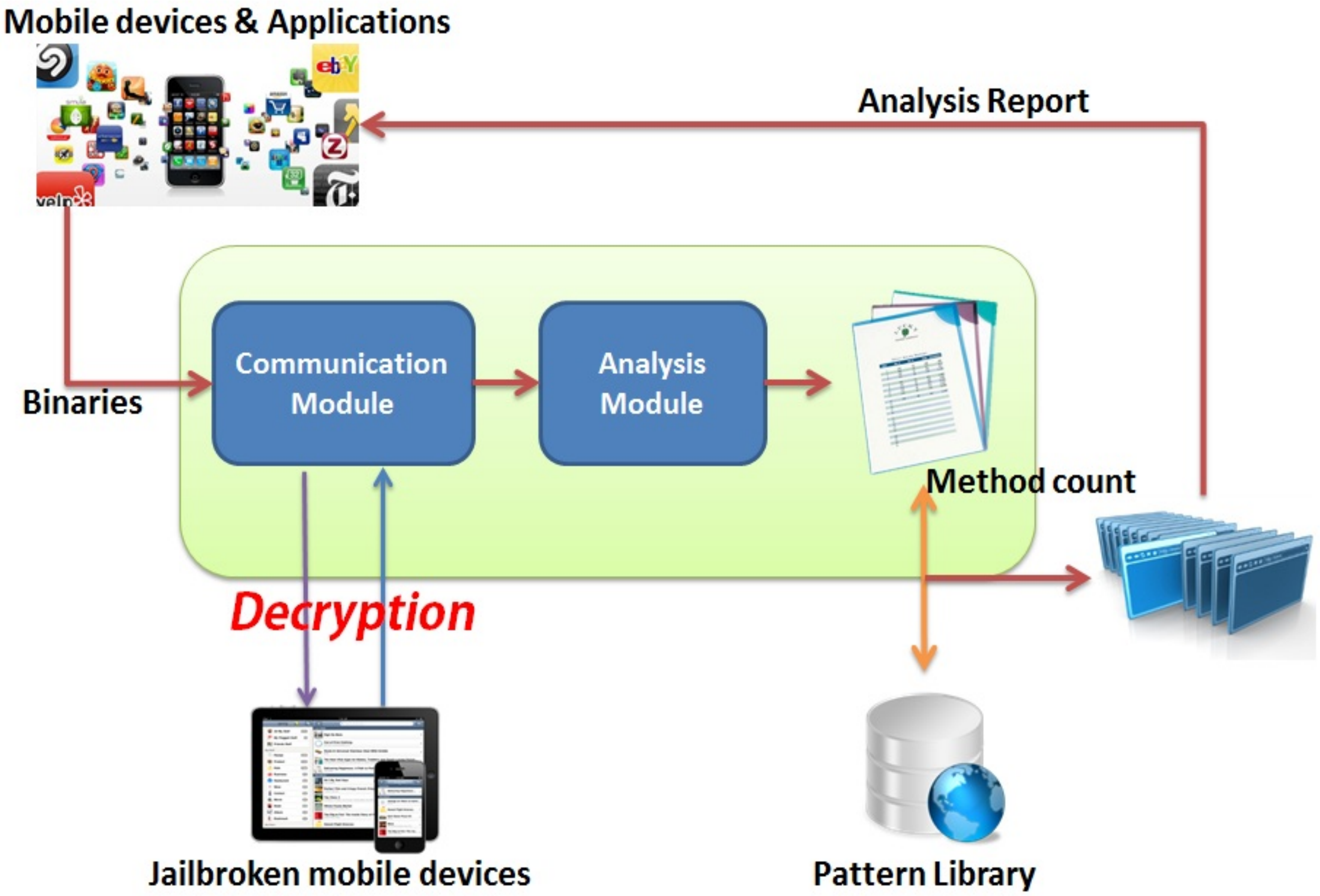
Characterize and Detect Malicious Behaviors in Apps

