

OBJECTIFS

Une plate forme d'analyse statique et dynamique de malware Android

- ▶ Représentation des comportements malveillants par des *System Flow Graph*
- ▶ Reconnaitre statiquement du code malveillant
- ▶ Reconnaitre d'exécutions malveillantes
- ▶ Classification de malware
- ▶ Bibliothèque de malware bien documentée

Verrous

- ▶ reconnaître statiquement du code malveillant parmi du code bénin
- ▶ déclencher du code reconnu comme malveillant
- ▶ produire un résultat d'analyse pertinent et réutilisable
- ▶ mener des analyses sur des milliers d'exemples.

Ressources 2015 → 2018

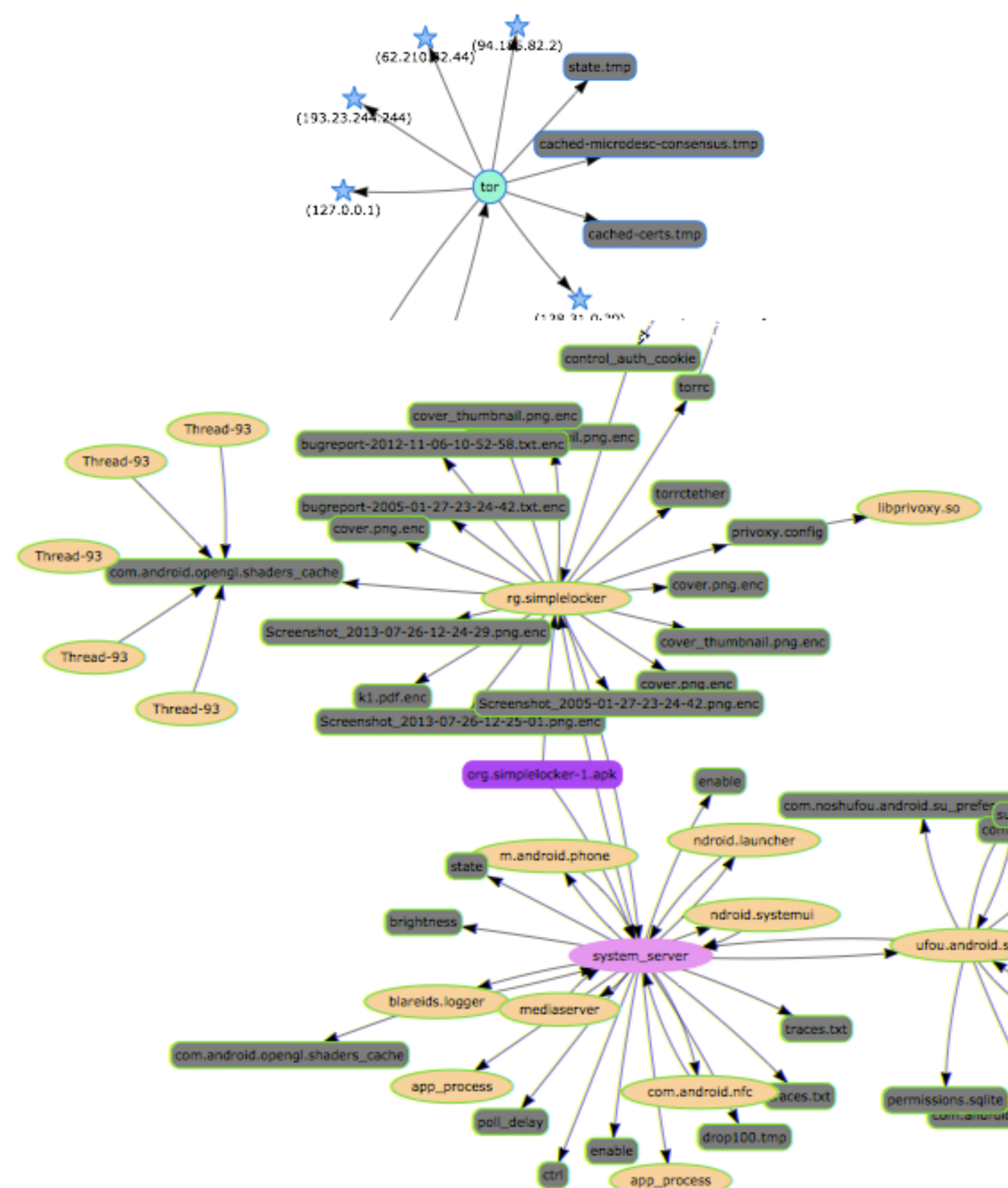
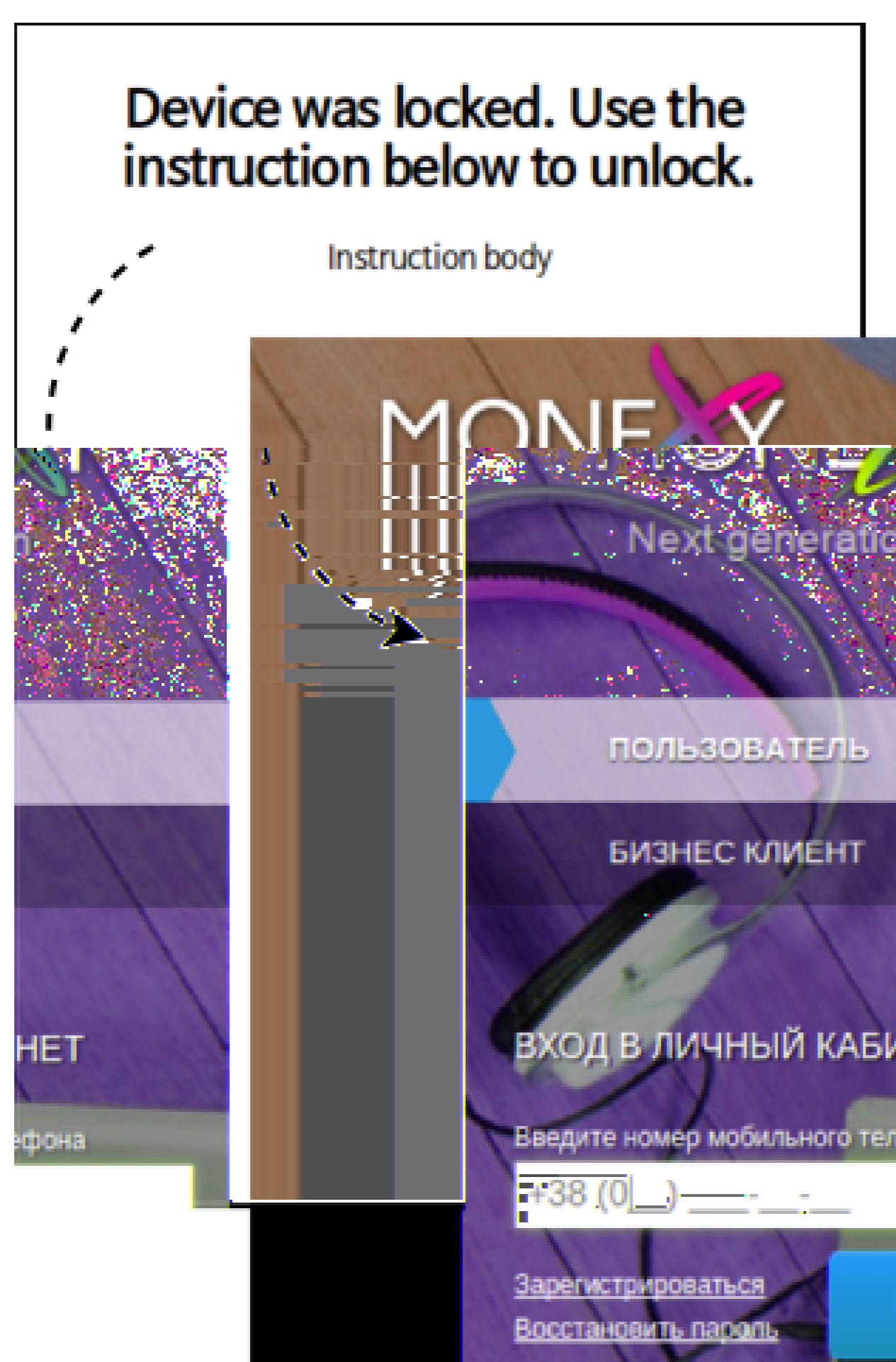
- ▶ Implications de trois membres permanents des équipes Celtique & Cidre
- ▶ 1 ingénieur expert (1 an)
- ▶ 1 stagiaire de M2 (5 mois)
- ▶ 1 *doctorant à partir de l'automne 2015 (3 ans)*
(Sous réserve de son recrutement effectif)

System Flow Graph: Représente comment une application contamine son environnement pendant une exécution

- ▶ graphe orienté
- ▶ les nœuds sont des conteneurs d'information du système d'exploitation (fichier, socket, processus)
- ▶ un arc entre deux objets désigne un flux d'information observé durant l'exécution

Exemple: le malware SimpleLocker

chiffre les fichiers de l'utilisateur et demande une rançon à verser par le service en ligne MoneXy. Ce malware utilise le réseau anonyme Tor pour communiquer avec l'attaquant.



sd.su_preferences.xml
s.sqlite-journal
s.cache

System Flow Graph d'une exécution de SimpleLocker