藉由DroidScope的擴充幫助Android惡意程式分析

9917047 毛　瑩
9917083 朱若慈
9917252 蔡昀延

指導教授　：謝續平 教授

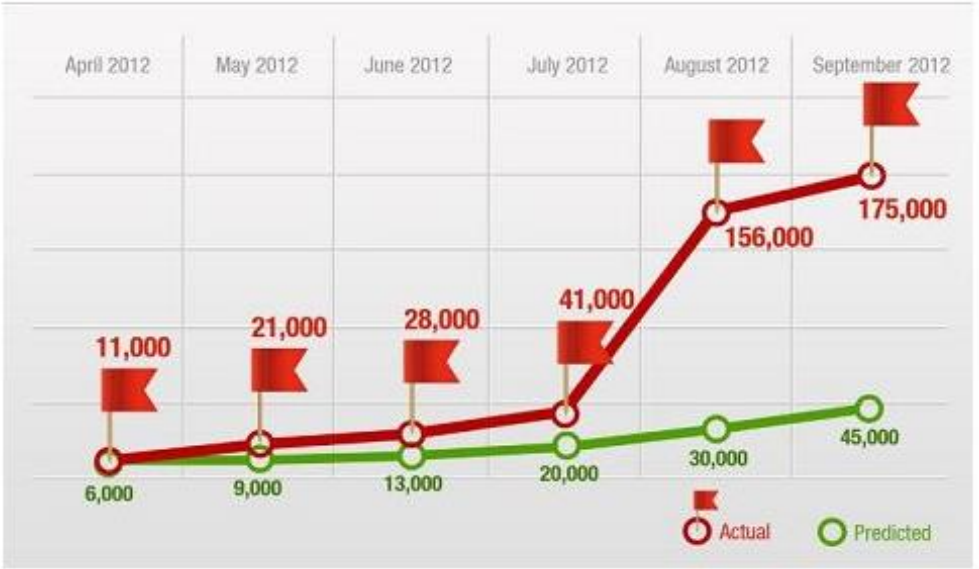
Motivation

- APP市場蓬勃發展
- 但是因為Android自由度及開放性造成許多惡意程式流竄
- 智慧型手機受惡意程式侵害

Target

- 利用現有分析工具提供惡意程式分析介面
  - Root exploit
  - File operations
  - Dalvik instructions

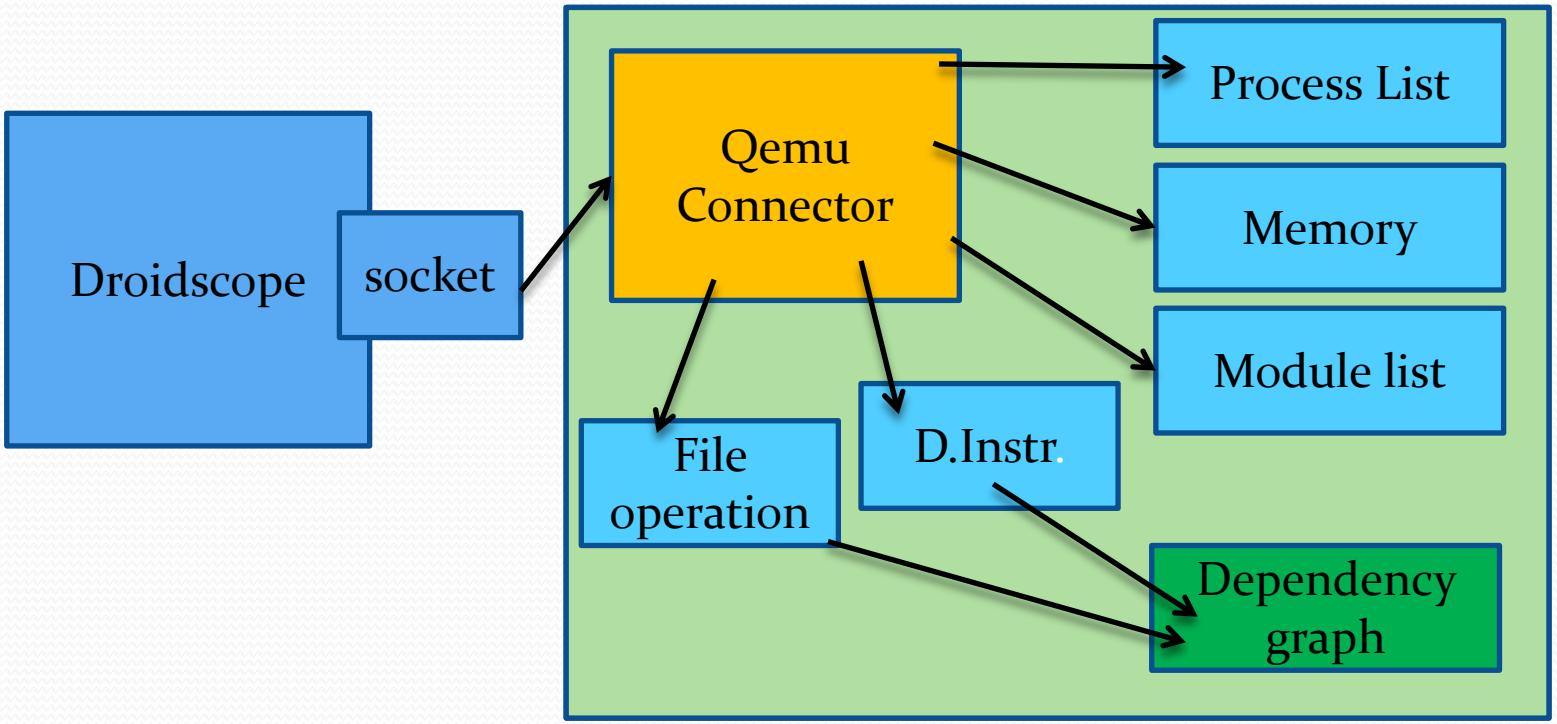
鎖定Android裝置的惡意程式數量持續成長，第二季共偵測到2.8萬個Android惡意程式，到了第三季暴增至17.5萬個，遠高於原先預估的4.5萬個。相對地，只有1/5的行動裝置使用安全軟體。