Fang Yu

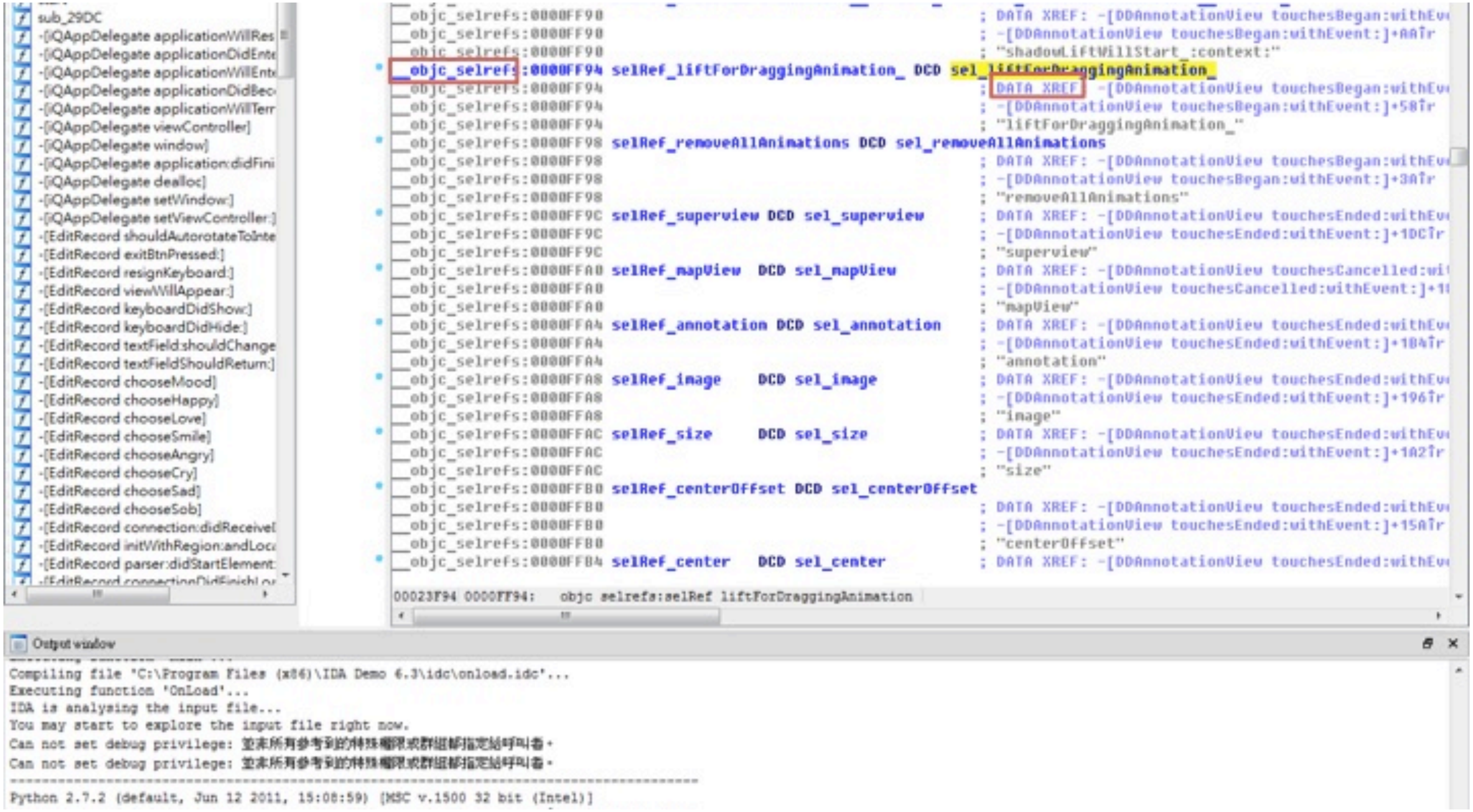
Advance Software Security

April 2, 2013

Analyzing iOS executable



References of system method calls (IDA Pro)



