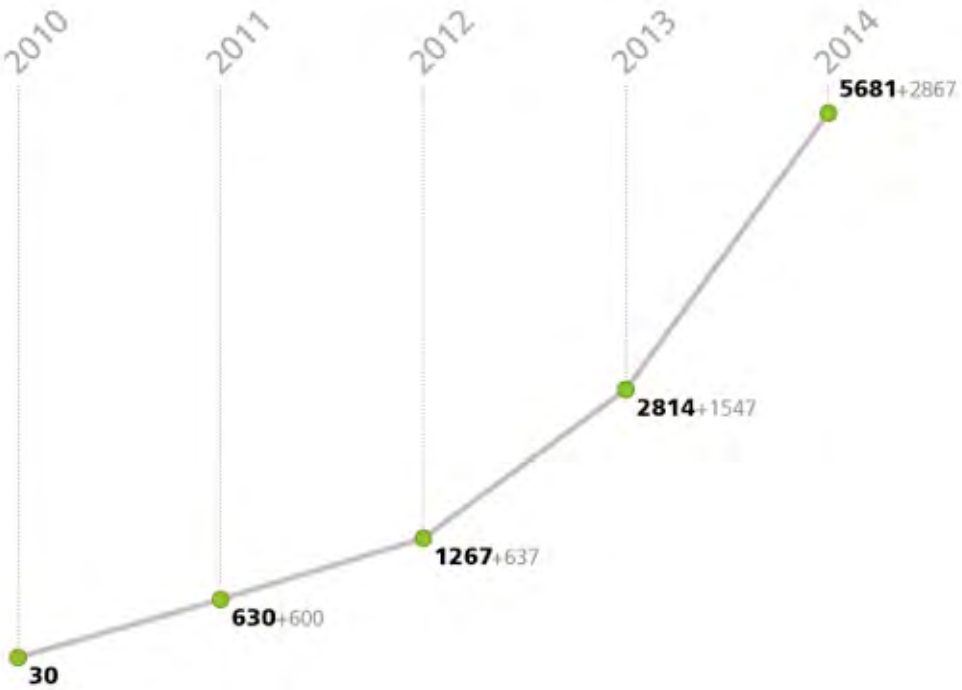
手机盗窃

安卓是用户最常用的移动设备操作系统，也是排在Windows之后病毒编写者的第二个攻击目标。首个安卓恶意程序出现在2010年。

安卓是用户最常用的移动设备操作系统，也是排在Windows之后病毒编写者的第二个攻击目标。首个安卓恶意程序出现在2010年。

下图为Dr.Web病毒库所记录的安卓恶意程序数量增长情况



仅2014年记录数量就增长了102%!

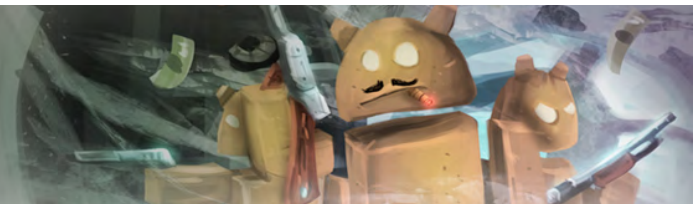
自2010年以来，记录数量增长了188倍!

截止到2015年4月1日，添加到Dr.Web数据库安卓恶意程序特征码已达到近7000个。

这意味着仅2015年前三个月此类恶意程序的数据库记录数量就增长了25%以上！

而一个Dr.Web特征码可侦测的不是一个恶意软件，而是多个恶意程序。

大多安卓恶意程序的用途都是盗窃。



移动设备具有很强大的功能，而安卓木马编写者则有能力窃取一切可能窃取的东西：

- 从移动账户、在线支付系统和银行卡窃取钱财；
- 窃取网上银行系统、电子支付系统和社交网络账户等的用户名和密码；
- SMS短信；
- 通话；
- 电子邮件消息；
- 窃取照片，可使用照片勒索受害人或将其发布到互联网，给用户造成精神损失；
- 移动设备用户通话记录，即便是用户没有进行记录，木马也能自行记录；
- 通讯录；
- 设备定位，也就是可以得知用户所在地点及其移动路线；
- 设备的各类技术信息（IMEI/IMSI/SID标识符、手机号码、操作系统版本、SDK系统版本、设备型号、厂商信息）。

