恶意二维码变本加厉 刷码也可导致网银资金被盗

移动安全风险急剧增长 趋势科技提醒用户不要见码就刷

[趋势科技中国]– [2013 年 12 月 5 日] 由于二维码具备方便、快捷的优势，通过“扫一下”来访问二维码信息日益受到欢迎。然而，趋势科技近期却监测发现，大量带有恶意文件下载链接的二维码正不断涌现，用户若盲目“扫”下这些链接背后指向的恶意软件，可能会“中招”并导致网银资金被盗。趋势科技提醒消费者不要盲目扫描二维码，并同时安装趋势科技移动安全个人版（TMMS），以保护个人信息的安全。

在趋势科技监测到的一起事件中，用户扫描二维码后会链接至一个恶意 URL，该 URL 指向的文件为恶意软件安装包。如果用户不加防范的访问该链接，恶意软件安装包就会下载并安装在用户的移动设备内，继而窃取用户的账号密码等个人信息。更可怕的是，在成功窃取信息后，该恶意软件还可能在用户不知情的情况下自动划取账户存款，令受害者蒙受经济损失。

【用微信扫描该恶意二维码后弹出的信息】

趋势科技（中国区）高级产品经理刘政平指出：“在 2013 年 1 月至 9 月期间，针对安卓平

台、以窃取用户信息为目的的恶意程序数量急剧上升，并日益广泛的利用二维码等新手段进行传播。当这些恶意软件抵达用户手机系统之后，往往会在后台监控用户的短信和其他信息。如果用户用手机号码作为某电子商务网站的用户名，黑客很可能用该手机号码登录该网站后选择修改密码，用户手机会收到相关验证码，而此带有验证码的短信一旦被黑客获得，黑客就可以修改密码盗取账户的资金。”

而且，恶意程序不仅仅只有诱导用户下载这一种模式，还会通过某些带有扫描功能应用的漏洞来进行攻击。当用户使用这些应用去扫描带有恶意链接二维码时，则有可能使程序自动执行恶意命令，继而盗取用户个人信息。

对于普通用户来说，要防范此类攻击，需要谨记移动互联网安全保护“规则”，不要随意扫描可疑的二维码，更不要点击扫描后得到的不明链接。此外，**趋势科技还建议用户采取以下防范措施：**

1. 当用户没有主动点击下载过文件，移动设备自动弹出安装程序请求时，要谨慎辨别，不要安装不明程序。
2. 如果已经发现手机收到或向外发送不明短信的现象应及时重视异常情况，并迅速检查账户状态和手机的安全状态。
3. 如果用户对于自己辨识恶意程序或链接的能力不自信，可以安装趋势科技移动安全个人版（TMMS）等移动安全产品进行防护。TMMS 软件基于 Mobile App Reputation 云端评价系统（MARS），可以检查应用程序的安全性，同时给出应用程序是否收集隐私信息、评估泄露个人隐私的风险和指出具体泄漏的内容，让用户安心享受刷二维码带来的便利。

###

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。