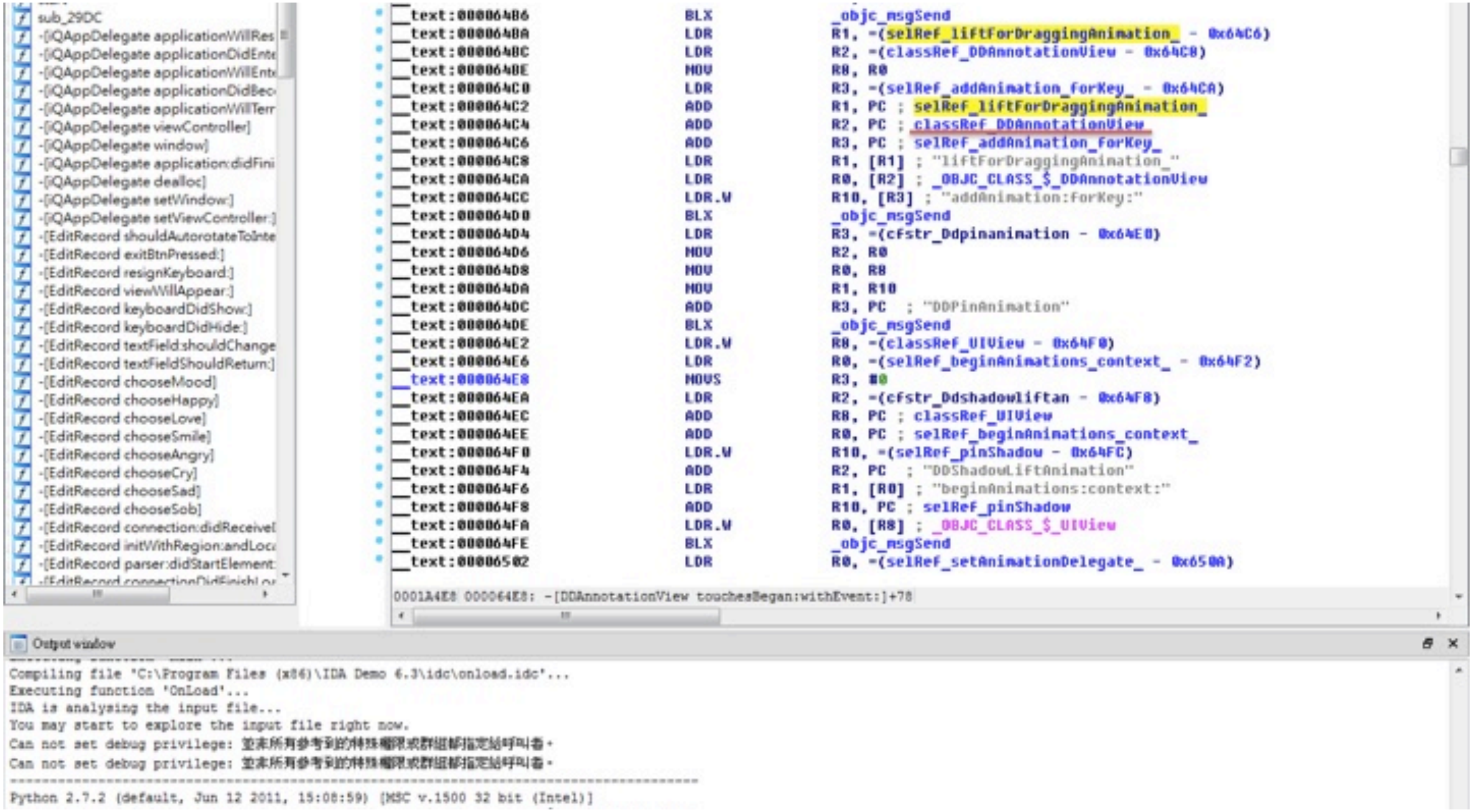
```
sub_29DC
-[iQAppDelegate applicationWillRes
-[iQAppDelegate applicationDidEnte
-[iQAppDelegate applicationWillEnte
-[iQAppDelegate applicationDidBec
-[iQAppDelegate applicationWillTerr
-[iQAppDelegate viewController]
-[iQAppDelegate window]
-[iQAppDelegate application:didFini
-[iQAppDelegate dealloc]
-[iQAppDelegate setWindow:]
-[iQAppDelegate setViewController:]
-[EditRecord shouldAutorotateToInte
-[EditRecord exitBtnPressed:]
-[EditRecord resignKeyboard:]
-[EditRecord viewWillAppear:]
-[EditRecord keyboardDidShow:]
-[EditRecord keyboardDidHide:]
-[EditRecord textField:shouldChange
-[EditRecord textFieldShouldReturn:]
-[EditRecord chooseMood]
-[EditRecord chooseHappy]
-[EditRecord chooseLove]
-[EditRecord chooseSmile]
-[EditRecord chooseAngry]
-[EditRecord chooseCry]
-[EditRecord chooseSad]
-[EditRecord chooseSob]
-[EditRecord connection:didReceive
-[EditRecord initWithRegion:andLoc
-[EditRecord parser:didStartElement:
-[EditRecord connectionDidFinishLo
```

```
__objc_selrefs:0000FF90                                                ; DATA XREF: -[DDAnnotationView touchesBegan:withEv
__objc_selrefs:0000FF90                                                ; -[DDAnnotationView touchesBegan:withEvent:]+AAîr
__objc_selrefs:0000FF90                                                ; "shadowLiftWillStart_:context:"
__objc_selrefs:0000FF94 selRef_liftForDraggingAnimation_ DCD sel_liftForDraggingAnimation_
__objc_selrefs:0000FF94                                                ; DATA XREF -[DDAnnotationView touchesBegan:withEv
__objc_selrefs:0000FF94                                                ; -[DDAnnotationView touchesBegan:withEvent:]+58îr
__objc_selrefs:0000FF94                                                ; "liftForDraggingAnimation_"
__objc_selrefs:0000FF98 selRef_removeAllAnimations DCD sel_removeAllAnimations
__objc_selrefs:0000FF98                                                ; DATA XREF: -[DDAnnotationView touchesBegan:withEv
__objc_selrefs:0000FF98                                                ; -[DDAnnotationView touchesBegan:withEvent:]+3Aîr
__objc_selrefs:0000FF98                                                ; "removeAllAnimations"
__objc_selrefs:0000FF9C selRef_superview DCD sel_superview             ; DATA XREF: -[DDAnnotationView touchesEnded:withEv
__objc_selrefs:0000FF9C                                                ; -[DDAnnotationView touchesEnded:withEvent:]+1DCîr
__objc_selrefs:0000FF9C                                                ; "superview"
__objc_selrefs:0000FFA0 selRef_mapView  DCD sel_mapView                ; DATA XREF: -[DDAnnotationView touchesCancelled:wi
__objc_selrefs:0000FFA0                                                ; -[DDAnnotationView touchesCancelled:withEvent:]+1
__objc_selrefs:0000FFA0                                                ; "mapView"
__objc_selrefs:0000FFA4 selRef_annotation DCD sel_annotation           ; DATA XREF: -[DDAnnotationView touchesEnded:withEv
__objc_selrefs:0000FFA4                                                ; -[DDAnnotationView touchesEnded:withEvent:]+184îr
__objc_selrefs:0000FFA4                                                ; "annotation"
__objc_selrefs:0000FFA8 selRef_image    DCD sel_image                  ; DATA XREF: -[DDAnnotationView touchesEnded:withEv
__objc_selrefs:0000FFA8                                                ; -[DDAnnotationView touchesEnded:withEvent:]+196îr
__objc_selrefs:0000FFA8                                                ; "image"
__objc_selrefs:0000FFAC selRef_size     DCD sel_size                   ; DATA XREF: -[DDAnnotationView touchesEnded:withEv
__objc_selrefs:0000FFAC                                                ; -[DDAnnotationView touchesEnded:withEvent:]+1A2îr
__objc_selrefs:0000FFAC                                                ; "size"
__objc_selrefs:0000FFB0 selRef_centerOffset DCD sel_centerOffset
__objc_selrefs:0000FFB0                                                ; DATA XREF: -[DDAnnotationView touchesEnded:withEv
__objc_selrefs:0000FFB0                                                ; -[DDAnnotationView touchesEnded:withEvent:]+15Aîr
__objc_selrefs:0000FFB0                                                ; "centerOffset"
__objc_selrefs:0000FFB4 selRef_center   DCD sel_center                 ; DATA XREF: -[DDAnnotationView touchesEnded:withEv
```

```
00023F94 0000FF94:    objc selrefs:selRef liftForDraggingAnimation
```

```
Compiling file 'C:\Program Files (x86)\IDA Demo 6.3\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Can not set debug privilege: 並非所有參考到的特殊權限或群組都指定給呼叫者。
Can not set debug privilege: 並非所有參考到的特殊權限或群組都指定給呼叫者。
---------------------------------------------------------------------------------------
Python 2.7.2 (default, Jun 12 2011, 15:08:59) [MSC v.1500 32 bit (Intel)]
```

