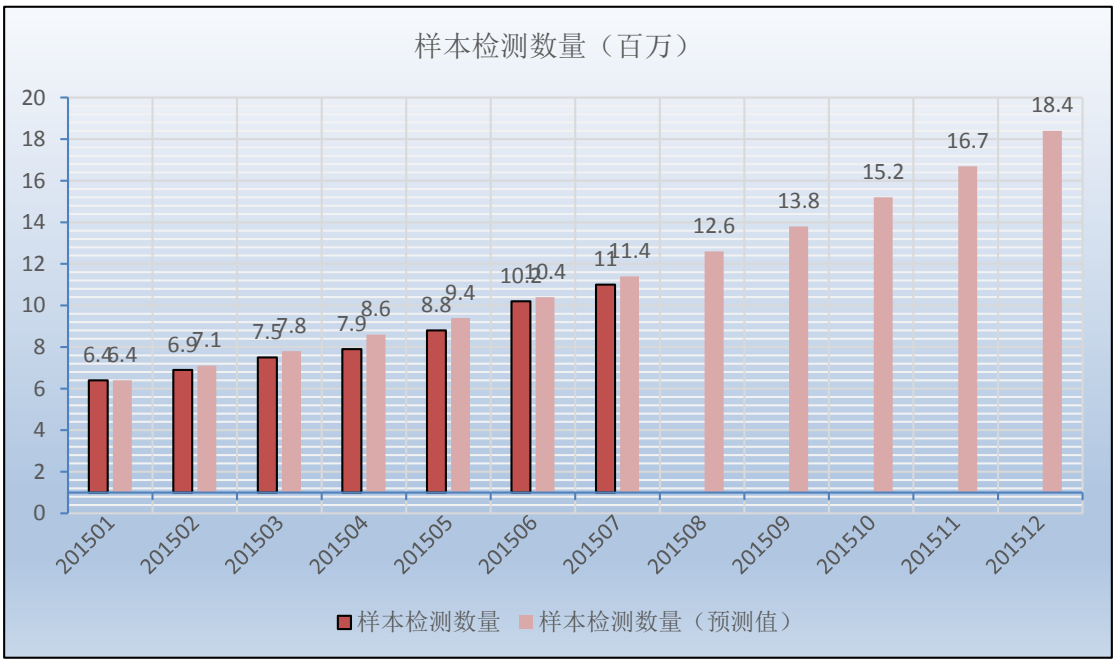
趋势科技移动客户端病毒报告

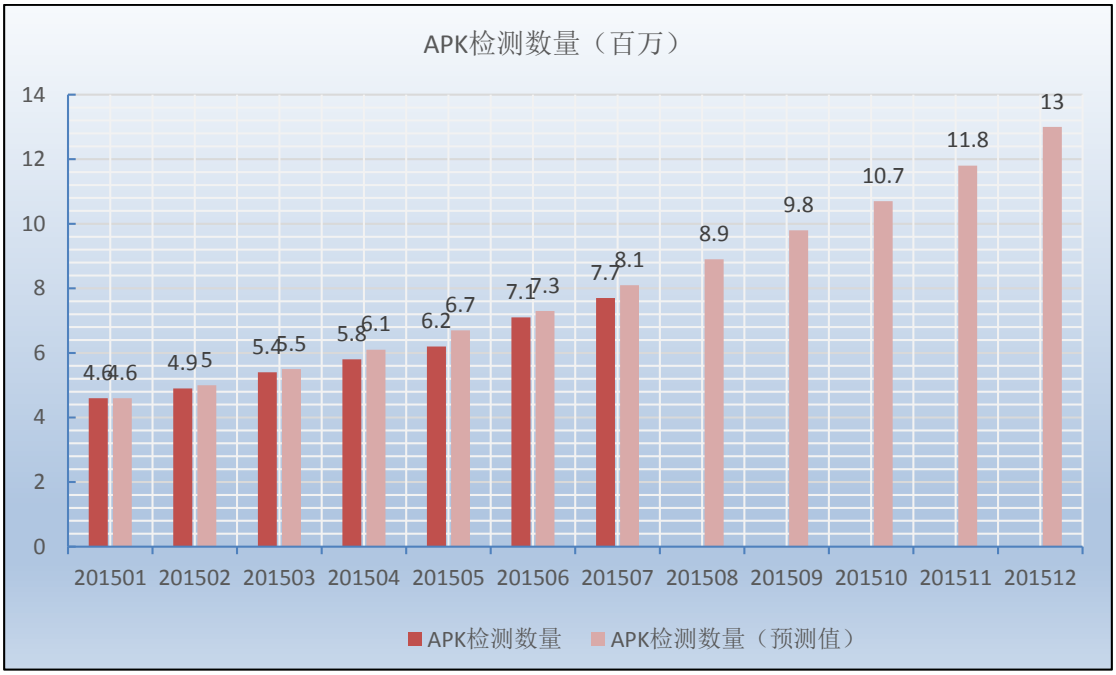
2015年7月移动客户端安全威胁概况

本月，截至 2015.7.31 日，发布中国区移动客户端病毒码 1.925.00，大小 9,168,333 字节。

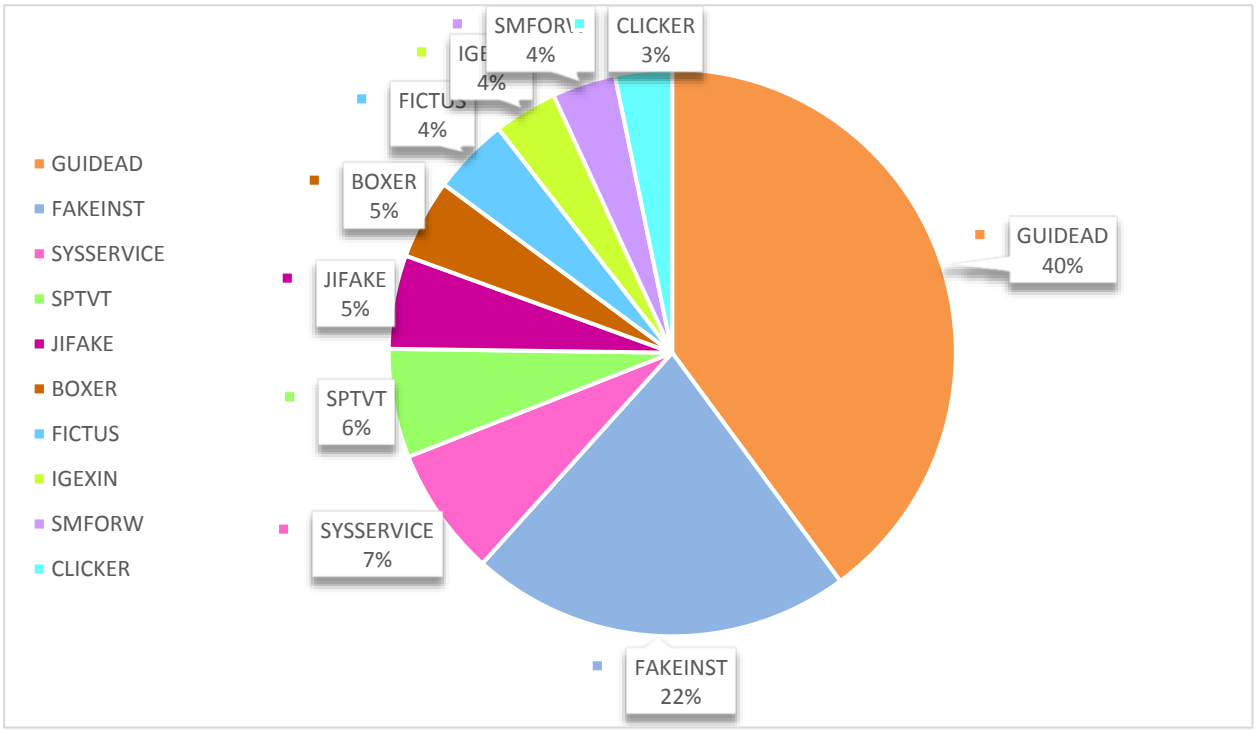
样本检测数量



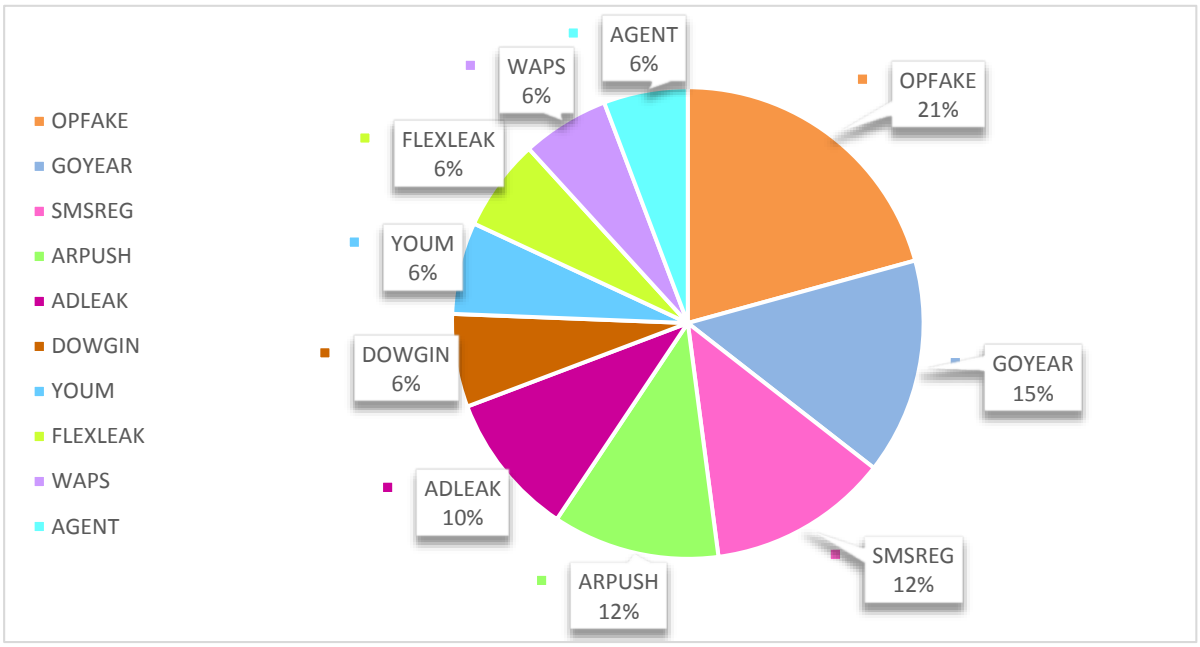
APK检测数量



十大恶意软件家族



十大广告软件家族


OPFAKE
GOYEAR
SMSREG
ARPUSH
ADLEAK
DOWGIN
YOUM
FLEXLEAK
WAPS
AGENT