在很多情况下，将恶意程序下载并安装到移动设备的是用户自己！

例如，能够收集并上传被感染设备信息的Android.Plankton在被管理部门从官方网站Android Market（前身是Google Play）删除之前就被用户手动下载了15万次（！）。

Dr.Web for Android的统计信息显示，约50%的用户会允许设备安装未知来源的应用程序（即可以下载非Google Paly软件）。这意味着用户有可能会自己安装从论坛或其他可疑网站下载的恶意应用程序。

网络犯罪分子在使用社会工程学方法大规模传播木马。比如，有超过3万的韩国安卓用户在查询邮件时下载了银行木马Android.SmsBot.75.origin。

大多数用户都确信自己能够发现移动设备有木马活动。

好木马是让用户察觉不到的木马。

病毒编写者在很久以前就掌握了这种技术。

多数情况下，最成功的盗窃木马在实施盗窃后才会被发现。

- 例如，拨号木马Android.Dialer.7.origin为了降低用户发现其活动可能性，在其启用通讯时会关闭移动设备的扬声器，并从系统日志以及通话记录中删除其所有活动记录，达到完全隐藏恶意活动的目的。
- 通过订阅付费服务从手机账户窃取钱财的木马还会对受害者设备进行加密。普通收费服务在成功完成操作时会向用户发送确认短信，而木马会隐藏这些短信，使用户不会在账号被窃前有所察觉。一些恶意程序会自动发送短信确认码来完成付费服务验证，而且会隐藏这些短信。
- 许多“技术先进”的木马伪装成合法程序进行传播，启动后会删除自身图标，使用户无法察觉。
- 还有木马会被不法分子植入操作系统内部或嵌入常见的固件，这种木马权限更广，能够暗中执行众多恶意功能。
- 为了防止被反病毒程序侦测，一些木马还具备对抗反病毒软件的功能：可阻断反病毒软件的运行，甚至能将其从设备完全删除。

银行木马

是从银行卡和网上支付系统盗取资金的安卓木马家族。

移动银行确实很方便。许多银行向用户提供安卓版本的网上银行应用程序。个人和企业都可以利用这些应用程序进行银行支付，通常都是具备账户访问权限的公司高层管理人员才能使用此功能。

盗取用户钱财是病毒编写者进行攻击的最重要的目的。

Android.BankBot.33.origin

能够：

- 获取银行帐户的当前余额和与用户手机绑定的银行卡信息；
- 在被感染设备浏览器加载模仿银行互联网网站外观的欺诈网站，要求受害者输入机密的登录信息；
- 将受害者资金转到不法分子的账户。

由于Android.BankBot.33.origin 能够拦截交易完成后银行发出的短信通知，受害者无法立即发觉账号已被盗。

只要是在操作系统设置为允许从第三方来源安装程序，就等于是用户自己安装这一木马！

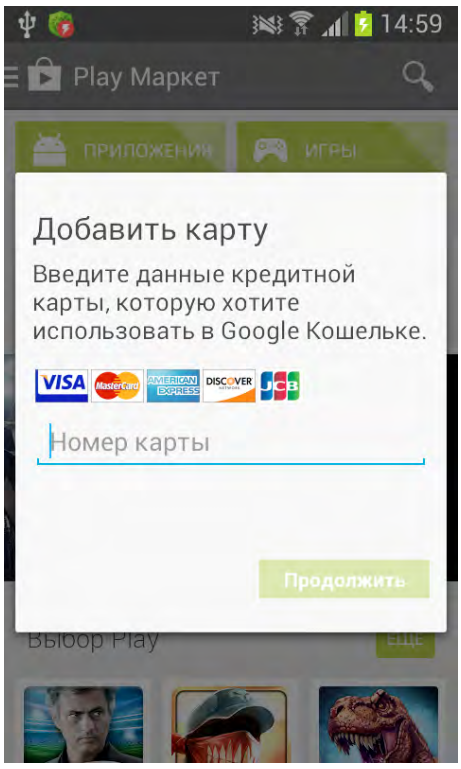
2015年1月到4月，Dr.Web Anti-virus for Android在用户设备侦测到这种木马程序共计62840次，占这一时间段内发现的威胁总数的0.37%。