Resolving the class name of system calls (IDA Pro)



```
sub_29DC
-[iQAppDelegate applicationWillRes
-[iQAppDelegate applicationDidEnte
-[iQAppDelegate applicationWillEnte
-[iQAppDelegate applicationDidBec
-[iQAppDelegate applicationWillTerr
-[iQAppDelegate viewController]
-[iQAppDelegate window]
-[iQAppDelegate application:didFini
-[iQAppDelegate dealloc]
-[iQAppDelegate setWindow:]
-[iQAppDelegate setViewController:]
-[EditRecord shouldAutorotateToInte
-[EditRecord exitBtnPressed:]
-[EditRecord resignKeyboard:]
-[EditRecord viewWillAppear:]
-[EditRecord keyboardDidShow:]
-[EditRecord keyboardDidHide:]
-[EditRecord textField:shouldChange
-[EditRecord textFieldShouldReturn:]
-[EditRecord chooseMood]
-[EditRecord chooseHappy]
-[EditRecord chooseLove]
-[EditRecord chooseSmile]
-[EditRecord chooseAngry]
-[EditRecord chooseCry]
-[EditRecord chooseSad]
-[EditRecord chooseSob]
-[EditRecord connection:didReceive
-[EditRecord initWithRegion:andLoca
-[EditRecord parser:didStartElement:
-[EditRecord connectionDidFinishLoa
```