AGENT 6%
WAPS 6%
FLEXLEAK 6%
YOUM 6%
DOWGIN 6%
ADLEAK 10%
ARPUSH 12%
SMSREG 12%
GOYEAR 15%
OPFAKE 21%

Hacking Team 的 RCS Android 可以监控电话

我们注意到关于 iOS 设备受到 Hacking Team 间谍软件威胁的消息，其实 Android 设备同样会受到威胁。我们在泄露的内部文件中发现开源间谍软件包 RCSAndroid (Remote Control System Android),这个间谍工具套件被用于向客户出售，用来监控目标。（有研究者早在 2014 年已经发现了这个恶意软件，详情请见链接）

RCSAndroid 可以称为目前最复杂，技术最成熟的安卓恶意软件。泄露的源代码为其他黑客生产更多的监控工具提供了素材。

基于泄露的源码，RCSAndroid 可以实现以下监控功能：

- 通过“screencap”命令抓取屏幕截图
- 监控剪切板内容
- 收集 Wifi 网络密码以及网上账户信息，包括 Skype,Facebook,Twitter,Google,WhatsApp,Mail 和 Linkedin 账户
- 收集短信、彩信以及 Gmail 信息
- 收集用户地理位置
- 收集设备信息
- 用前置或后置摄像头拍照
- 收集联系人姓名或从 IM 账户解码信息，包括 Facebook Messenger,WhatsApp,Skype,Viber, Line,WeChat,Hangouts,Telegram 和 Blackberry Messenger
- 通过挂钩系统服务“mediaserver”捕获实时通话内容

