 Android十大吸费病毒软件曝光

第一名：病毒名称：a.payment.dg.a.[系统杀手]

  病毒描述：该病毒被内置到ROM内，具有系统最高权限，不但不能通过正常途径卸载，而且能够阻止指定安全软件被安装，同时发送大量的扣费短信并删除指定号码发送的短信，给用户带来一定的经济损失。

  第二名：病毒名称：a.payment.keji.[饥渴吸费魔]

病毒描述：该病毒捆绑正常游戏软件诱导用户安装，安装主程序后启动，提示升级，用户一确认升级便安装了该病毒子包;同时该病毒尝试利用系统漏洞获取root权限，进行静默安装。病毒激活后，每隔数分钟向号码106\*\*\*56发送信息，并屏蔽10086短信，同时，在后台拨打指定号码，该号码通过服务器远程设定，可能会消耗用户大量的资费;另外该病毒会终止某些安全应用，给用户的手机带来一定的安全隐患。

第三名：病毒名称：a.payment.live.a.[伪google服务框架]

病毒描述：该病毒伪装成系统关键程序(google\*\*框架)，它主要通过其他恶意软件引导下载安装到用户手机，病毒激活后便会在后台从病毒服务器获取扣费端口号和IVR电话号码等信息，无提示向100\*\*\* 发送短信，短信的内容可能是定制高额SP业务，并删除回执短信;此外还会私自拨打IVR电话，在泄露用户隐私的同时，给用户带来经济损失。

第四名：病毒名称：a.payment.ryengine

病毒描述：该病毒安装后开机自动运行，启动后在后台偷偷发送扣费短信，获取短信信息，静默下载软件等流氓行为，给用户的手机安全造成威胁。

第五名：病毒名称：a.payment.jz.[变形\*\*\*王]

病毒描述：该病毒常吸附在被篡改过的知名软件特别是益智类游戏中，病毒激活后会驻后台发送短信，泄露用户隐私;同时，根据服务器返回的指令执行后台拨打电话，在用户毫不知情的情况下肆意消耗用户资费;通过云端控制将不明软件安装在用户手机中并卸载干扰病毒运行的其他软件;驻后台悄悄的自动记录本机所有的短信内容和通话记录，分别存放在名为zjphonecall.txt和zjsms.txt的文件中，并且定期上传到指定的服务器lebar.gicp.n et，导致用户的隐私泄露。

第六名：病毒名称：a.payment.pmx.[刷机吸费大盗]

病毒描述：该病毒安装后没有启动图标，一旦激活便在特定的时间向某些特定的SP号码发送扣费信息，删除相关的反馈信息，让用户在不知情的情况下造成严重的经济损失;同时该病毒还会自动后台联接网络，读取并且上传用户信息，造成用户个人隐私的泄露。

第七名：病毒名称：a.payment.paojapp.[泡椒]

病毒描述：该病毒以常用软件为名诱使用户下载安装，病毒安装运行后，会订购一个名为"\*\*业务 支付\*元/月"的业务，同时病毒将会屏蔽运营商订购回复短信,让用户无法及时了解服务订购信息，在用户毫不知情的情况下，恶意扣取用户资费，带来经济损失。

第八名：病毒名称：a.payment.rootsmart.a

病毒描述：该病毒通过其它恶意应用进行传播，伪装成系统关键程序，在后台受控于其它恶意应用，发送扣费短信并拦截回执，同时自动拨打IVR电话，造成用户资费消耗，给手机用户的安全造成较大的威胁。

第九名：病毒名称：a.payment.webcool.[美 女壁纸]

病毒描述：该病毒常伪装成壁纸应用诱导用户下载，安装后定期在屏幕上方强制弹出广告窗口，定期发送扣费短信并删除指定回执短信，给用户带来直接的经济损失。同时收集用户隐私信息发送到指定邮箱或者服务器，泄漏用户隐私。

第十名：病毒名称：a.payment.fish

病毒描述：该病毒经常伪装成正常软件诱骗用户下载，启动后私自发送扣费短信，给用户的财产安全造成一定损失。