



Applications mobiles et sécurité

Révélation sur les comportements
cachés des Apps



Agenda ...

- Qui sommes-nous ? Quel est le problème ?
- Qu'en pense l'opinion publique ?
- Le livre blanc de la sécurité des Apps

A propos de Pradeo ...

Qui sommes-nous ?

- Une jeune entreprise innovante
- Spécialisée dans la sécurité des applications mobiles
- Reconnue pour sa vision et la portée de ses innovations
- En phase de développement accéléré à l'international

Nos innovations

- Une approche de la sécurité basée sur l'analyse comportementale
- Une technologie brevetée
- Une nouvelle génération de solutions dédiée à la protection antimalware des terminaux mobiles et objets connectés

Le syndrome de l'Appsberg ...

Des usages et des permissions déclarées ...

Accès aux contacts



Accès au réseau



Accès aux données



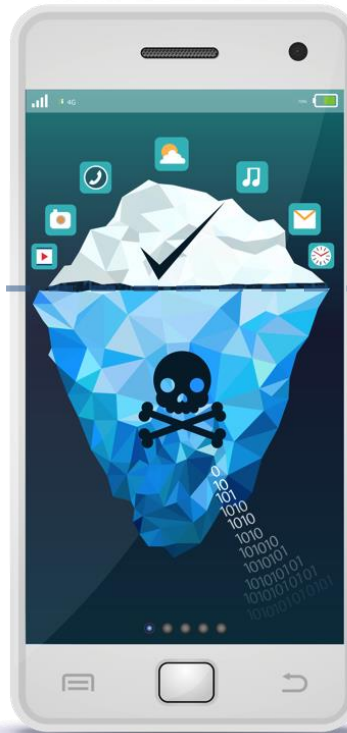
Accès aux messages



Accès à la localisation



...et davantage



Récupération de données personnelles

Connection à des serveurs non sécurisés

Appel automatique

SMS/MMS automatique et invisible

... et davantage



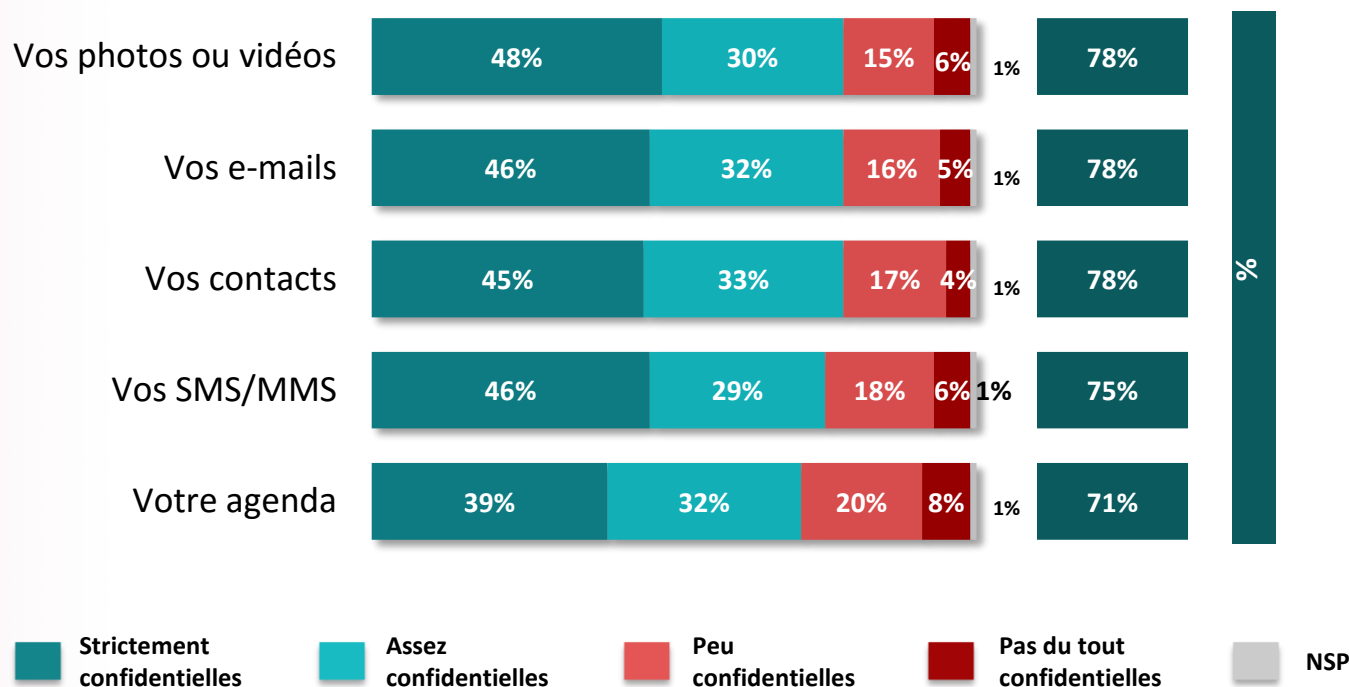
Mais des comportements et des processus cachés ...

Agenda ...

- Qui sommes-nous ? Quel est le problème ?
- Qu'en pense l'opinion publique ?
- Le livre blanc de la sécurité des Apps

Confidentialité des données ...

