一本带领您重新认识自己手机的安全图书

手机病毒大曝光

王继刚　编著

西安交通大学出版社
XI'AN JIAOTONG UNIVERSITY PRESS

手机病毒大曝光

王继刚　编著

西安交通大学出版社
XI'AN JIAOTONG UNIVERSITY PRESS

图书在版编目(CIP)数据

手机病毒大曝光/王继刚编著. —西安:西安交通大学出版社,2009.10

ISBN 978-7-5605-3220-2

Ⅰ.手… Ⅱ.王… Ⅲ.移动通信-携带电话机-计算机病毒-防治 Ⅳ.TN929.53

中国版本图书馆 CIP 数据核字(2009)第 153749 号

书　　名 手机病毒大曝光
编　　著 王继刚
责任编辑 任振国　李　文

出版发行 西安交通大学出版社
(西安市兴庆南路 10 号　邮政编码 710049)
网　　址 http://www.xjtupress.com
电　　话 (029)82668357　82667874(发行中心)
(029)82668315　82669096(总编办)
传　　真 (029)82668280
印　　刷 陕西新世纪印刷厂

开　　本 727mm×960mm　1/16　**印张** 12　**字数** 212 千字
版次印次 2009 年 10 月第 1 版　2009 年 10 月第 1 次印刷
书　　号 ISBN 978-7-5605-3220-2/TN·116
定　　价 19.00 元

读者购书、书店添货、如发现印装质量问题,请与本社发行中心联系、调换。
订购热线:(029)82665248　(029)82665249
投稿热线:(029)82664954
读者信箱:jdlgy@yahoo.cn

版权所有　侵权必究

前　言

电视里放着一个广告："天翼189，既是上网账号又是E-mail账号……连手机都可以上网了！"相信很多人都看到过这个广告，电信公司推出的这种新式上网方式大大刺激了手机上网市场。与此同时，可视通话业务、手机看电视业务也如火如荼地在中国手机市场上展开。

这一切都仿佛给我们一个信号，手机这个现代人必备的通讯工具已经更加深入地进入到我们的日常生活。

无论是基于传统语音网络的手机，还是现在正在推广使用的3G可视化网络手机，手机在每一个人的口袋中都保存了大量的用户个人信息。

电话簿、短消息都记录了一个手机用户他在做什么，与什么人联系。有时，手机还成为人们进行商业谈判、公司事务汇报等等场合的及时联系工具。那种带有微型摄像头的多功能手机更是具有了让用户随时随地记录更多信息的功能。

可是，当我们在享受这些由科技发展带来的各种方便之时，一些奇怪的、让人心烦的事情也开始发生：每个月本来100元的通讯花费，忽然间变成了300元；手机总是无缘无故地开始死机、重启；总是接到一些陌生的短消息、电话等等。排除了那些质量原因，这些现象让我们一时间不知所措，于是送去让手机的售后服务商来修理，可是维修结果让你大吃一惊："尊敬的用户，您的手机中毒了！"

中毒！手机也能中毒！你一定不相信自己的耳朵，可是当售后人员给你详细解释之后，你终于明白了自己手机上发生的那些莫名其妙的事件原来真的是手机病毒造成的。

对大多数的人来说，手机病毒的概念还没有正式进入人们的认识，但是这些病毒程序却早已经危害到了我们的手机，甚至是我们的生活！

手机病毒不但可以损坏手机本身，还可以被利用成为监视我们行为和谈话内容的间谍工具。可能你不相信这些，但是如果你看过中央电视台播放的关于手机安全的访谈节目，你一定会被里面的内容吓得不敢使用自己的手机，尽管你曾经连睡觉的时候都将手机放在身边！

手机安全问题不再是一个空空而谈的东西，国外在2004年的时候就已经出现了手机病毒，而国内这两年也开始出现各种各样的手机病毒。它们小则破坏手机

正常使用，大则盗窃手机用户资料信息。还记得我们前面提到过的带摄像头的手机吗？如果这种手机被病毒控制，那么你的一切隐私就早已暴露在病毒制造者的眼前了！

正是处于保护广大手机用户使用安全的目的，我才编写了这本书籍。

本书第一次将手机病毒的原理、手机病毒的实现技术揭露出来，带领读者明白手机病毒的可怕与可恶的地方，更加注重教会读者如何防范手机病毒。

这是一次大胆的尝试，更是一次令人激动的学习之旅！

本书的写作思路

本书采用通俗易懂的语言，将手机病毒的来龙去脉描述给每一位读者。

本书也第一次让读者走近手机病毒制造者，去看一看一个手机病毒是怎样编写出来的。

在讲述手机病毒的时候，将其危害性、破坏性一起告诉读者，将病毒的感染运行现象也告诉读者，目的就是为了让读者能够识别出自己的手机在出现问题时是不是被感染了手机病毒。在这些原理技术都清晰明了地告诉读者后，本书又特意指导读者进行自己的手机杀毒工作，做到了有始有终。

