MALWARES ANDROID

Ashiahanim AYASSOR
Supervisé par Pr Gabriel GIRARD

SOMMAIRE

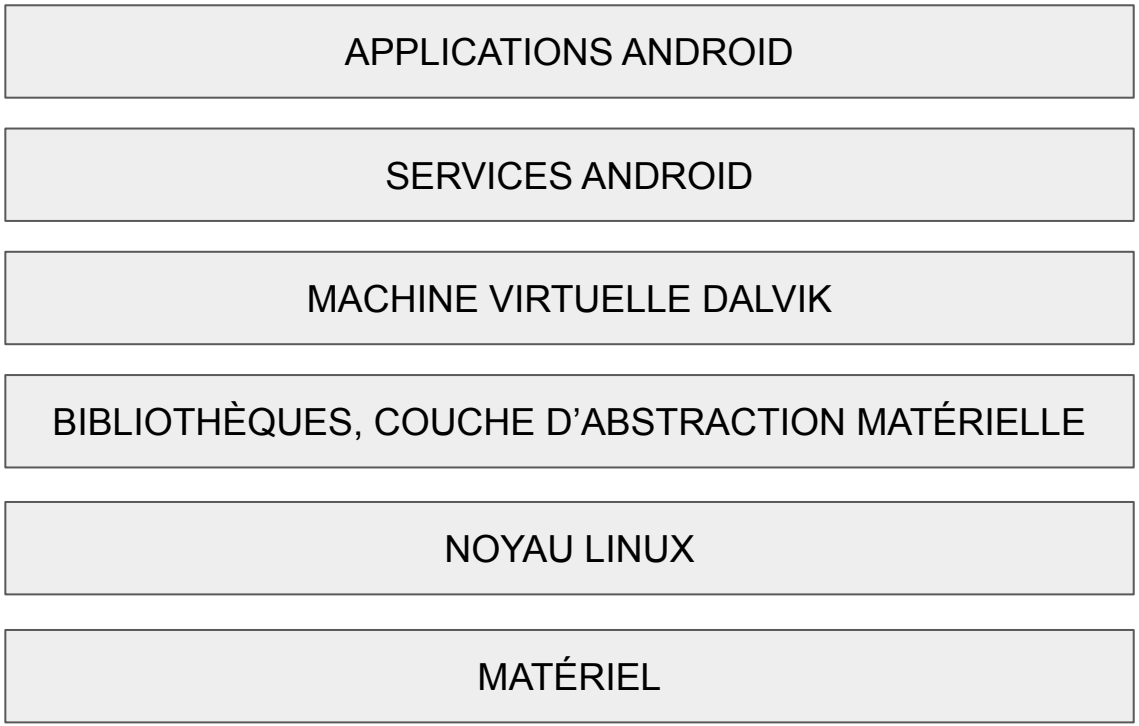
Mise en contexte

- Architecture de sécurité sur Android
- Analyse d’applications malveillantes
- Rencontres hebdomadaires