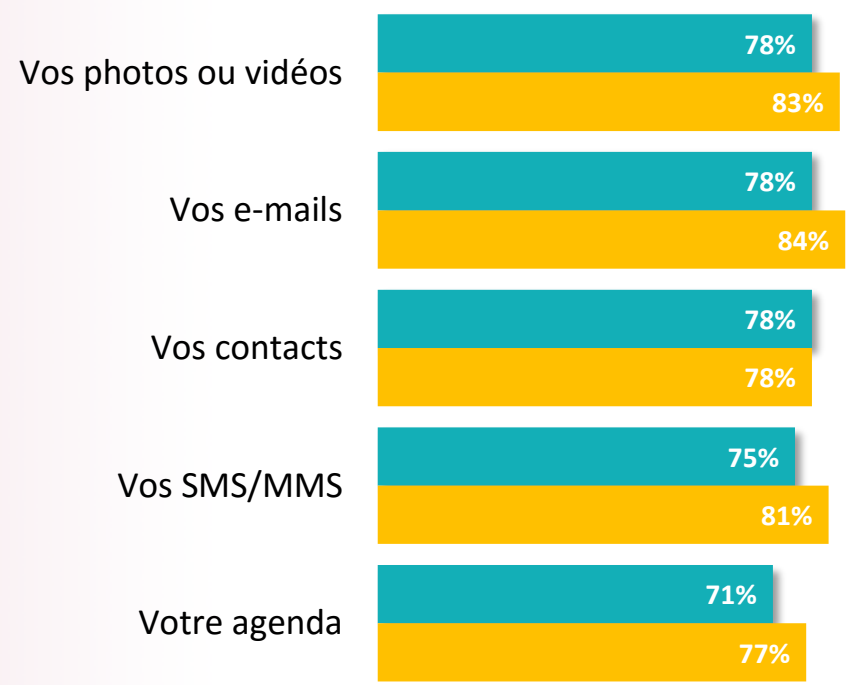
- Q. Si vous deviez qualifier les informations suivantes conservées dans votre Smartphone ou sur votre tablette, vous diriez qu'elles sont... ?



Enquête opinionway

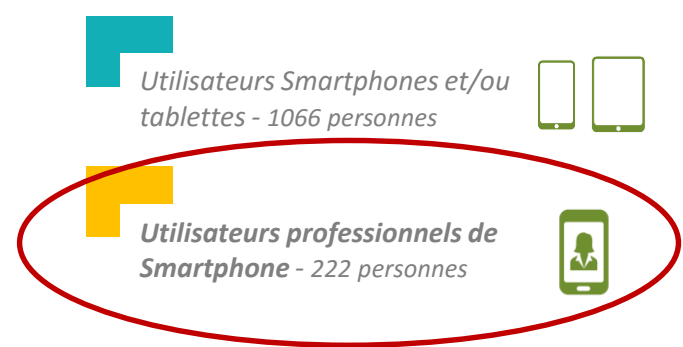
Confidentialité des données ...

- Q. Si vous deviez qualifier les informations suivantes conservées dans votre Smartphone ou sur votre tablette, vous diriez qu'elles sont... ?



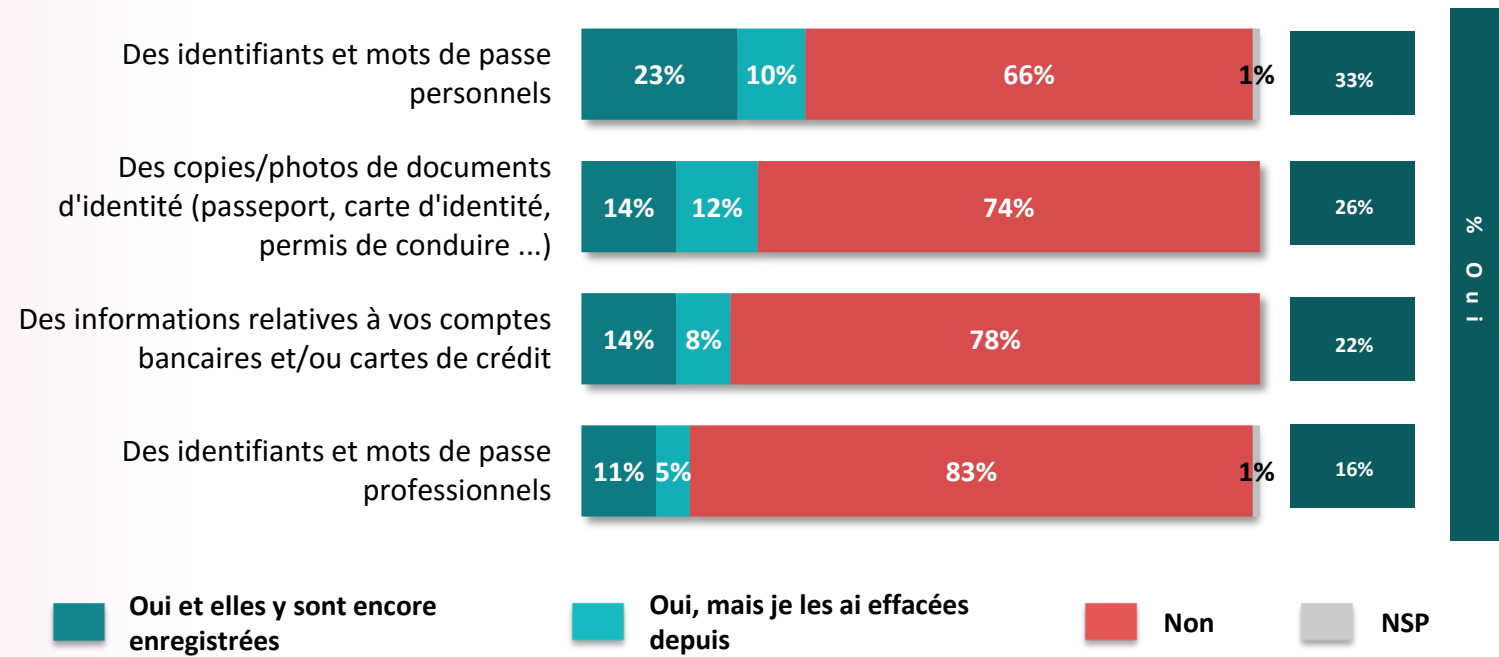
Sous-Total des réponses : Confidentielles

Enquête opinionway



Comportements à risque ...