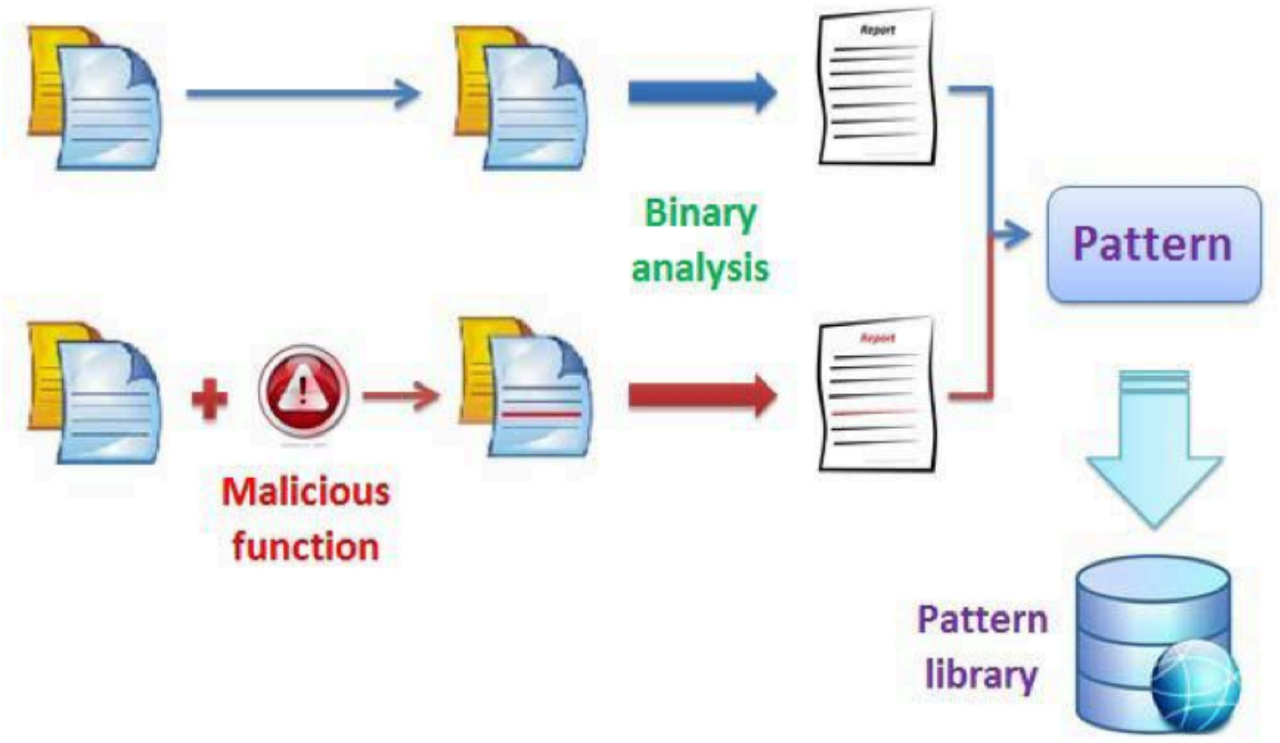
```
__text:000064B6    BLX      _objc_msgSend
__text:000064BA    LDR      R1, =(selRef_liftForDraggingAnimation_ - 0x64C6)
__text:000064BC    LDR      R2, =(classRef_DDAnnotationView - 0x64C8)
__text:000064BE    MOV      R8, R0
__text:000064C0    LDR      R3, =(selRef_addAnimation_forKey_ - 0x64CA)
__text:000064C2    ADD      R1, PC ; selRef_liftForDraggingAnimation_
__text:000064C4    ADD      R2, PC ; classRef_DDAnnotationView
__text:000064C6    ADD      R3, PC ; selRef_addAnimation_forKey_
__text:000064C8    LDR      R1, [R1] ; "liftForDraggingAnimation_"
__text:000064CA    LDR      R0, [R2] ; _OBJC_CLASS_$_DDAnnotationView
__text:000064CC    LDR.W    R10, [R3] ; "addAnimation:forKey:"
__text:000064D0    BLX      _objc_msgSend
__text:000064D4    LDR      R3, =(cfstr_Ddpinanimation - 0x64E0)
__text:000064D6    MOV      R2, R0
__text:000064D8    MOV      R0, R8
__text:000064DA    MOV      R1, R10
__text:000064DC    ADD      R3, PC  ; "DDPinAnimation"
__text:000064DE    BLX      _objc_msgSend
__text:000064E2    LDR.W    R8, =(classRef_UIView - 0x64F0)
__text:000064E6    LDR      R0, =(selRef_beginAnimations_context_ - 0x64F2)
__text:000064E8    MOVS     R3, #0
__text:000064EA    LDR      R2, =(cfstr_Ddshadowliftan - 0x64F8)
__text:000064EC    ADD      R8, PC ; classRef_UIView
__text:000064EE    ADD      R0, PC ; selRef_beginAnimations_context_
__text:000064F0    LDR.W    R10, =(selRef_pinShadow - 0x64FC)
__text:000064F4    ADD      R2, PC  ; "DDShadowLiftAnimation"
__text:000064F6    LDR      R1, [R0] ; "beginAnimations:context:"
__text:000064F8    ADD      R10, PC ; selRef_pinShadow
__text:000064FA    LDR.W    R0, [R8] ; _OBJC_CLASS_$_UIView
__text:000064FE    BLX      _objc_msgSend
__text:00006502    LDR      R0, =(selRef_setAnimationDelegate_ - 0x650A)
0001A4E8 000064E8: -[DDAnnotationView touchesBegan:withEvent:]+78
```

```
Compiling file 'C:\Program Files (x86)\IDA Demo 6.3\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Can not set debug privilege: 並未所有參考到的特殊權限或群組都指定給呼叫者。
Can not set debug privilege: 並未所有參考到的特殊權限或群組都指定給呼叫者。
---------------------------------------------------------------------------------
Python 2.7.2 (default, Jun 12 2011, 15:08:59) [MSC v.1500 32 bit (Intel)]
```

