手机支付病毒

属手机病毒的一种，包括山寨支付网银类 APP，手机验证码、钓鱼网站、二维码等类型的支付病毒，腾讯移动安全实验室发现，大量被二次打包的支付购物类软件内也被植入有恶意代码。典型病毒代表如“伪淘宝”病毒、“银行窃贼”及“洛克蛔虫”鬼面银贼、盗信僵尸等。

传播方式

手机中的软件，嵌入式操作系统（固化在芯片中的操作系统，一般由 JAVA、C++等语言编写），相当于一个小型的智能处理器，所以会遭受病毒攻击。而且，短信也不只是简单的文字，其中包括手机铃声、图片等信息，都需要手机中的操作系统进行解释，然后显示给手机用户，手机病毒就是靠软件系统的漏洞来入侵手机的。

手机病毒要传播和运行，必要条件是移动服务商要提供数据传输功能，而且手机需要支持 Java 等高级程序写入功能。许多具备上网及下载等功能的手机都可能会被手机病毒入侵。

病毒数据

1、截止到 2016 年第一季度，第三方支付类、电商类、团购类、理财类、银行类这五大手机购物支付类 APP 下载量增长迅猛[1] 。

2、2016 年第一季度支付类软件共 364 款，其下载量占全部软件下载量的 30.38%。

3、2016 年第一季度截获手机病毒包数 143945 个，感染手机病毒用户数达到 4318.81 万。

4、电商类 APP 下载量和该类别感染的病毒包数均排名第一。

典型病毒

“银行鬼手”(a.expense.tgpush)

“银行扒手”(a payment googla b)

“银行毒手”(a.expense.googla.a)

“伪淘宝”(a.privacy.leekey.b)

“短信盗贼”（a.remote.eneity）

“盗信僵尸”（a.expense.regtaobao.a）

“鬼面银贼”（a.rogue.bankrobber）

攻击对象

1．攻击为手机提供服务的互联网内容、工具、服务项目等。

2．攻击 WAP 服务器使 WAP 手机无法接收正常信息。

3．攻击和控制“网关”，向手机发送垃圾信息。

4．直接攻击手机本身，使手机无法提供服务。

5．破坏手机应用程序，试软件或者游戏无法正常运行。

6．窃取手机私人信息，侵害个人隐私。