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

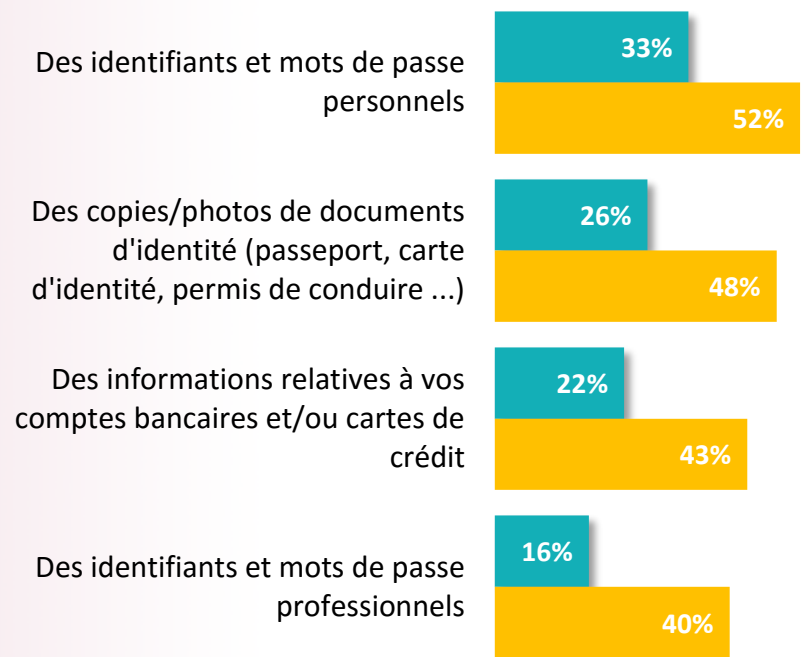


Enquête opinionway

ino %

Comportements à risque ...

- Q. Vous est-il déjà arrivé d'enregistrer dans votre Smartphone ou 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 »

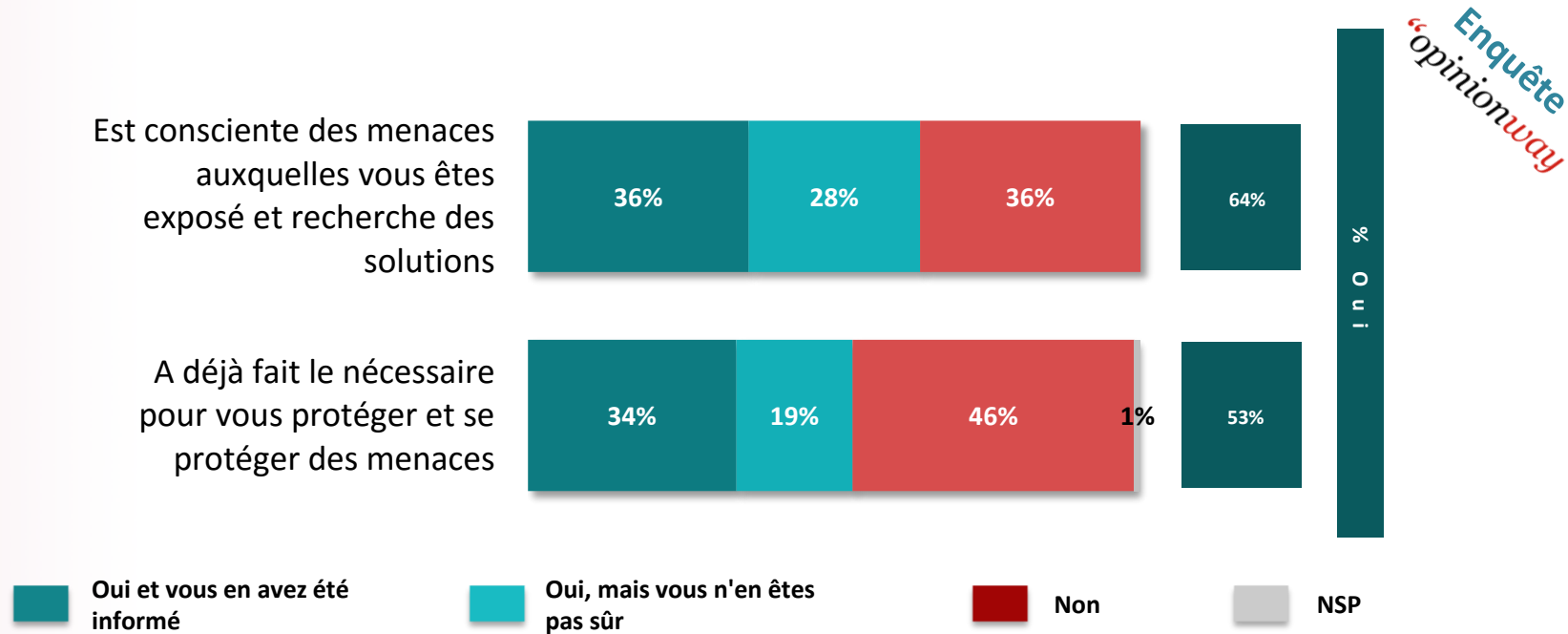


Enquête opinionway

Rôle de l'entreprise ...

- Q. Concernant le Smartphone que vous utilisez à titre professionnel, avez-vous le sentiment que votre entreprise... ?