RCSAndroid 流行样本

我们的研究显示最早的 RCSAndroid 样本出现在 2012 年。我们是通过其配置文件发现这一时间的。

- 它的 C&C 服务器位于美国，当然现在这个域名已经失效了。

- RCS 通过一个来自捷克的号码的短信来激活。攻击者可以发送特定的信息来激活客户端或者发送相关指令。

- 通过流出的邮件我们发下一个捷克的公司在于 Hacking Team 进行交易，同时进行交易的还有一个奥林匹克运动会的 IT 合作商。

Re: New RCS Hotfix: 8.0.4

Email-ID	528561
Date	2012-05-11 19:27:43 UTC
From	tom[redacted]@[redacted]cz
To	rcs-support@hackingteam.com, jose[redacted]@[redacted]cz

释放集束炸弹

RCSAndroid 的工作方式就像一个集束炸弹，它利用多种危险的 exploit 和技术来感染安卓设备。我们通过分析代码，发现整个系统分为如下四个重要组成部分：

1. 渗透方法，通过短信、邮件或合法程序
2. 底层 native 代码，成熟的 exploit 和间谍工具
3. 高层 Java 代码，恶意 APK
4. C&C 服务器，用来远程发送攻击指令

攻击者通过两种方式使目标下载 RCSAndroid

第一个方法是通过短信或邮件向目标发送精心伪造的 URL。该 URL 会触发默认浏览器的

CVE-2012-2825 内存任意地址读取漏洞以及 CVE-2012-2871 堆溢出漏洞，涉及系统包括从 Android 4.0 到 4.3.这些漏洞利用成功后还可能导致本地提取漏洞的利用。当机器的 root 权限被获得，后门即被安装，RCSAndroid 恶意 APK 也会随之被安装到手机上。

This Android remote exploit targets the default browser installed on Android 4 devices up to version 4.3.*.

In order for the exploit to be effective, customers must provide an URL that the target's browser will automatically load after successful exploitation or in case of error.

Customers must as well provide the APK that will be installed on the target's device, upon a successful execution of the exploit. Such a file can be generated directly from the RCS console by selecting a mobile factory, clicking on "Build", selecting "Installation Package" -> "Android" -> "Create..." and extracting the file called <name>.v2.apk from the generated zip archive.

HT will then provide a URL where the exploit is hosted. A link pointing to the exploit can finally be sent to the target, for instance via sms or email. The full exploit will be served exclusively to Android 4.0.*-4.3.* devices. If the exploit URL is visited from a different browser or device no payload will be executed and the redirect will happen immediately.

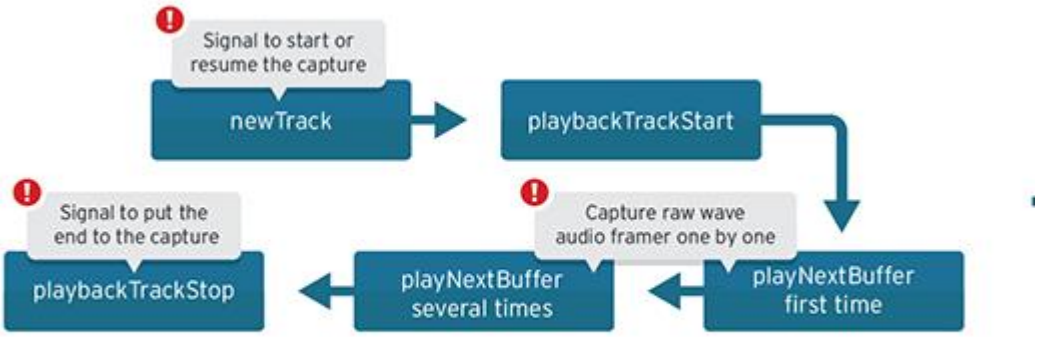
第二种方法是用一个可以绕过 Google Play 检测的后门程序，比如 ANDROID_HTBENEWS.A。在这里 ANDROID_HTBNEWS 以及前面提到的恶意 APK 目的都是来利用安卓设备上的本地提权漏洞。Hacking Team 已经在代码里利用 CVE-2014-3153 和 CVE-2013-6282。这两个漏洞会 root 手机并由此安装后门。

```
fb - try to capture a screen snapshot↓
vol - kill VOLD twice↓
reb - reboot the phone↓
blr - mount /system in READ_ONLY↓
blw - mount /system in READ_WRITE↓
rt - install the root shell in /system/bin/rilcap↓
ru - remove the root shell from /system/bin/rilcap↓
rf <mntpoint> <file> - remove <file> from <mntpoint>");↓
sd - mount /sdcard↓
air - check if the shell has root privileges↓
qzx "command" - execute the given commandline↓
fhc <src> <dest> - copy <src> to <dst>↓
fhs <mntpoint> <src> <dest> - copy <src> to <dst> on mountpoint <mntpoint>↓
fho <user> <group> <file> - chown <file> to <user>:<group>↓
pzm <newmode> <file> - chmod <file> to <newmode>↓
adm <package name/receiver>↓
qzs - start a root shell↓
lid <proc> <dest file> - return process id for <proc> write it to <dest file>↓
ape <content> <dest file> - append text <content> to <dest files> if not yet present↓
srh <content> <file> - search for <content> in <file>↓
```

