TREND MICRO 趋势科技

全程护航
迈向云端

您的手机安全吗

前言

进入了信息化的时代，手机在人们的生活中扮演了越来越重要的角色。手机本身也从最初的只能打电话或发短信的通讯工具朝着智能化方向快速的发展，俨然成为一台随身携带的小电脑，而智能手机用户数量也在飞速增长。

中国互联网络信息中心发布的《第27次中国互联网络发展状况统计报告》显示，我国手机网民规模达3.03亿，并有望在2014年超越PC网民。其中，智能手机数量保持迅猛增长势头，预计2014年，智能手机数量将超过5.1亿。

手机病毒的兴起

智能终端和移动互联网的发展使越来越多的手机用户开始使用丰富的手机应用，如此庞大的用户群，高速发展的智能手机平台，以及高速的移动通讯技术，为手机恶意程序提供了发展空间。由于手机和资费紧密相联，经济利益的驱动使移动应用产业链中的部分环节出现不法现象，垃圾短信、骚扰电话、恶意扣费、电信诈骗等问题给手机用户带来很大的困扰和损失。

手机病毒的四大危害

1 用户信息被窃

1.1 窃取个人信息

窃取个人信息

越来越多的手机用户将个人信息存储在手机上，如个人通讯录、个人信息、日程安排、各种网络帐号等。这些重要的资料，都是恶意程序的窃取对象。例如之前饭店业名人希尔顿的手机通讯录即在莫名其妙的状况下遭窃，后依专家研判指出，有可能是黑客通过蓝牙入侵所致。

1.2 交易资料外泄

交易资料外泄

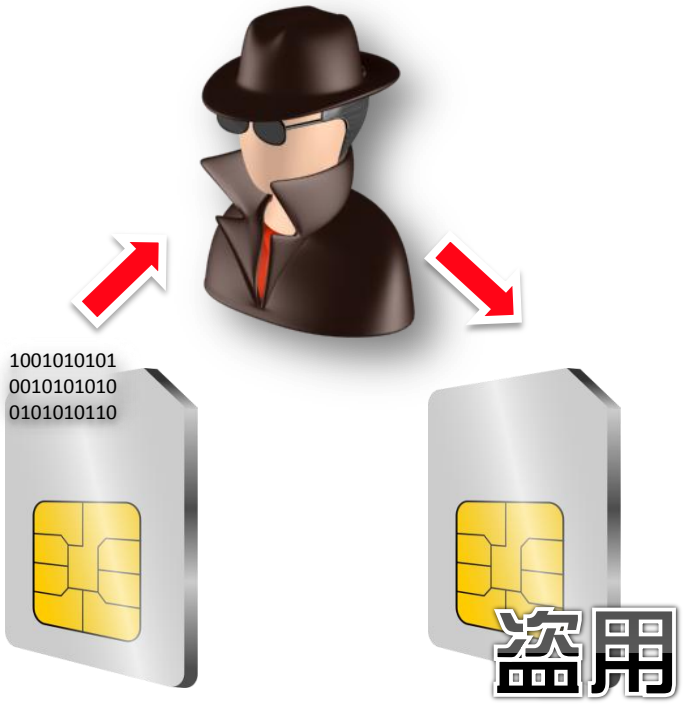
手机也可以进行在线交易以及付款，所以银行账号密码等也可能会被黑客盗窃，造成使用者的经济损失。

1.3 窃取照片或文件资料

窃取照片或文件资料

大多数只能手机都带有照相以及文档编辑功能，所以使用者存储在手机上的照片或文档也可能会被黑客窃取用于敲诈勒索。

1.4 窃取手机及SIM卡信息



窃取手机及SIM卡信息

感染病毒的手机会将自身的手机串号.或SIM卡的SISM 信息反馈给手机病毒制造者,从而使被感染手机或手机号码被利用.可能被利用来发送 广告短信或其他用途.

