APP WHITE TEAM

Round3

分析流程


拿到binary
反組譯binary
查出好與壞app的method call
比較method call結果，認出pattern
用上述pattern判別其他app是否有壞行為

拿到4份binary

Private API app類的攻擊

1. 乾淨原始版的計算機
   - Calculator_Clean
2. 有編譯private API header檔但是不會發簡
   - Calculator_SMS_1
3. 有編譯private API header檔而且會發簡訊
   - Calculator_SMS_2
4. 會做螢幕截圖
   - Calculator_Screen

Diff_sms1

- null

Diff_sms2

- +[_OBJC_CLASS_$_CTMessageCenter "sendSMSWithText:serviceCenter:toAddress"...]: 1
- +[stru_8220 _objc_msgSend_ptr_0]: 1
- +[_OBJC_CLASS_$_CTMessageCenter "h3LL0 W0rlD"]: 1
- +[_objc_msgSend_ptr_0 char hasInput;]: 1
- +[stru_8330 _objc_msgSend_ptr_0]: 1

- -[stru_8210 _objc_msgSend_ptr_0]: 1
- -[stru_82F0 _objc_msgSend_ptr_0]: 1

Diff_sms1_sms2

- +[_OBJC_CLASS_$_CTMessageCenter "sendSMSWithText:serviceCenter:toAddress"...]: 1
- +[stru_8220 _objc_msgSend_ptr_0]: 1
- +[_OBJC_CLASS_$_CTMessageCenter "h3LL0 W0rlD"]: 1
- +[_objc_msgSend_ptr_0 char hasInput;]: 1
- +[stru_8330 _objc_msgSend_ptr_0]: 1

- -[stru_8210 _objc_msgSend_ptr_0]: 1
- -[stru_82F0 _objc_msgSend_ptr_0]: 1

Diff_screen

- +[stru_8300 _objc_msgSend_ptr_0]: 1
- +[stru_8220 _objc_msgSend_ptr_0]: 1

- -[stru_8210 _objc_msgSend_ptr_0]: 1
- -[stru_82F0 _objc_msgSend_ptr_0]: 1

Analysis Result

- Diff_sms1結果是空的，所以無法找出有編譯private API header檔但是不會發簡訊的差別
- Diff_sms2結果有找到CTMessageCenter這個Class，所以可以找出有編譯private API header檔而且會發簡訊的差別
- Diff_screen結果沒有明顯的Pattern可以提供辨識，所以無法找出會做螢幕截圖的差別