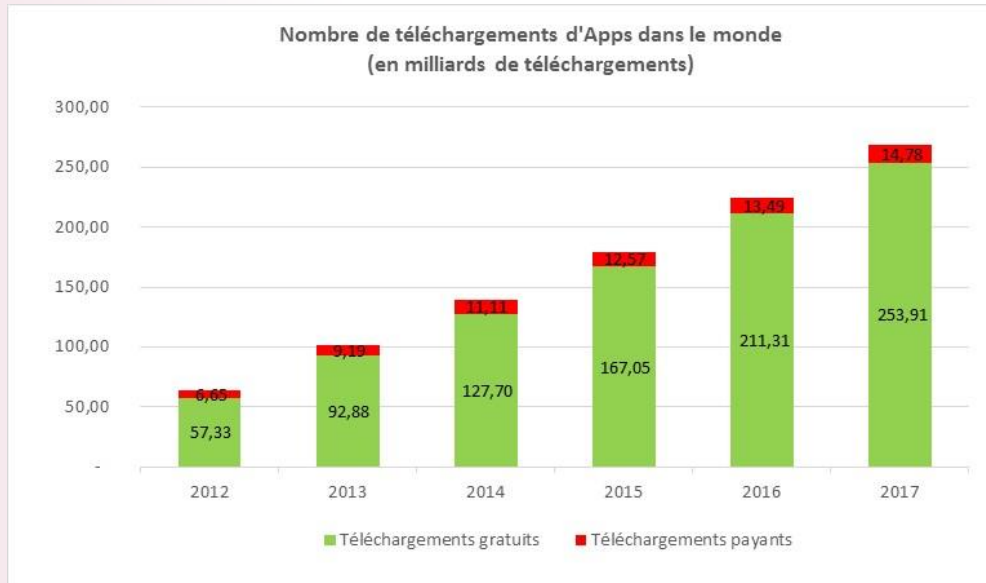
Question posée uniquement aux actifs utilisant un Smartphone dans le cadre de leurs fonctions



Agenda ...




- Qui sommes-nous ? Quel est le problème ?
- Qu'en pense l'opinion publique ?
- Le livre blanc de la sécurité des Apps

Les applications mobiles ont-elles de l'avenir ?



Quelques chiffres qui valent bien mieux qu'un long discours

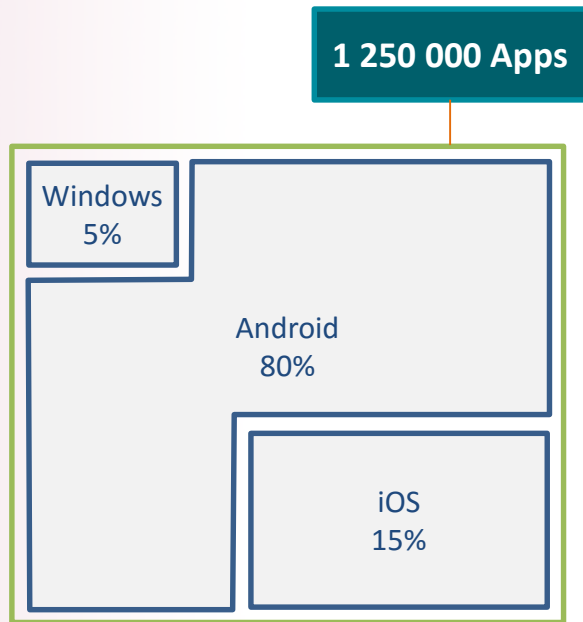
- 268 milliards de téléchargement en 2017
- Chiffre d'affaires généré de près de 77 milliards de dollars en 2017
- Sans compter le booster attendu des objets connectés : 20,8 milliards en 2020 selon le cabinet Gartner

			
Nb d'applications dans les stores officiels à fin 2015	1 600 000	1 500 000	670 000



Le modèle Apps a de l'avenir

Quelle histoire pour un simple échantillon d'Apps ...

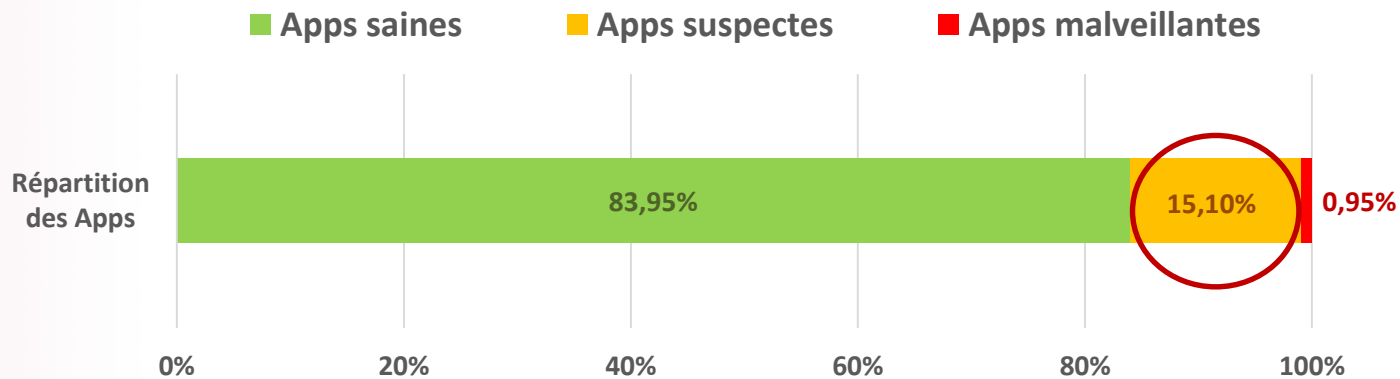


Une mise en examen à grande échelle pour un interrogatoire particulièrement serré

- Niveau de sécurité des applications présentes sur les stores publics
- Répartition des menaces pour le consommateur
- Informations récupérées par les applications à risque
- Analyse des menaces par catégorie d'applications
- Les nouveaux malwares

Quel est le niveau de sécurité des applications mobiles ?