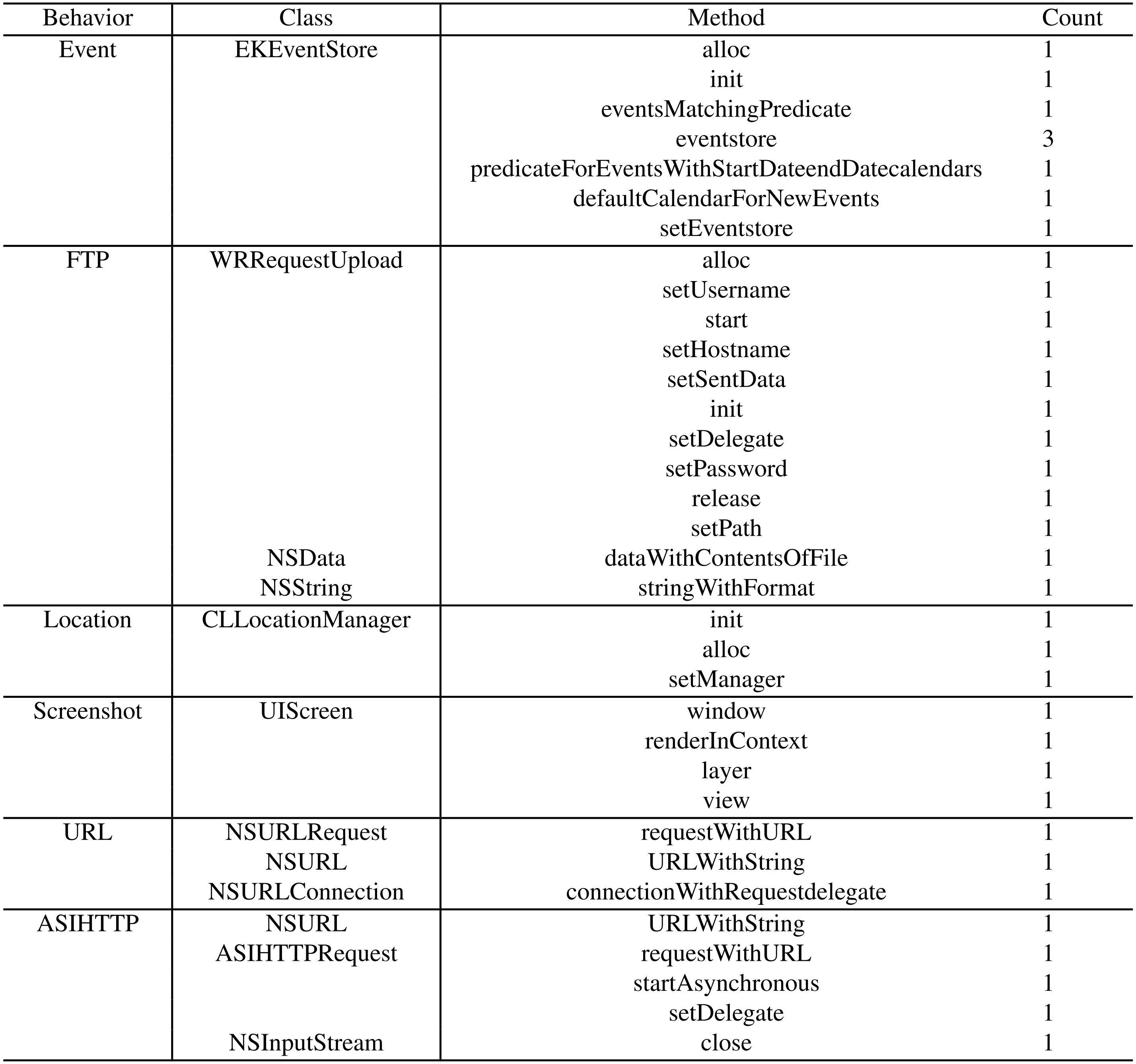
An example of the analysis result

```
…
[ classRef_GAD_GTMStringEncoding sel_rfc4648Base64WebsafeStringEncoding]: 1
[ classRef_NSURL sel_setObject:forKey:]: 3
[ classRef_NSString sel_stringWithUTF8String:]: 16
[ classRef_GADBrowserController_0 sel_init]: 1
[ classRef_NSCharacterSet sel_linebreaksCharacterSet]: 4
[ classRef_GADMNSURLConnectionFactory sel_sharedFactory]: 3
[ classRef_NSString sel_isKindOfClass:]: 2
[ classRef_NSDate sel_dateWithYear:month:day:]: 13
[ classRef_NSDictionary sel_serializeArray:]: 2
[ classRef_GADLocation sel_class]: 1
[ classRef_NSDateFormatter sel_alloc]: 4
[ classRef_GADImpressionTicketGestureRecognizer_0 sel_touchesCancelled:withEvent:]: 1
[ classRef_GADBrowserWebViewDelegate_0 sel_init]: 1
[ classRef_NSNull sel_appendString:]: 2
[ classRef_NSURLResponse sel_alloc]: 2
[ classRef_NSDictionary sel_class]: 19
[ classRef_NSDictionary sel_addObject:]: 2
…
```