Architecture ANDROID

- Architecture en couches
- Sécurité en couches
- Sécurité applicative

Architecture en couches

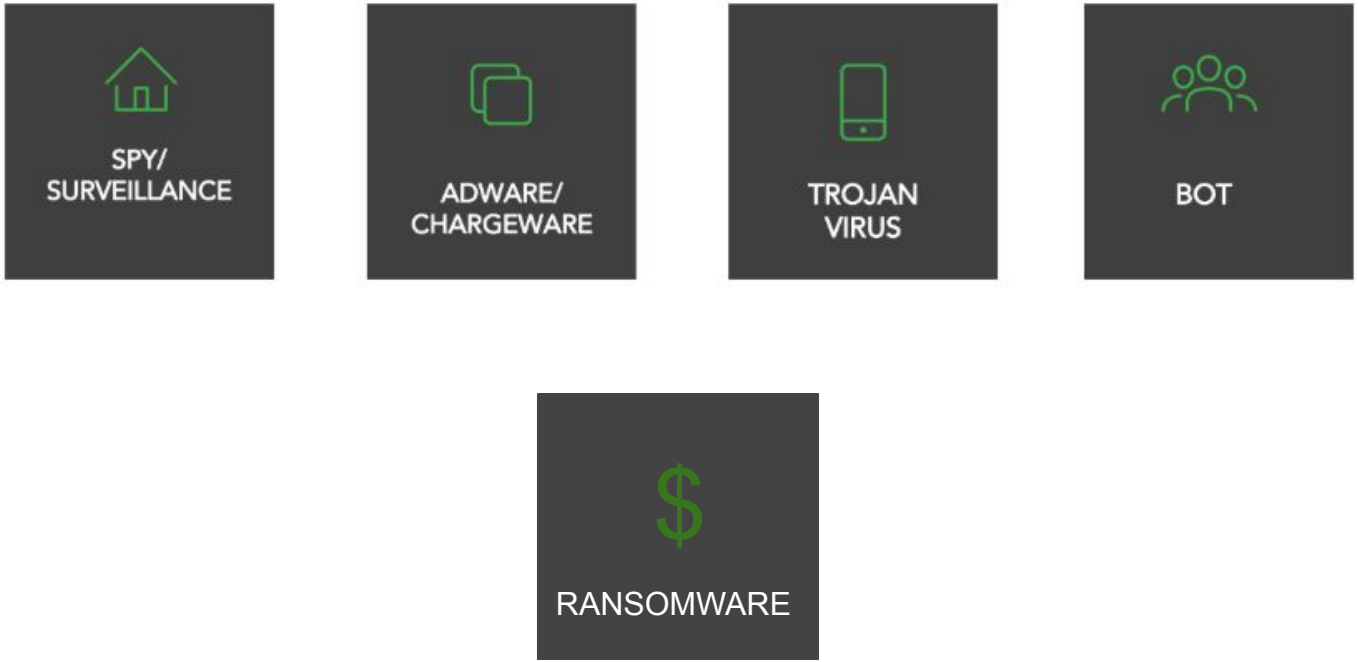


Sécurité en couches

Applications malveillantes

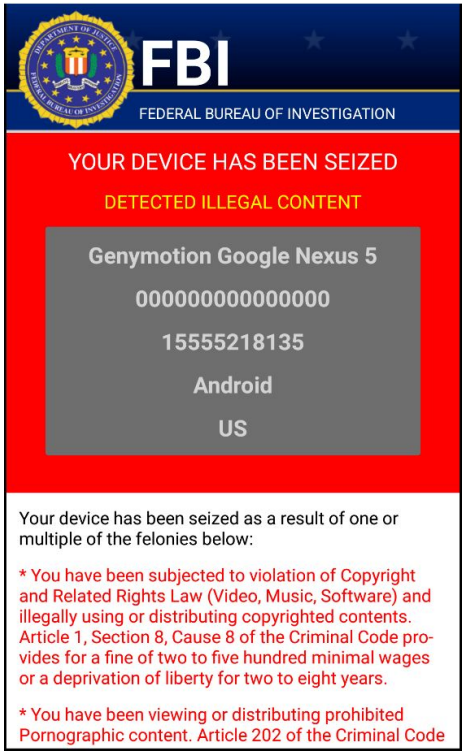
- Types d’applications malveillantes
- Choix d’applications malveillantes

