

# 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

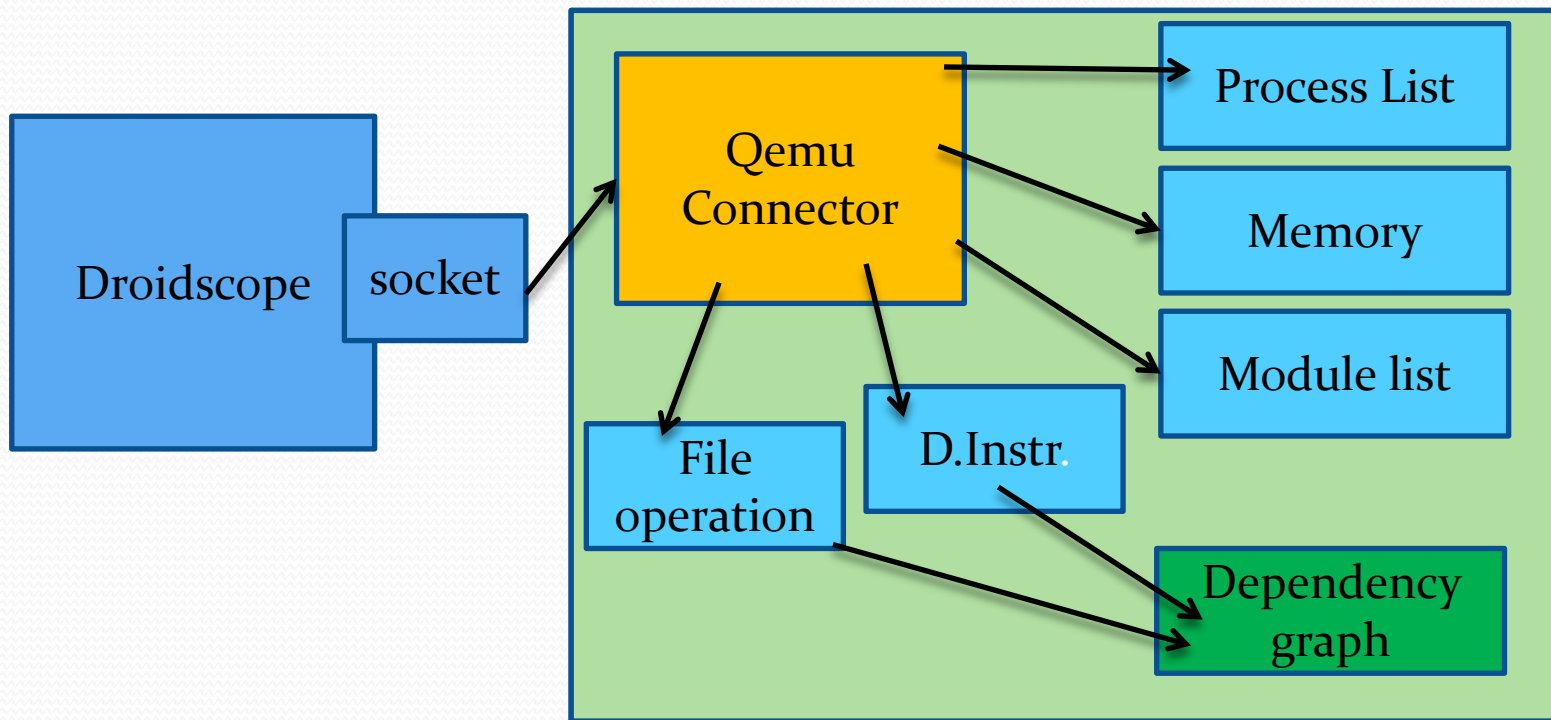
- 利用現有分析工具提供惡意程式分析介面
  - Root exploit
  - File operations
  - Dalvik instructions

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。  
<http://www.it-ebooks.com/news/industry/article.php?id=7134>  
(趨勢2012第三季安全季報)

# Architecture



# Process List & Physical Memory

The screenshot shows the DroidScopeGUI interface. The top bar displays the host information: NX - god9595995@140.113.216.172:2004 - 140.113.216.172. The main window is titled "Start Tool" and contains two panes:

- Process list:** A table listing system processes with columns for PID, PPID, and NAME.
- Physical memory:** A hex dump view showing memory addresses, hex values, and their corresponding ASCII characters.

Overlaid on the process list is a text box with the following text:

可以在需要的一列Process上按右鍵  
可trace該process的module和thread

PID	PPID	NAME
0	453	System Idle Process
4	654	System
412	234	smss.exe
548	238	csrss.exe
592	123	wininit.exe
604	986	csrss.exe
636	34	services.exe
648	973	lsass.exe
660	347	lsm.exe
760	563	winlogon.exe
836	236	svchost.exe
924	673	svchost.exe
964	752	svchost.exe
1032	321	svchost.exe
1084	782	svchost.exe
1100	230	svchost.exe

Address	Hex	Ascii
00000000	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f	.
00000010	10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f	.
00000020	20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f	! " # \$ % & ' ( ) * + , - . /
00000030	30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f	0 1 2 3 4 5 6 7 8 9 : ; < = > ?
00000040	40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f	@ A B C D E F G H I J K L M N O
00000050	50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f	P Q R S T U V W X Y Z [ \ ] ^ _
00000060	60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f	` a b c d e f g h i j k l m n o
00000070	70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f	p q r s t u v w x y z {   } ~ .
00000080	80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f	.
00000090	90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f	.
000000a0	a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af	.
000000b0	b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf	.
000000c0	c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf	.
000000d0	d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df	.
000000e0	e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef	.
000000f0	f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff	.
00000100	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f	.
00000110	10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f	.

# Dependency graph

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