Android.SpyEye.1

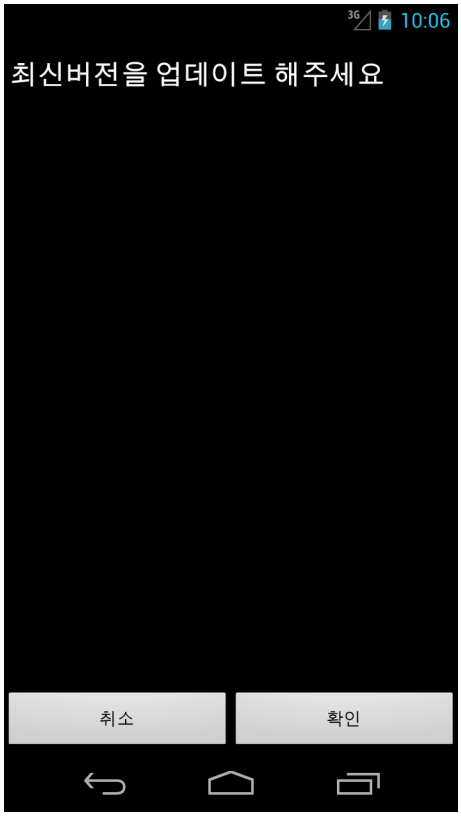
如果台式机用户或笔记本电脑用户访问银行网站，且网站地址记录到感染了计算机的银行木马的配置文件中，则在用户浏览的Web网页中会插入第三方文本或账户访问信息输入格式。不知情的受害者会在浏览器加载银行Web网页，在网页上登录账户，这时会看到所谓的银行新安全措施通知，通知不遵守新措施的用户将无法访问“银行-客户”系统，并建议将移动客户端更新下载到手机，实际上这种更新就是木马程序，一旦被用户下载就会拦截访问“银行-客户”系统的一次性密码短信并将其转发给不法分子。

Android.BankBot.21.origin

为了获取用户银行卡账户信息达到窃取账户金额的目的，Android.BankBot.21.origin 会检查移动设备是否打开Google Play应用程序窗口，如果窗口已打开，木马会伪装成将用户账户与银行卡绑定的标准格式。之后将受害者输入的信息发送到不法分子的服务器。接下来取走资金就是很简单的事了。



Android.BankBot.29.origin



这种木马试图获取移动设备管理员权限时，将相应的系统对话框“隐藏”在自身对话框后，造成大部分用户在不知情的情况下给恶意应用程序提供了管理员权限。接下来木马盗取钱财就变得轻而易举。

拦截短信

有人可能会认为拦截短信没有什么大不了，这要看拦截的是谁发来的短信。

木马拦截哪些短信会给用户造成经济损失?