Characterizing Malicious Behaviors



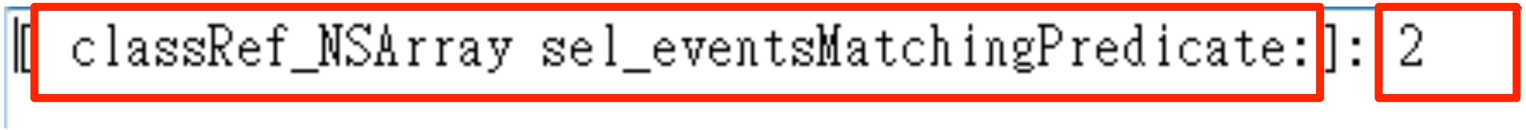
Malicious Patterns



Behavior	Class	Method	Count
Event	EKEventStore	alloc	1
		init	1
		eventsMatchingPredicate	1
		eventstore	3
		predicateForEventsWithStartDateendDatecalendars	1
		defaultCalendarForNewEvents	1
		setEventstore	1
FTP	WRRequestUpload	alloc	1
		setUsername	1
		start	1
		setHostname	1
		setSentData	1
		init	1
		setDelegate	1
		setPassword	1
		release	1
		setPath	1
	NSData	dataWithContentsOfFile	1
	NSString	stringWithFormat	1
Location	CLLocationManager	init	1
		alloc	1
		setManager	1
Screenshot	UIScreen	window	1
		renderInContext	1
		layer	1
		view	1
URL	NSURLRequest	requestWithURL	1
	NSURL	URLWithString	1
	NSURLConnection	connectionWithRequestdelegate	1
ASIHTTP	NSURL	URLWithString	1
	ASIHTTPRequest	requestWithURL	1
		startAsynchronous	1
		setDelegate	1
	NSInputStream	close	1