1.5 窃取用户通话及短信内容

窃取用户通话及短信内容

这类手机病毒具备窃听通话、窃取短信、监听手机环境音和定位地理位置等功能，使得黑客对手机使用者的隐私了如执掌。

手机病毒的四大危害

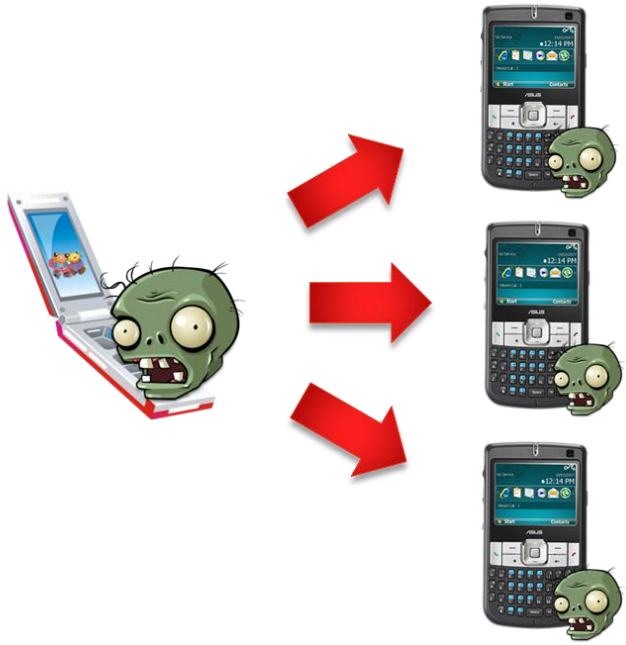
2 收发恶意信息

2.1 成为僵尸手机

成为僵尸手机

一些被感染的手机，会将自己的号码或信息上传到恶意地址，从而接收到一些别有用心的恶意信息，一旦访问了信息中涉及到的恶意网站或下载运行了其中的文件，便会造成不良后果。

2.2 传播垃圾短信



传播垃圾短信

被病毒感染的手机可能在用户不知情的情况下发送垃圾信息。虽然一些垃圾短信并不带有危害性，但是却耗费了发信人的资费，并且浪费了收信人的宝贵时间。而且如果垃圾短信中包含有病毒就会导致收件人也被感染，成为了病毒和垃圾短信的帮凶或僵尸机器。

手机病毒的四大危害

3 造成经济损失

3.1 通过短信造成扣费

通过短信造成扣费

一旦手机用户不慎感染存在屏蔽业务短信行为的恶意软件，将让手机几乎成为“瞎子”，任由其通过后台实施恶意扣费等行为。例如：某种恶意软件及其变种会在感染用户手机后，会通过外发短信给SP号码的形式从中扣取用户的手机资费。

3.2 通过自动拨号造成扣费

通过自动拨号造成扣费

恶意软件植入用户的智能手机之后，会自动外拨电话至指定的SP业务号码。由于此号段会单独收取高额的SP费用，一旦拨打此号码将对用户造成相当程度的资费损失。

手机病毒的四大危害

4 破坏手机软硬件

4.1 手机硬件损坏

手机硬件损坏

恶意病毒制造者可能通过手机操作系统平台漏洞攻击手机导致机器死机或者频繁的开关机，这会造成手机零件或寿命的损害。有些病毒，例如SYMBOS_LOCKNUT木马还会造成手机按键功能丧失。

