MENACES LIÉES AU TERMINAL - 2018

1

**OS vulnérable**

2

**Modification des paramètres système**

3

**Exploitation du Root / Jailbreak**

## MENACES



Root



OS obsolète & vulnérabilités du système



Profil malveillant



Certificat non fiable



Modification du fichier host



Fonctionnalités de sécurité



Sources inconnues



Accessibilité



Données chiffrées



Mode debug



Fichier malveillant

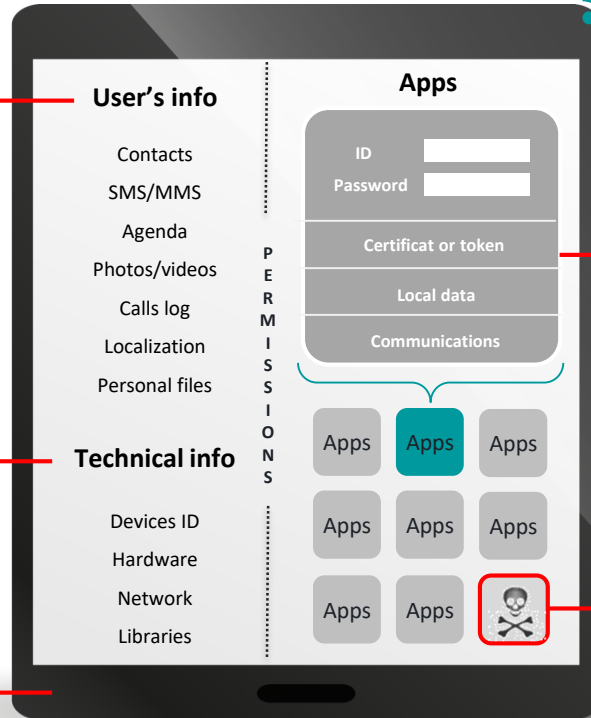
1. Introduction : la pièce manquante de votre sécurité
2. Exemples d'attaque ciblant les applications mobiles bancaires
3. Point de situation sur les menaces mobiles
4. La réponse de sécurité à déployer
5. Synthèse et bénéfices



Quelle utilisation des données personnelles de l'utilisateur ?

Quelle utilisation des données à caractère technique ?

Quel contrôle sur le terminal ?



Quel contrôle sur les connexions réseau ?

Quelle protection pour les composants sensibles des Apps de l'entreprise ?

Quel contrôle sur les Apps publiques ?

## Un petit bout de code (SDK)

- Un SDK, facile à intégrer dans une application sensible
- Qui externalise et centralise la gestion des règles de sécurité pour se protéger des menaces en provenance des Apps tierces



## Une plateforme d'administration

- Une plateforme d'administration pour gérer la politique de sécurité de l'application sensible
- Et superviser les menaces en sur les terminaux des utilisateurs



## Une protection embarquée "in-App"

- La solution de sécurité face aux menaces présentes dans l'environnement d'une application sensible
- Qui renforcer sa sécurité lors de son exécution sur un terminal non sécurisé et non managé

Protection contre les **Screenloggers**

Protection contre les **Intercepteurs OTP**

Protection contre les **Keyloggers**

Protection contre les **Clones**

Protection contre ...

# PROTECTION IN-APP : ARCHITECTURE GENERALE DE LA SOLUTION

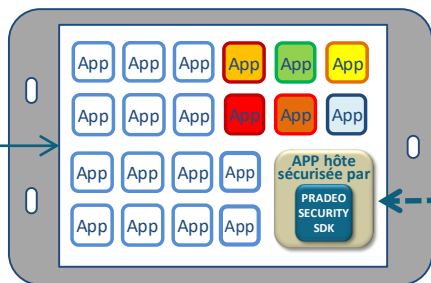
## Store publique



Téléchargement des Apps publiques



Terminal mobile



A

Intégration des APIs de Pradeo Security dans le code source de l'App critique

Adaptation de l'expérience utilisateur pour prendre en compte les alertes de sécurité à chaque lancement de l'App critique

Publication de la nouvelle version de l'App critique sur le store

## Serveur pradeo Security

### Services de pradeo

- 1 Gestion de la politique de sécurité de l'App critique
- 2 Contrôle de conformité du terminal de l'utilisateur aux règles de sécurité

Règles de sécurité

B

Contrôle du terminal et des Apps téléchargées par l'utilisateur, sur la base des règles de sécurité spécifiques, dédiées à la protection de l'App critique

### Services de pradeo

- 3 Contrôle du terminal et protection de l'App hôte critique



App critique, intégrant le SDK Pradeo Security,

## Apprendre puis agir

### 1 Apprendre sur les menaces

**Cas d'usage :** Acquérir la connaissance des menaces effectives présentes sur le parc

**Finalités :**

- Identifier les menaces réelles sur le parc mobile des clients
- Evaluer leur impact potentiel

**Bénéfice client :**

- **Service prêt à déployer**
- Zéro impact sur l'Expérience Utilisateur
- Qualification et quantification des menaces



### 2 Activer la protection

**Cas d'usage :** Se protéger des menace avérée sur le parc client avec risque majeur quantifié

**Finalités :**

- Activer le dispositif de protection pour bloquer / dégrader l'exécution de l'App sensible
- Protéger l'utilisateur presque à son insu

**Bénéfice client :**

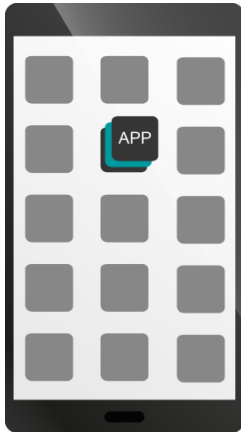
- **Protection des transactions sensibles**
- Alerte utilisateur sur des menaces qualifiées
- Mise en œuvre rapide du mode blocage

1. **Introduction : la pièce manquante de votre sécurité**
2. **Exemples d'attaque ciblant les applications mobiles bancaires**
3. **Point de situation sur les menaces mobiles**
4. **La réponse de sécurité à déployer**
5. **Synthèse et bénéfices**

Collecte et qualification de données et  
événements de sécurité

+

Protection des données et transactions  
sensibles



- ✓ SDK prêt à l'emploi (s'intègre en 2h)
- ✓ Protection en temps réel sur le terminal
- ✓ Permet d'enrichir SOC/SIEM
- ✓ Aide à se conformer au GDPR et PSD2
- ✓ Politique de sécurité personnalisable
- ✓ Administration à distance

Une solution simple et unique pour :

- faire face aux nouvelles menaces auxquelles sont exposées les Apps sensibles
- et contrôler le niveau de sécurité des terminaux non-gérés

**PROTEGER vos APPS en maîtrisant la sécurité du terminal de l'utilisateur**

**PRADEO**  
SECURITY  
SDK

**Protection à 360° lors de l'exécution**

- Selon vos propres règles de sécurité
- Déployé sur 100% de vos clients/utilisateurs
- Sans être dépendant d'un tiers et en ayant en mains tous les leviers de décision
- Avec des règles évolutives gérées depuis un console d'administration



Merci de votre attention