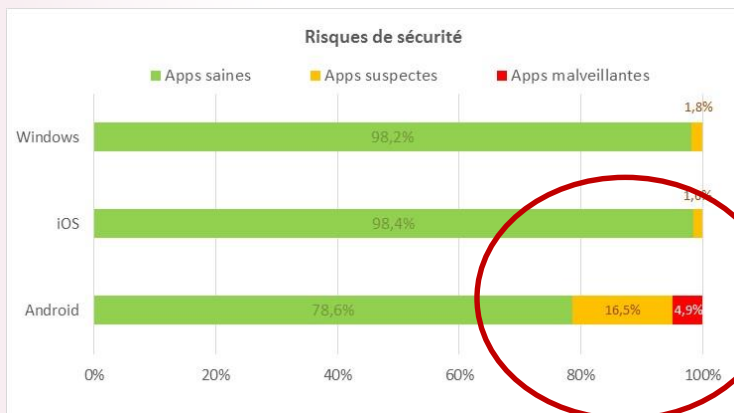
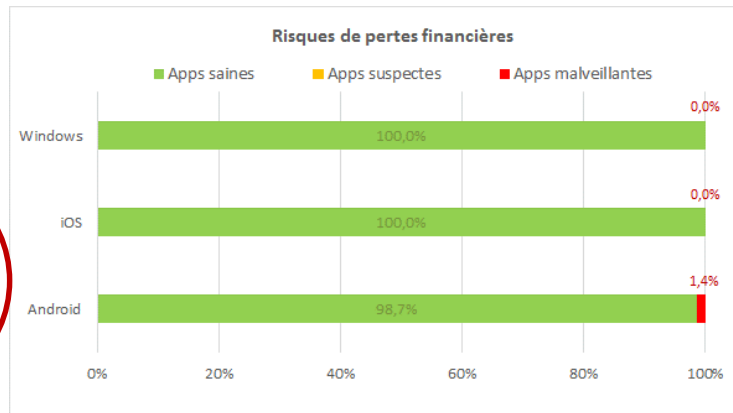
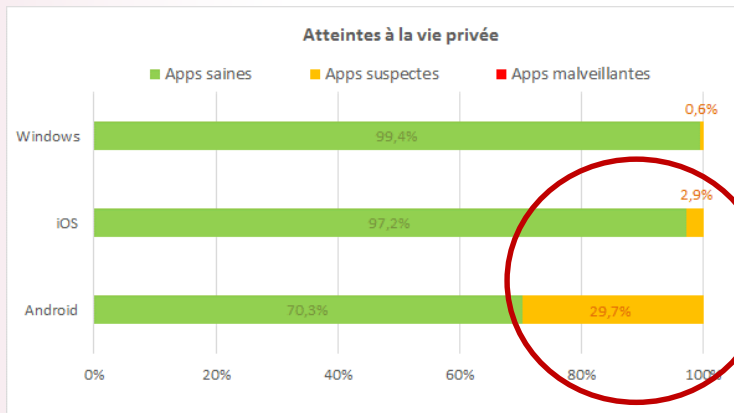
Les Apps grises sont la vraie source de complexité dans la gestion de la sécurité des Apps



- Plus de 15% des Apps présentent au moins un comportement suspect
- Qui sera jugé acceptable ou malveillant selon des règles personnalisées

Comment se répartissent les menaces pour le consommateur ?

Android est toujours la cible majeure mais ses concurrents ne sont pas épargnés



01

Des risques de sécurité importants dans l'environnement Android 4,9% d'Apps dangereuses ...

