2016看雪等安全网站android安全最新经典文章第一期总结

转载

ab6326795 于 2018-02-24 11:08:17 发布 348 收藏 1
分类专栏： android安全与逆向


android安全与逆向 专栏收录该内容
74 篇文章 19 订阅
订阅专栏

主要涉及dex，elf，xml等文件结构和一些脱壳，然后so hook和java hook的实现，经过本人实践，一下文章大部分均是可以操纵运行和正确的好文章

一、android安全保护办法总结

http://drops.wooyun.org/mobile/12172 Android应用安全开发之源码全 2016/01/21

http://www.cnblogs.com/develop/p/4397397.html **AndroidVMP加壳 POC**

iOS安全攻防(十九)重组mach-o格式实现简单反ida - 16字节 - 博客园

【原创】APK自我保护方法 -看雪安全论坛

申请会员ID：Colbert仔【未报到，账号删除】 - 『申请专区』 - 吾爱破解论坛 - LCG - LSG |安卓破解|病毒分析|破解软件|www.52pojie.cn

android防破解方法汇总 - beijingshi1的专栏 -博客频道 - CSDN.NET

APK反破解之一：Android Java混淆(ProGuard)-beijingshi1的专栏 - 博客频道 - CSDN.NET

【原创】分享一个菜鸟专用的资源混淆方法 - 看雪安全论坛

【原创】利用文件系统漏洞阻止 apktool,baksmali 反汇编apk - 看雪安全论坛

【原创】安卓加密壳（dexcrypt) , 防止apktool,dex2jar 等工具逆向你的apk，附上下载地址 - 第 2 页 - 看雪安全论坛

【原创】APK自我保护方法 - 看雪安全论坛

【原创】应用资源文件格式解析及阿里破解示例 - 看雪安全论坛

http://drops.wooyun.org/tips/14782 Android勒索软件研究报告 2016/04/13 9:14

二、破解脱壳知识

一、各种脱壳

1.360脱壳

http://bbs.pediy.com/showthread.php?t=192020 【原创】某加固保动态脱壳 2014-09-07

http://bbs.pediy.com/showthread.php?t=190384 【原创】某加密新版动态脱壳 2014-07-22

2.dump出odex结构，根据头部还原dex，等于就是去掉odex头部一点和尾部部分

http://bbs.pediy.com/showthread.php?t=198418 【原创】逆向360加固等dex被隐藏的APK 2015-03-05

http://bbs.pediy.com/showthread.php?t=188793 **【原创】360无线攻防第三题详细分析** 2014-06-07

http://bbs.pediy.com/showthread.php?t=210275 **【原创】360加固成功脱壳** 2016-05-16, 17:14:08

http://bbs.pediy.com/showthread.php?t=210532 **【原创】腾讯加固脱壳**2016-05-26, 17:35:56

3.不用apktool和shakapktool的办法,直接解压，反编译dex

http://bbs.pediy.com/showthread.php?t=200070 **【原创】微信5.3反编译及**

安卓动态调试七种武器之离别钩 – Hooking（上） | WooYun知识库

4、资源保护

http://bbs.pediy.com/showthread.php?t=202303 【原创】微信系列研究之-----资源文件保护的小把戏 2015-07-11

5、反调试和隐藏dex方法

http://drops.wooyun.org/tips/9471 Android应用方法隐藏及反调试技术浅析 猎豹科学院 · 2015/10/1012:20

6、爱加密

http://blog.csdn.net/jiangwei0910410003/article/details/51620236 **Apk脱壳圣战之---脱掉“爱加密”的壳** 2016-06-0917:43

dvmDexFileOpenPartial

dvmLoadNativeCode

7、其它

http://bbs.pediy.com/showthread.php?t=203776 **【原创】Android dex文件通用自动脱壳器** 2015-09-01

https://whitelaning.github.io/2015/09/12/AndroidApkZipEncryption.html AndroidApk 防反编译之伪加密 2015-09-12

http://bbs.pediy.com/showthread.php?t=174825 **【分享】APK伪加密制作和解密** 2013-07-04

http://www.52pojie.cn/thread-287242-1-1.html **apk伪加密技术，附工具** *2014-8-25*

【求助】android_server运行出错 - 看雪安全论坛

【原创】Android软件去广告方法总结[2012.3.6更新工具] - 看雪安全论坛

反调试技术（针对lldb），反调试，antidbg，lldb

IDA_PRO动态调试总结 - Android - 吾爱看雪

通过linker加载so流程ida在.init或ini_array函数下断点_app安全（逆向反编译）_八分饱技术博客

【原创】android动态调试，dex文件脱壳。第一次写东西！高台贵手 - 看雪安全论坛

Android程序的反编译对抗研究 - 跬步者 - 博客园

【原创】360加固成功脱壳 - 看雪安全论坛

【水果忍者炫酷版】内购破解IDE工具图文思路流程，基本通杀 所有电信游戏。 -『移动安全区』 - 吾爱破解论坛 - LCG - LSG |安卓破解|病毒分析|破解软件|www.52pojie.cn