Les familles d'applications malveillantes



Choix des applications malveillantes

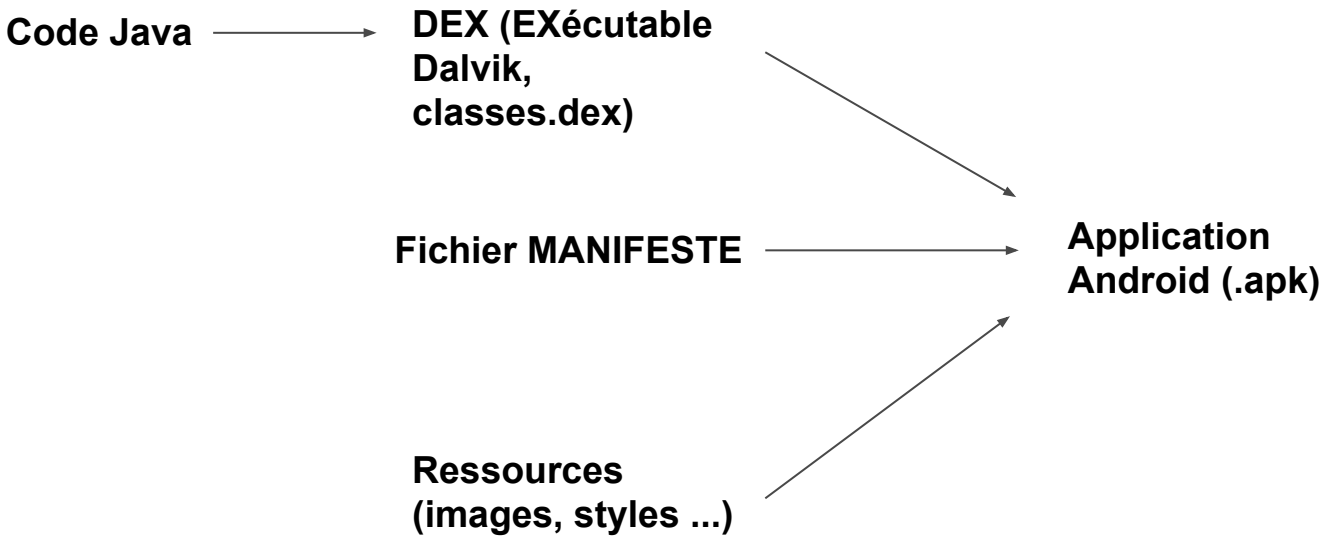
- **CICAndMal2017** de l'institut canadienne pour la cybersécurité
- identification par Hash MD5