Identifying Malicious Behaviors

- Pattern

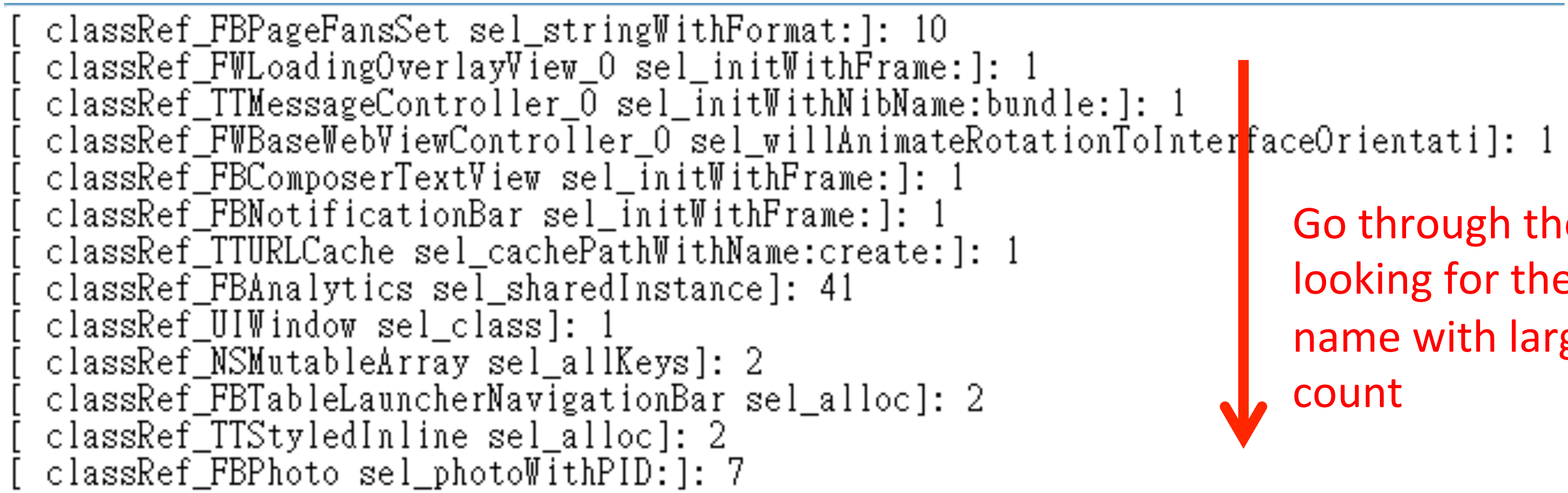


```
[ classRef_NSArray sel_eventsMatchingPredicate:]: 2
```

Class name & method name of sensitive function

Times of such function been called

- Class & method count of Apps



```
[ classRef_FBPageFansSet sel_stringWithFormat:]: 10
[ classRef_FWLoadingOverlayView_0 sel_initWithFrame:]: 1
[ classRef_TTMessageController_0 sel_initWithNibName:bundle:]: 1
[ classRef_FWBaseWebViewController_0 sel_willAnimateRotationToInterfaceOrientati]: 1
[ classRef_FBComposerTextView sel_initWithFrame:]: 1
[ classRef_FBNotificationBar sel_initWithFrame:]: 1
[ classRef_TTURLCache sel_cachePathWithName:create:]: 1
[ classRef_FBAnalytics sel_sharedInstance]: 41
[ classRef_UIWindow sel_class]: 1
[ classRef_NSMutableArray sel_allKeys]: 2
[ classRef_FBTableLauncherNavigationBar sel_alloc]: 2
[ classRef_TTStyledInline sel_alloc]: 2
[ classRef_FBPhoto sel_photoWithPID:]: 7
```

Go through the file looking for the same name with larger count