【原创】IDA插件，一键附加调试android so - 看雪安全论坛

http://www.52pojie.cn/thread-334969-1-1.html **【水果忍者炫酷版】内购破解IDE工具图文思路流程，基本通杀 所有电信游戏** **2015-3-5**

三、xposed源码学习

- 【教程】Xposed框架使用教程_三星吧_百度贴吧
- 使用Xposed框架HOOK任意函数及API - 0n1y3nd's Blog
- AndroidHook神器：XPosed入门与登陆劫持演示-CSDN.NET
- 编写基于xposed框架截取账号和密码的外挂和安全防护 -beyond296089727的专栏 - 博客频道 - CSDN.NET
- Developmenttutorial· rovo89/XposedBridge Wiki · GitHub
- 【原创】XPOSED的小笔记 - 看雪安全论坛
- 【原创】XPOSED的小笔记 - 第 2 页 - 看雪安全论坛
- 【原创】Xposed框架初步分析 - 看雪安全论坛
- AndroidHook框架Xposed原理与源代码分析
- Alibaba-DexposedBug框架原理及源码解析 - Coolspan - 博客频道 - CSDN.NET
- Android Hook框架Xposed原理与源代码分析 - H.O.T-WxChevalier - 博客频道 - CSDN.NET
- 深入理解Android（三）：Xposed详解 - 推酷
- 深入理解Android系列书籍资源分享更新 - Innost的专栏 - 博客频道 - CSDN.NET
- 深入理解Android之Xposed详解 - Innost的专栏 - 博客频道 - CSDN.NET

四、androidManifest.xml保护修AndroidManifest.xml导致不能反编译

http://bbs.pediy.com/showthread.php?t=194206 **【原创】AndroidManifest二进制文件格式分析**

http://blog.csdn.net/jiangwei0910410003/article/details/50568487 Android逆向之旅---解析编译之后的AndroidManifest文件格式

http://bbs.pediy.com/showthread.php?t=194201 **【原创】AndroidManifest Ambiguity方案原理及代码** 2014-11-09

http://www.0791quanquan.com/news_keji/topic_1389199/

http://bbs.pediy.com/showthread.php?p=1354330 **【原创】AndroidManifest.xml修复小工具**

五、apk加壳学习

1.apk动态加载和加壳，不通用的方案下，没有通用性

动态加载apk办法，就是不安装，运行一个apk

http://blog.csdn.net/jiangwei0910410003/article/details/48104455 **Android中插件开发篇之----动态加载Activity(免安装运行程序)**

http://blog.csdn.net/jiangwei0910410003/article/details/47679843

Android中插件开发篇之----应用换肤原理解析

http://blog.csdn.net/jiangwei0910410003/article/details/41384667 **Android中插件开发篇之----类加载器**

http://blog.csdn.net/jiangwei0910410003/article/details/17679823 **Android中的动态加载机制**

扩展阅读

http://blog.csdn.net/myarrow/article/details/14223493 AndroidActivityThread(主线程或UI线程)简介

apk加壳没用只能用简单的hellowrold

http://blog.csdn.net/jiangwei0910410003/article/details/48415225 **Android中的Apk的加固(加壳)原理解析和实现**

http://blog.csdn.net/androidsecurity/article/details/9674251 Android4.0内存Dex数据动态加载技术 2013-08-01

2、我试着把上面那个dex加载弄成通用一点的，别人的思路借鉴

http://taoyuanxiaoqi.com/2015/01/16/apkshell2/ APK加壳【2】内存加载dex实现详解 Jan 16 2015

http://taoyuanxiaoqi.com/2015/01/25/apkshell3/ APK加壳【3】通用内存加载dex方案分析

http://bbs.pediy.com/showthread.php?t=205577 **【原创】分享一个快速加载dex文件的方法** 2015-11-07

http://bbs.pediy.com/showthread.php?t=205822 **APK加壳后应用的启动速度问题** 2015-11-16

http://bbs.pediy.com/showthread.php?t=207595 **【求助】Dex加壳内存动态加载遇到的问题** 2016-02-02

http://bbs.pediy.com/showthread.php?t=206169 **[求助]关于Android加壳之内存加载dex的几点疑问** 2015-11-30

http://bbs.pediy.com/showthread.php?t=209305 **【讨论】Dex加壳Application.attachBaseContext被多次执行** 2016-04-11

http://bbs.pediy.com/showthread.php?p=1428821 **【求助】关于使用DexClassLoader加载的一些问题** 2014-11-24