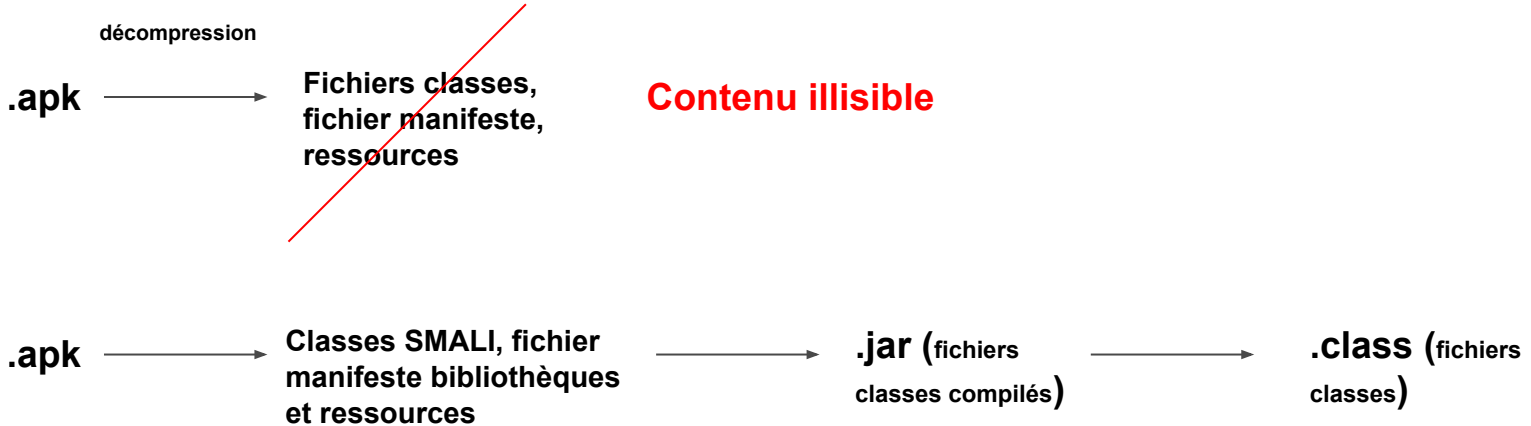
Analyse des applications Android

- Analyse statique
- Analyse dynamique

Création d'une application Android



Analyse statique d'une application Android



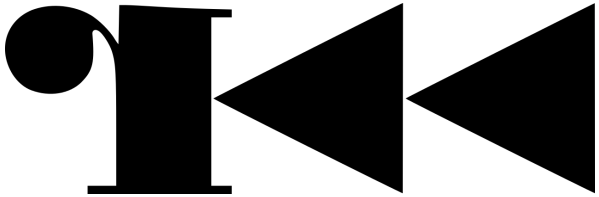
Analyse dynamique d’une application Android

Installer l’application:
- **Téléphone**
- **Émulateur**

Lancer l’application et la monitorer

Récupérer les logs et les analyser

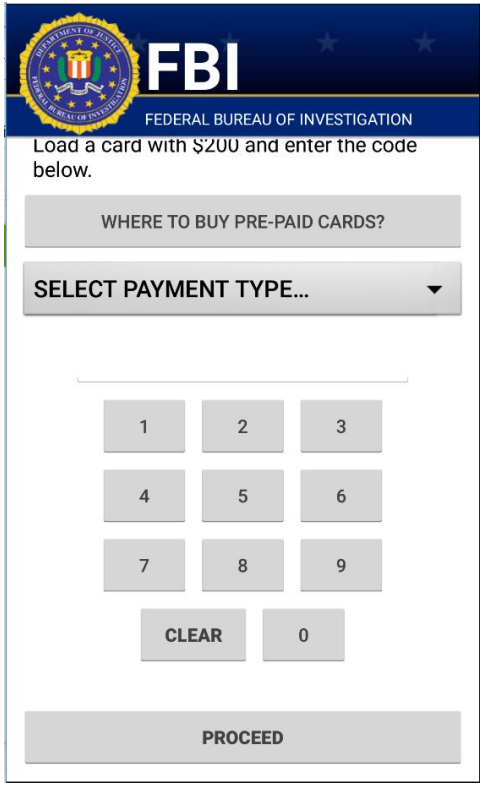
Outil d'analyse d'une application Android