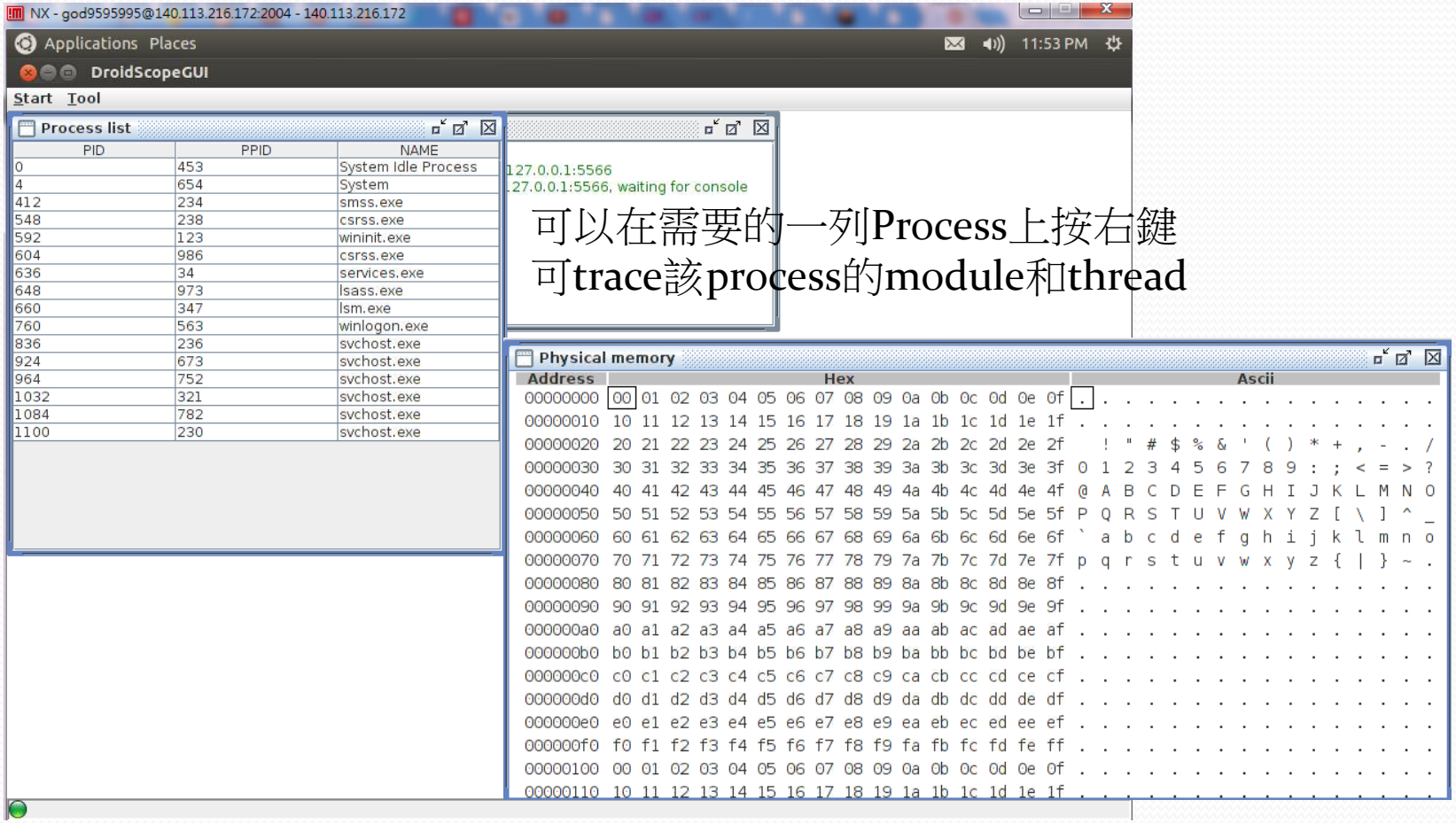
Android惡意程式數量不斷增加，從4月的1.1萬個成長到6月的2.8萬個，9月增加近6倍達17.5萬個。（趨勢2012第三季安全季報）

http://www.ithome.com.tw/itadm/article.php?c=75734

Architecture



Process List & Physical Memory



Dependency graph

- Node
  - Dalvik instruction basic block
- Arc
  - Dependency
- Tag
  - File operations
  - Change of EUID