通过这个后门就可以安装上 RCS 了。这个 RCS 客户端包括两个核心部分，一个是信息收集模块，另外一个是事件触发模块。

- 信息收集模块负责收集前面提到的各种隐私信息。其中最重要的是通话收集功能，这个是通过 hook 系统服务 mediaserver 来实现的

  以语音通话 playback 为例。Mediaserver 会首先创建一个唯一的音轨，循环播放所有的声音缓存，最后停止 playback。声音的波形文件可以通过 getNextBuffer()函数来 dump 下来。借助开源的 Android Dynamic Instrumentation Toolkit 和 root 权限，攻击者可以拦截任何函数的执行。



- 事件触发模块用来根据相应事件触发恶意行为。这些事件可以基于时间，充电，或者电量状态，地理位置，信号强度，运行中的程序，当前程序，SIM 卡状态，短信中的关键字，以及是否锁屏等状态。

  根据 RCS 的配置文件，包括以下行为

  1. 同步配置文件，升级模块，下载新的病毒主体
  2. 上传收集到的信息
  3. 锁定设备
  4. 执行远程命令
  5. 发送指定的短信
  6. 禁用网络
  7. 禁用 root 权限
  8. 取消 root 权限

为了避免在内存中被检测到，RCS 还会检测模拟器和沙箱，用 DexGuard 混淆代码，对 ELF 字符串进行混淆，调整 OOM（out-of-memory）值。有趣的是，还有一个未利用到的功能，它可以通过操纵安卓包管理器里面的数据来添加或者删除程序的权限或者组件，甚至可以隐藏程序的图标。

我们的建议

Android 作为流行的智能手机平台已经成为商业化监控软件的重要目标。攻击懂得通过 root 设备或者恶意 exploit 攻击是控制设备的有效手段。在一个被 root 的设备上，想保持安全简直是天方夜谭。

遵循以下建议可以最大限度地避免此类安全威胁：

- 禁止安装来源不明的第三方软件
- 定期升级系统来避免漏洞攻击。尤其是在 RCSAndroid 这个案例中，系统漏洞可以影响到 4.4.4 KitKat 版本的系统。当然这是通过泄露的邮件得到的信息，Hacking Team 当时已经开始研发针对 Android 5.0 Lollipop 的漏洞利用了。
- 安装手机安全软件

泄露的 RCSAndroid 是一个商业化的监控工具，移动用户受到其带来的安全威胁。一些反常的现象，比如意外的手机重启，不明软件的安装，聊天程序突然失去响应等有时可能意味着手机已经被攻击了。

如果手机已经被感染上该恶意软件，那么没有 root 权限是无法移除它的。用户可以和手机厂商联系重刷手机固件。

趋势科技为您的安卓设备保驾护航，全新的移动安全客户端已经可以防范这类威胁。关于 Hacking Team 带来的 Android 安全威胁，您可以参考以下文章

7 Android Security Hacks You Need to Do Right Now

关于趋势科技（Trend Micro）

趋势科技是全球虚拟化及云计算安全的领导厂商，致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的 1,500 余名趋势科技安全专家可为各国家和地区的企业级个人用户提供 7×24 的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问：www.trendmicro.com.cn。请访问 Trend Watch：www.trendmicro.com/go/trendwatch 查询最新的信息安全威胁的详细资讯。