- 确认或请求开通移动增值服务和内容服务的短信。拦截此类短信后能够让受害者暂时察觉不到订阅了这些服务，也就不会阻止木马活动。
- 来自“银行-客户”系统的含有mTAN验证码的短信。

被拦截的短信会转发到不法分子的木马控制服务器。多个木马家族都具有这种功能。

通过发送短信盗取钱财

例如，Android. SmsSend家族木马能通过从受害者手机发送高价短信，将钱款转到犯罪分子的移动账户上。

Dr.Web for Android的统计信息显示，2014年Android.SmsSend家族木马侦测数量达20223854次。

Android.SmsBot家族木马还能够发送、拦截并删除短信

Dr.Web for Android的统计信息显示，2014年Android.SmsBot家族木马侦测数量达5985063次。

通过拨打收费电话盗取钱财

拨号器是从用户移动设备暗中拨打收费电话的安卓木马家族。这也是病毒编写者常用的“赚钱”方式。

Dr.Web for Android的统计信息显示，2014年 Android.Dialer 家族木马侦测数量达177397次。

盗取通讯录

这种看似完全无关紧要的事情实际上也是不法分子的一门生意。任何一个实际使用的联系方式都可被出售，其购买用途分为：

1. 垃圾短信: 垃圾短信仍十分盛行，而且不只是群发无害的垃圾广告。

包含恶意程序下载链接的短信群发已成为传播安卓威胁的常用方法。

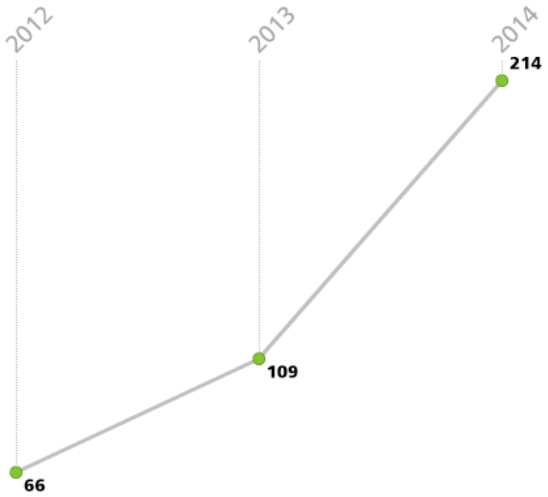
例如，Android.Wormle.1.origin可以通过短信消息在设备持有者的所有联系人间进行传播。到2014年11月末，Android.Wormle.1.origin已感染了来自30个国家用户的15000多个安卓移动设备。

2. **钓鱼木马**：此类木马会收集联系方式，用来发送含有银行系统或支付系统虚假网页链接的钓鱼邮件。如果用户登录这种网站，钓鱼木马就会窃取用户登录网上银行系统的验证信息或银行卡信息。而且用户在不能辨别网站真伪的情况下输入了钓鱼木马所需信息，亲手将这些机密信息发送给不法分子。

3. DDoS攻击：进行这种攻击非常需要移动设备用户的通讯录，感染后用来组织DDos攻击，如攻击竞争对手。

4. 间谍（情报机构，竞争对手）：所有通讯方式对间谍或勒索者都是很重要的信息。实施监视的同时还能阅读用户的来往短信，记录通话，将照片上传到远程服务器。
例如， Android.Spy.130.origin 会向不法分子传送来往短信、通话记录、GPS当前定位信息，还能够暗中拨打指定号码，将被感染的智能手机或平板电脑变成窃听装置。

Dr.Web病毒库中Android.Spy家族木马数量增长情况



您一定经常在使用

- Google Play
- Google Play Music
- Gmail
- WhatsApp
- Viber
- Instagram
- Skype
- « VKontakte «
- « Odnoklassniki «
- Facebook
- Twitter...?

您保存在那里的数据不法分子会很感兴趣：盗窃数据后可将其出售或用来进行敲诈！

Dr.Web抵御不法分子利用安卓设备进行盗窃

保护组件

反病毒
抵御木马及其他恶意程序

防盗功能
在移动设备丢失或被盗时可协助找回设备，必要时可远程删除设备上的机密信息。

防骚扰功能
阻断不需要的来电和SMS消息

URL云过滤器
限制访问不良网络资源，不论Dr.Web for Android病毒库是否进行了最新更新

防火墙
监控应用程序的网络活动

安全审计
生成诊断书，显示安全问题并提出解决问题的方案

有益链接
手机盗窃专题信息