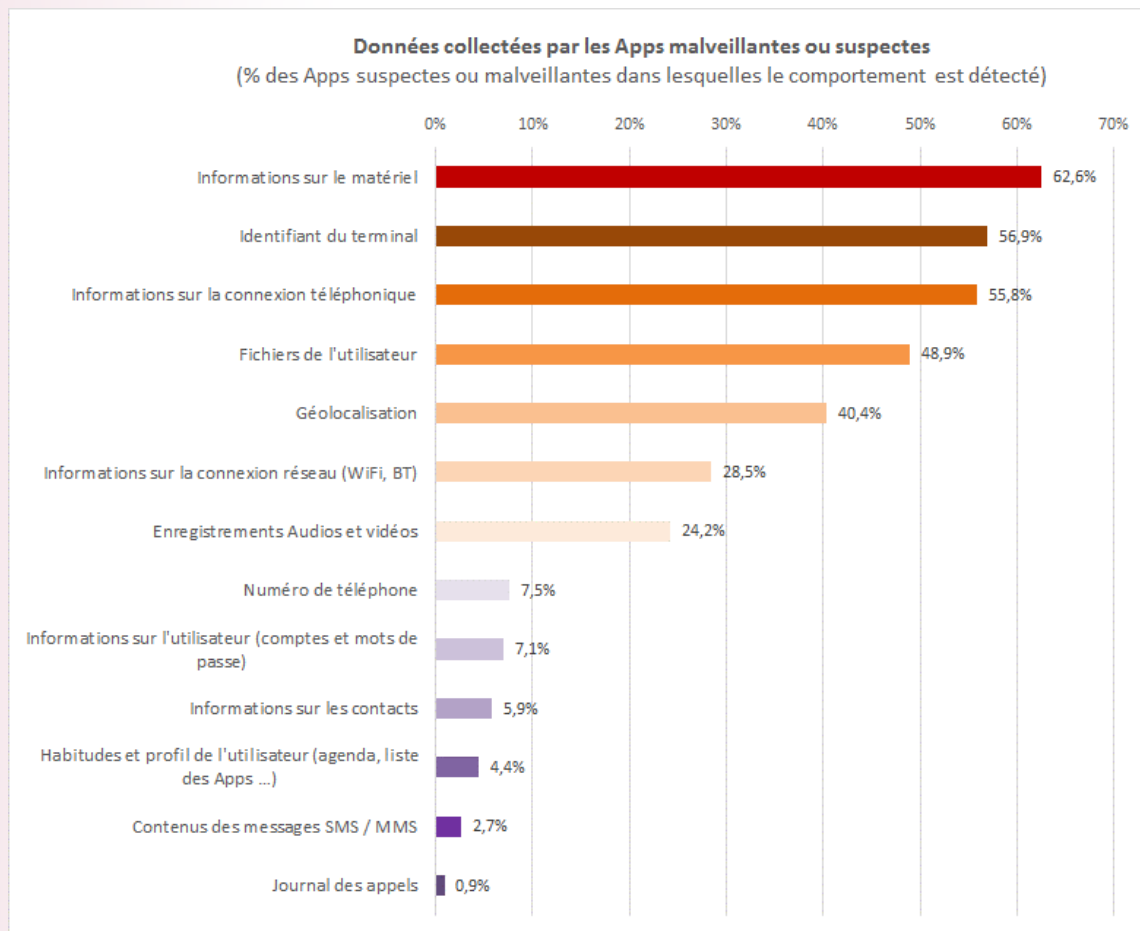
02

Des menaces sur la vie privée (récupération de données) qui peuvent atteindre près de 30% des Apps (sous Android)

03

Des menaces également présentes dans les environnements iOS et Windows

Données collectées par les Apps à risque ?



La collecte de données à l'insu de l'utilisateur est ancrée dans les mœurs

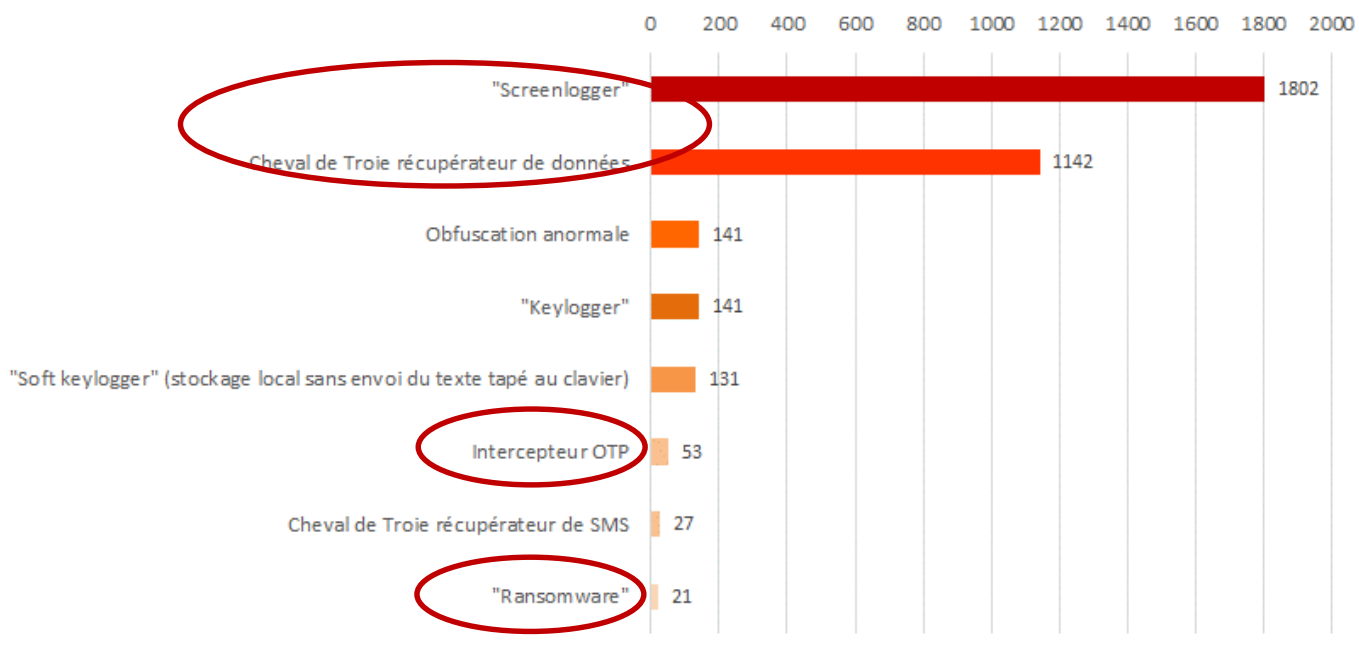
- Les données techniques sont les plus demandées
- Les données personnelles sont une cible de 1^{er} choix :
 - Fichiers de l'utilisateur pour 48,9% des Apps
 - Géolocalisation pour plus de 40% des Apps
 - Enregistrements audio et vidéo (pour 24,2%).
 - Numéro de mobile pour 7,5% des Apps

Les nouveaux malwares mobiles ...