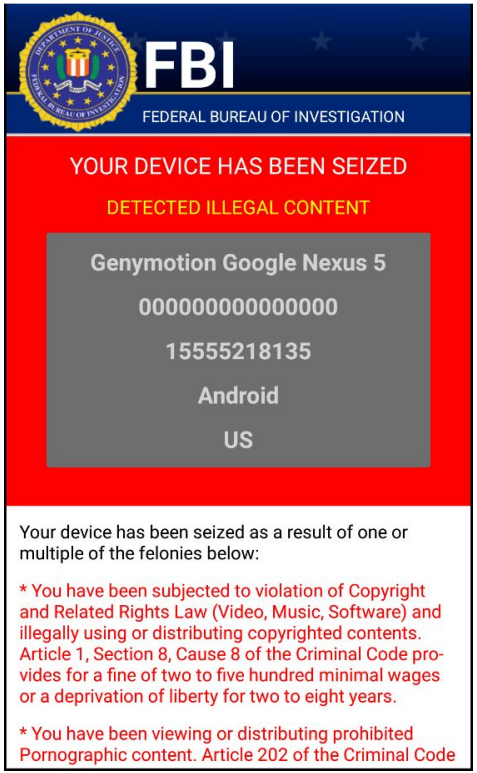


RANSOMWARE 1

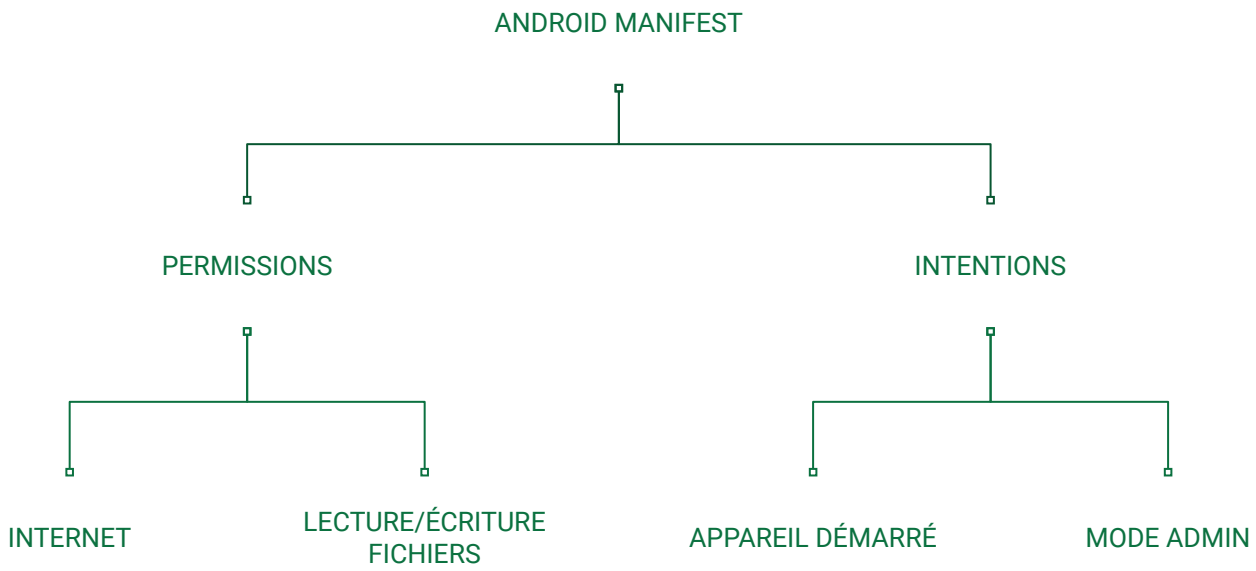
- Analyse statique
- Analyse dynamique

Ransomware1

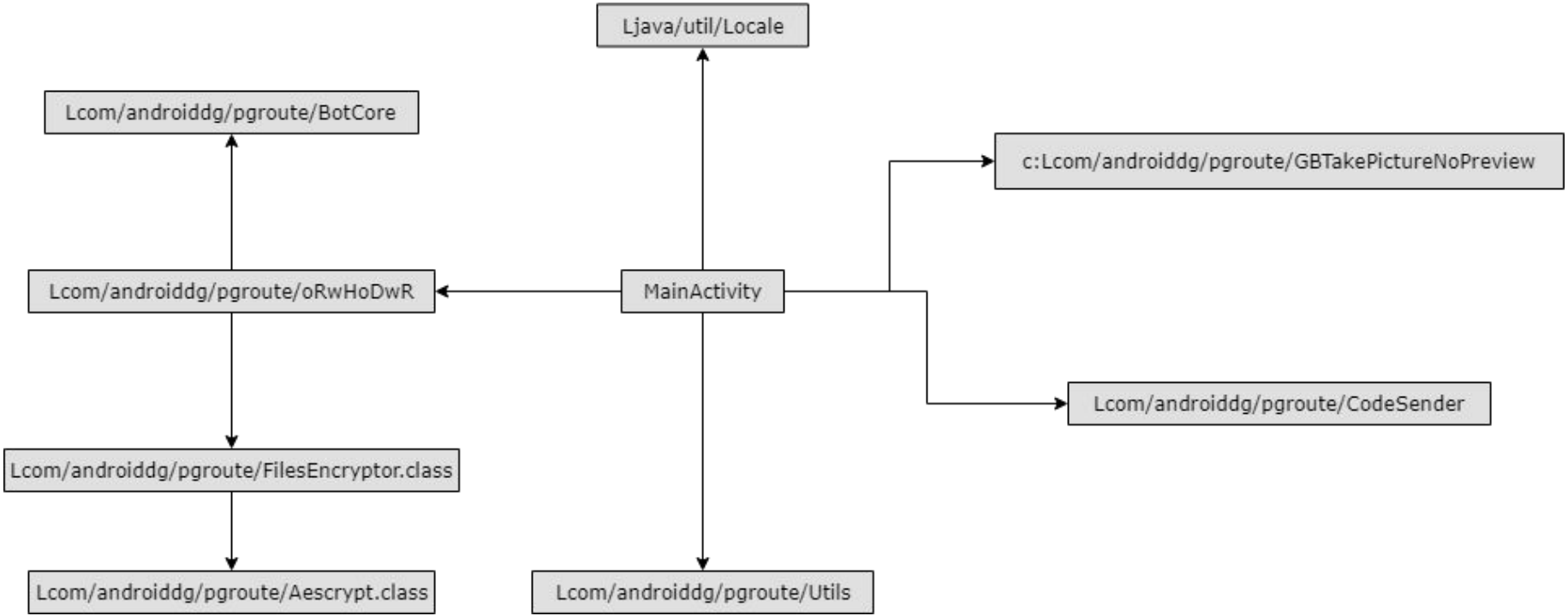




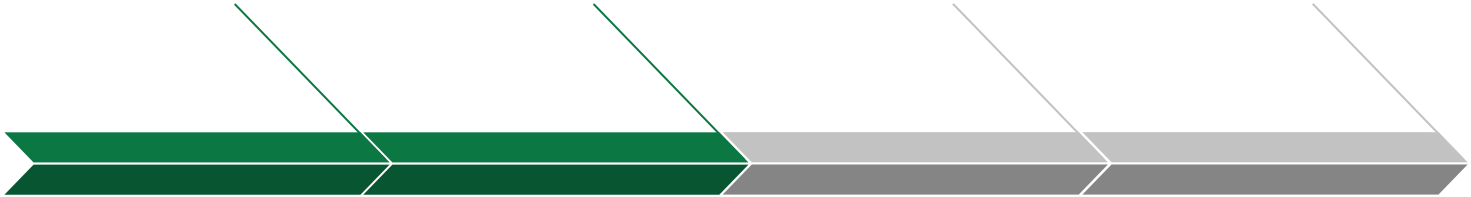
Analyse du Manifest Android



Architecture de classe



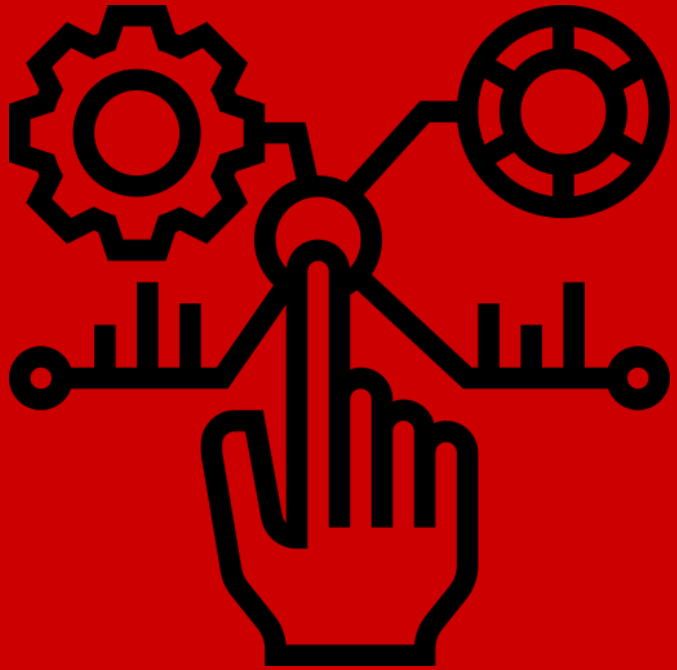
Fonctionnement du Ransomware



Analyse dynamique du Ransomware

01	Analyse des appels aux méthodes	• Application non déboguable • Analyse des arguments et résultats
02	Analyse du flux réseau	• Capture des paquets • Analyse des paquets • Injection de paquets
03	Accès aux données	• Préférences partagées • Accès au dispositif de stockage • Chiffrement des données