4.2 手机安全软件无法使用

手机安全软件无法使用

手机病毒可能伪装成防毒厂商的更新包，诱骗用户下载安装后使手机安全软件无法正常使用，这样一来就可以为后续的攻击行为打开方便之门。

4.3 手机内置卡的损坏

手机内置卡的损坏

早期的黑客会通过SIM卡的资讯存取长度的漏洞来展开对SIM卡的直接破坏，用户因此无法正常使用手机。

现在智能手机内一般都会有存储卡，所以也可能面临被黑客破坏或格式化的风险，造成重要数据的丢失。

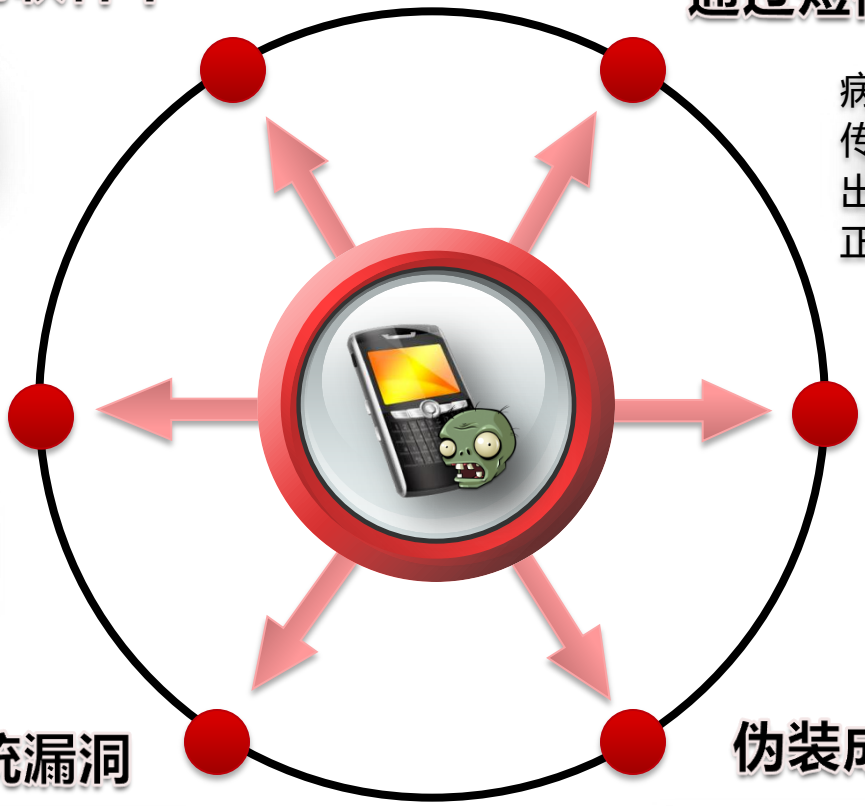
手机病毒的感染及传播途径

捆绑在正常软件中

很多病毒将自身捆绑在正常应用中，用户在安装这些应用时在无意间便被感染。

通过短信或彩信

病毒利用短信或彩信进行传播，造成手机内部程序出错，从而导致手机不能正常工作。



通过蓝牙

手机中了该病毒后，使用蓝牙功能对邻近有漏洞的手机进行扫描，并会复制自己到存在漏洞的手机上。

通过手机上网

在手机上网时,无意中访问了包含恶意恶意代码的网站,导致信息被窃取。

通过手机系统漏洞

病毒通过带有病毒程序的短信传播，只要用户查看带有病毒的短信，手机即刻自动关闭。

伪装成正常软件

某些手机病毒会将自己伪装成安全软件或游戏,一旦用户安装此病毒程序则会导致安全软件失效。

手机安全防护小贴士

手机安全防护小贴士 (一)

提高手机安全意识

- ✓ 不要在不安全的网站留下自己的手机号
- ✓ 应对诈骗短信要谨慎
- ✓ 在使用蓝牙之类设备时注意安全设置
- ✓ 在不需要上网时将手机的网络连接功能关闭
- ✓不使用破解软件
- ✓ 注意安装手机安全防护软件

手机安全防护小贴士（二）

密切关心自己的手机资费情况

✓ 每个月最好能够关注一下自己的话费详单，发现有不明扣费时及时联系运营商询问。

手机安全防护小贴士（三）

下载应用程序后及时进行安全检测

- ✓ 不要在不知名的论坛或网站下载手机软件
- ✓ 在下载应用软件后最好能够使用手机安全软件对其检测后再进行安装

TREND MICRO 趋势科技

全程护航
迈向云端

谢谢您的观赏