Un marché dynamique et des pirates toujours aussi créatifs

3 458 Apps

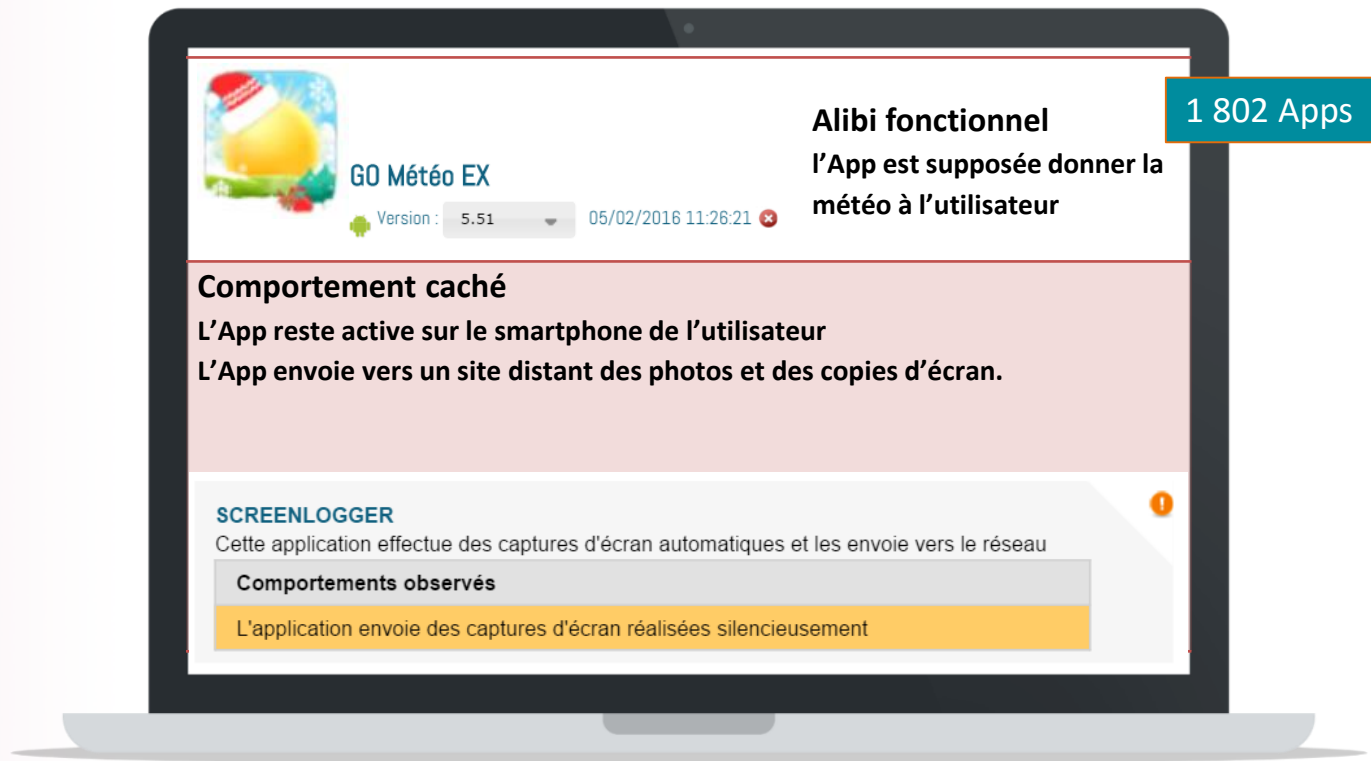
Nombre de malwares détectés selon leur typologie caractéristique (en unité)



- « Screenlogger » (52,1%) et Cheval de Troie récupérateur de données (33%) : les produits phares.
- « Keylogger » : une valeur sûre (4,1%)
- Des pratiques nouvelles qui se développent : Intercepteur OTP et Ransomware

Les nouveaux malwares mobiles ...

- Le Screenlogger



Les nouveaux malwares mobiles ...

- Le cheval de Troie récupérateur de données

The image shows a screenshot of an Android app page for 'VoiceWhats Root'. The app is described as a voice assistant for WhatsApp. A teal box in the top right corner indicates '1 142 Apps'. Below the app name, there is a warning section titled 'Comportement caché' (Hidden behavior) which states that the app recovers a lot of information without the user's knowledge. A detailed warning box titled 'DATA SENDING TROJAN (MALWARE RÉCUPÉRATEUR DE DONNÉES)' lists several observed behaviors, including sending terminal information, shared database information (SMS, etc.), user information, system information, geolocation data, and user contact information. At the bottom, it states that the app sends SMS automatically and invisibly to the user.

VoiceWhats Root
Version : 3.0.1 03/03/2016 09:17:28

Alibi fonctionnel
l'App est un assistant vocal pour l'application WhatsApp qui permet de dicter et d'écouter des messages

1 142 Apps

Comportement caché
L'App récupère beaucoup d'informations à l'insu de l'utilisateur.

DATA SENDING TROJAN (MALWARE RÉCUPÉRATEUR DE DONNÉES)
Cette application récupère et envoie un ensemble de données critiques (information de compte, identifiants du terminal...)

Comportements observés

- L'application envoie des informations relatives au terminal
- L'application envoie des informations provenant de la base de données partagée (SMS, etc)
- L'application envoie des informations concernant l'utilisateur
- L'application envoie des informations relatives au système
- L'application envoie des données de géolocalisation
- L'application envoie des informations relatives aux contacts de l'utilisateur

L'App envoie des SMS de manière automatique et invisible de l'utilisateur

Les nouveaux malwares mobiles ...

- Le Keylogger



Les nouveaux malwares mobiles ...

- L'intercepteur OTP

Trusteer Rapport
Version: 1.0 05/02/2016 11:22:50

Alibi fonctionnel
l'App déclare être un logiciel de sécurité qui surveille et protège les connexions sur les sites bancaires

53 Apps

Comportement caché
L'App récupère les codes OTP des transactions de paiement
C'est un clone d'une App d'IBM dédiée à la sécurité des transactions financières..