RANSOMWARE 2



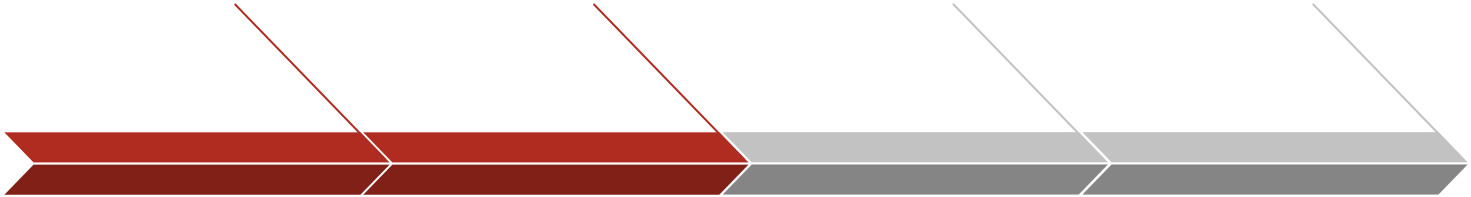
- Analyse statique
- Analyse dynamique

Ransomware2

Analyse statique du Ransomware

01	**Analyse du Manifest**	• Permissions • Intentions
02	**Analyse des classes**	• Changement du fond d'écran • Changement d'icône • Génération aléatoire de la clé de chiffrement • Suppression des données

Fonctionnement du Ransomware2



Récupération de la date et génération de la clé de chiffrement

Chiffrement des données et changement du fond d' écran

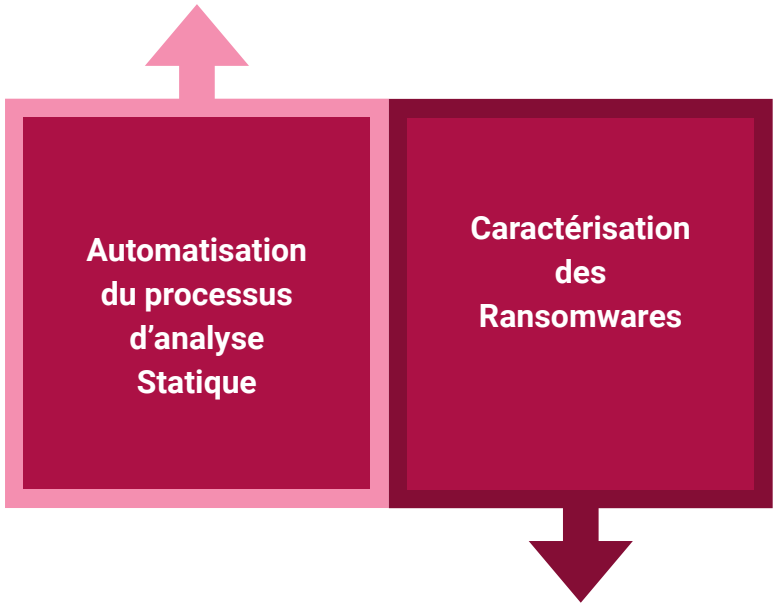
Accusation et demande de rançon dans les délais

Déchiffrement des données/ Suppression des données

Analyse dynamique du Ransomware

01	Analyse des appels aux méthodes	• Analyse des arguments et des résultats
02	Analyse du flux réseau	• Capture des paquets • Inspection des paquets
03	Accès aux données	• Préférences partagées • Accès au dispositif de stockage • Chiffrement des données

Caractérisation des Ransomwares



- apk-analyzer basé sur Radare2
- Journalisation des informations contenues dans le manifeste
- Recherche de symboles dans le code
- Fonction de score

Conclusion et perspectives

- Développement d'un outil d'analyse dynamique

- Amélioration de l'outil de caractérisation des Ransomwares
  - Analyse du contenu de l'application (accusation, rançon)
  - Prétraitement du code de l'application
  - Détecter les appels aux méthodes et leur occurrences
  - Utiliser l'intelligence artificielle

Merci!

Des questions?

Contact: ashiahanimay@gmail.com