https://segmentfault.com/a/1190000004062866 Android动态加载技术简单易懂的介绍方式 2016-2-10

http://blog.csdn.net/fenglibing/article/details/17471659 实现自己的类加载时，重写方法loadClass与findClass的区别

http://blog.csdn.net/xwl198937/article/details/49801975

基于cydiaHook在线热修复补丁方案

http://blog.csdn.net/hkxxx/article/details/42194387 动态加载APK原理分享 2014-12-27

https://github.com/javazjf/CSApkShellProject 为Apk加壳项目，防止二次打包，代码反编译

3、下面三种框架有用，实现动态加载，最终借鉴下面框架实现吧

http://blog.zhaiyifan.cn/2015/11/20/HotPatchCompare/ 各大热补丁方案分析和比较 2015-11-20

Dexposed、AndFix、ClassLoader

4.解析编译后的apk文件--------dex文件

重点看飞虫大哥那本书吧！！

http://blog.csdn.net/jiangwei0910410003/article/details/50668549 Android逆向之旅---解析编译之后的Dex文件格式

实现自己的类加载时，重写方法loadClass与findClass的区别 - 冯立彬的博客 - 博客频道 - CSDN.NET

6.apk无源码调试

http://www.kanxue.com/bbs/showthread.php?p=1338639

http://bbs.pediy.com/showthread.php?t=199729 **【原创】早期学习写壳代码**

六、2016年java hook大总结

http://bbs.pediy.com/showthread.php?t=192803【原创】Hook Java的的一个改进版本 2014-09-29 11:09:13

http://bbs.pediy.com/showthread.php?t=186054【原创】注入安卓进程,并hookjava世界的方法 2014-03-28 14:16:46

其它的方案

【原创】Hello world 版本Hook java - 看雪安全论坛

http://bbs.pediy.com/showthread.php?t=187522&highlight=java+hook

shuixi2013/AndroidHookJava:Androidso hook JAVA

【原创】手机毒霸去广告功能分析三：java代码（dex）注入 - 看雪安全论坛

dex注入实现详解 | 桃园小七的博客

【原创】抛砖引玉：Hook java方法，抵御静态破解！ - 看雪安全论坛

【注意】【讨论】【求助】看过hook java世界的牛牛看过来。。。 - 看雪安全论坛

七、2016年tomaskingso系列等so结构和linker等学习ThomasKing大大看雪论坛so系列文章

1、so加密函数和加节

http://bbs.pediy.com/showthread.php?t=191649 简单粗暴的so加解密实现 2014-08-26

2、无源码加密实现

http://bbs.pediy.com/showthread.php?t=192047【原创】无源码加解密实现&& NDK Native Hook 2014-09-08

3、修复ELF节

http://bbs.pediy.com/showthread.php?t=192874【原创】ELF section修复的一些思考2014-09-30

4、elfDIY

http://bbs.pediy.com/showthread.php?t=193279【原创】ELFDIY For Anddroid 2014-10-14

5、so dump工具

http://bbs.pediy.com/showthread.php?t=194053【原创】从零打造简单的SODUMP工具 2014-11-04

6.linker载入过程详细

http://bbs.pediy.com/showthread.php?t=197512【原创】SO文件格式及linker机制学习总结(1)2015-02-02

http://bbs.pediy.com/showthread.php?t=197559【原创】SO文件格式及linker机制学习总结(2)2015-02-03

其它人的文章

Android Linker学习笔记 | WooYun知识库

【原创】Linker阅读笔记一 - 看雪安全论坛

【求助】自己写一个linker然后加载另外的so文件 无法执行 - 看雪安全论坛

GCC学习笔记（三）——关于GCC属性中的弱符号（weak symbol) -鍾簡的个人空间 - 开源中国社区

C语言中的强符号与弱符号 - astrotycoon - 博客频道 - CSDN.NET

http://bbs.pediy.com/showthread.php?t=197514&highlight=linker 【原创】Linker阅读笔记一 2015-02-02

http://drops.wooyun.org/tips/12122 Android Linker学习笔记 2016/01/14

http://www.cnblogs.com/ilocker/p/4541936.html

【原创】基于HOOK的Anti-debug调用点trace和Anti-anti- 看雪安全论坛

7.其它一些文章

AndroidNative So加壳技术 - beijingshi1的专栏 -博客频道 - CSDN.NET

求助】libinject 注入zygote - 看雪安全论坛

三六零 so加壳动态脱法 -『移动安全区』 -吾爱破解论坛 -LCG -LSG |安卓破解|病毒分析|破解软件|www.52pojie.cn

动态调试SO之在.init_array段下断点 - 0n1y3nd's Blog

原文链接：http://blog.csdn.net/kingdiggrave/article/details/53993311