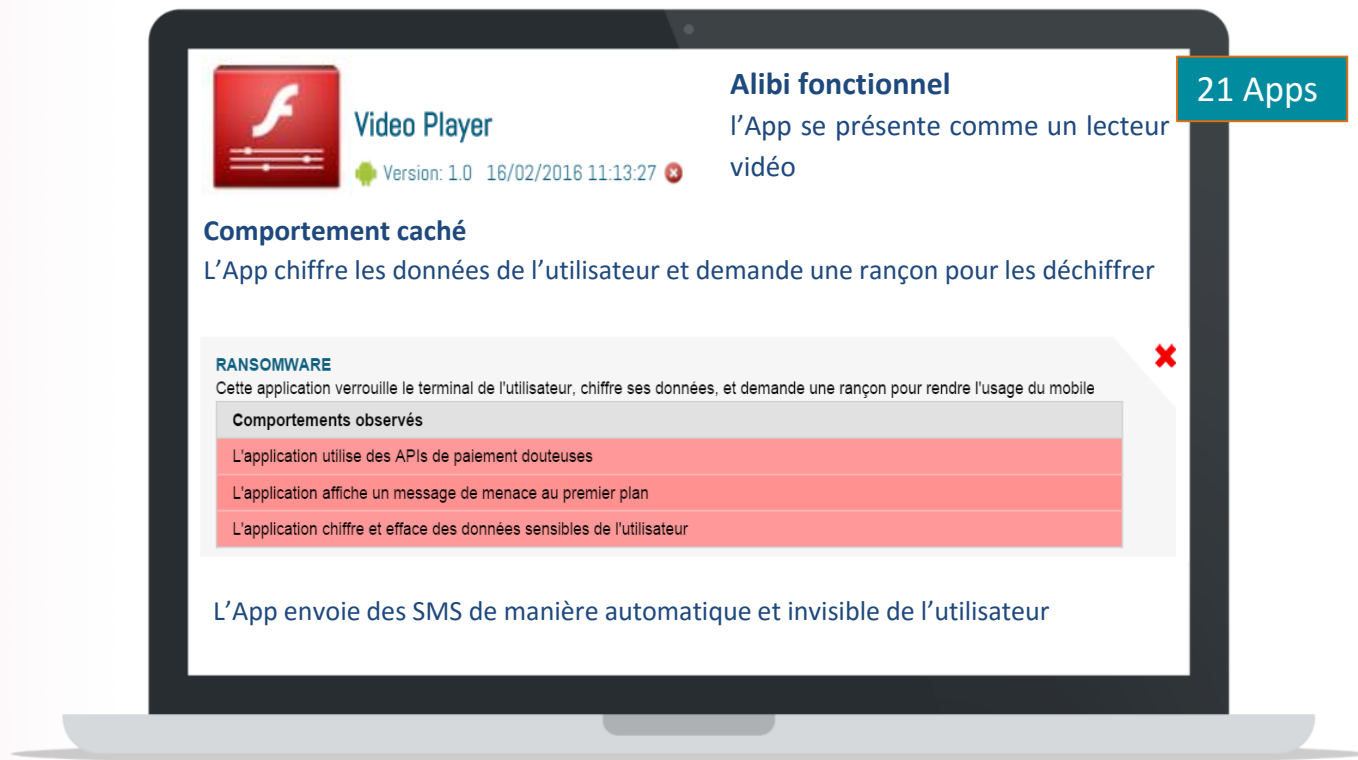
INTERCEPTION OTP
Cette application peut intercepter des SMS reçus par l'utilisateur pour les envoyer vers une destination distante.
Ce comportement peut être utilisé pour récupérer des mots de passe à usage unique utilisés pour valider une transaction bancaire.

Comportements observés

- L'application intercepte les SMS reçus
- L'application envoie le contenu des SMS reçus à une entité distante
- L'application efface silencieusement les SMS reçus

Les nouveaux malwares mobiles ...

- Le Ransomware



Les enseignements de l'étude...



Windows

Deux certitudes:

- Les apps malveillantes sont efficacement filtrées à la source par Microsoft,
- Mais les « Apps grises » y sont une réalité constatée



iOS

La mesure des menaces dans est impossible à appréhender, sauf par Apple ...

- Ses actions de contrôle permettent d'éradiquer à la source les malwares notoires.
- Mais les « Apps grises » y sont bel et bien présentes en raison de la subjectivité de la menace



Android

- Concentre le plus de menaces
- Donne la mesure étalon de la sécurité des Apps

Les enseignements de l'étude...



1%

Des Apps se révèlent malveillantes et présentent un risque avéré pour le grand public et les entreprises



15,1%

D'applications suspectes, forment la « zone grise » des Apps susceptibles de représenter une menace



Les Apps natives

Des fabricants et opérateurs ne sont pas irréprochables



Les Apps de Jeux

Utilitaires et Divertissement, concentrent les taux de menaces les plus importants.



Les Apps métiers

Encore moins qui révèlent des comportements inappropriés



Les pirates

Restent créatifs, en témoigne l'émergence des nouveaux malwares

Merci de votre attention

Clément Saad
Président
CEO & Founder

Mobile : +33 (0)6 71 24 04 50

Clement.saad@pradeo.com



@ClementSaad_

Renaud Gruchet
Directeur Marketing et
Communication

Mobile : +33 (0)6 08 67 28 15

Renaud.gruchet@pradeo.com



@GruchetRenaud

pradeo
BEYOND THE IMPOSSIBLE

Tel : +33 (0)4 67 20 99 11

communication@pradeo.com



@Pradeo_France