本书适合所有热爱通讯安全的人们，尤其是那些曾经被手机病毒折磨过的朋友。

同时，本书可做为通讯安全培训班以及高等院校的教材和参考书籍。

本书也为手机杀毒安全软件开发人员提供了不可多得的安全参考资料，有一定的实际利用价值。

本书的组织方式

本书的组织方式是按照手机病毒的种类进行编排的，全书总共分为 12 章。

第 1 章介绍了什么是手机病毒，手机病毒的特点以及手机病毒的未来发展方向。

第 2 章则为基本理论部分。介绍了手机硬件系统、手机系统的相关知识，以便为后面的手机病毒原理学习做铺垫。

第 3 章至第 9 章开始全面讲解各种类型的手机病毒，以及这些病毒的运行原理和表现特征。

第 10 章教授读者如何及时识别手机是否被病毒感染的相关方法。

第 11 章以图文并茂的方式，带领读者一步一步学习如何利用逆向工程技术来判断一个程序是不是手机病毒程序。

第 12 章向读者提供了可以用来实现手机防毒的各种杀毒软件产品以及性能

此为试读，需要完整PDF请访问：www.ertongbook.com

测试。

本书最后是参考部分，主要列举了书中需要的一些材料信息和来源。

致谢

特别感谢西安交通大学出版社对本书顺利出版所付出的汗水与辛苦。

感谢与我共同研究探讨安全技术的众多朋友。

感谢妻子曲慧文女士对我写作一如既往的支持。

本书由于作者水平有限，书中难免出现错误、不妥之处，恳请广大读者朋友们批评指正。

王继刚

2009年5月22日

目　录

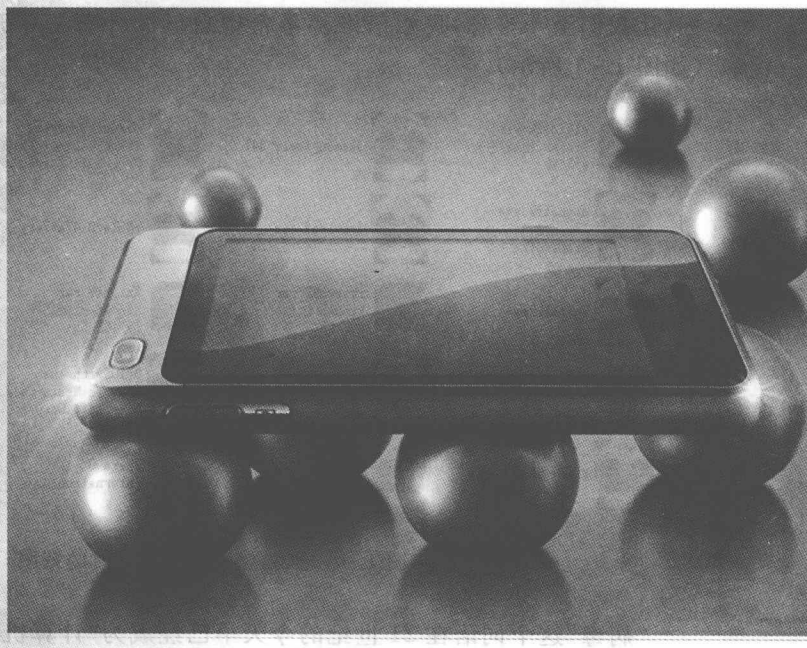
基础篇

认识篇

防范篇

此为试读，需要完整PDF请访问：www.ertongbook.com

基础篇



第1章　走近手机病毒

1.1　手机病毒的出现

如果有人问你，在2007年的时候什么计算机病毒最让你记忆犹新，我想大部分的人都会脱口而出："熊猫烧香"。那个满电视屏幕都是的、拿着三根香的熊猫图标，让我们至今难忘，我相信谁都不希望自己的计算机一开机也会变成那个样子（如图1-1所示）。

图1-1　熊猫烧香病毒发作时的截图

"病毒"这个词语在21世纪的今天早已经成为"计算机病毒"的缩写，这是因为计算机已经成为我们生活中不可缺少的一个组成部分。

现在个人计算机的价格不断下降，更加刺激了人们使用计算机的需求。当我们走进每一所高校、每一个企业、每一栋厂房的时候，我们都可以看见计算机的影子。那么如果有"病毒"这么一个不怀好意的东西感染了这些计算机，后果将是不堪设想的。

具体地讲，"计算机病毒"之所以让人感到可怕是因为它本身带有的破坏性和

感染性，而其中破坏性最为可怕。计算机一旦感染病毒，轻则不能正常运行，重则可能导致计算机使用者的隐秘信息泄露，进而发生商业上的经济损失，甚至会关系到国家、军事的安全。

但是，现在我告诉你有一种东西比“计算机病毒”更为可怕，而且它可能此时此刻就在你的身边，随时伴随着你。在你睡觉的时候，吃饭的时候，工作的时候，都在那里像一双眼睛一样，随时“监视”着你的一举一动，并且它不需要计算机那样明显的电线来工作，它就存在你的周围，随时可以接收指令攻击你，这就是“手机病毒”！

记得自己第一次想到手机病毒的时候是在 2002 年，那时我正在念大学，为了方便联系家人，我决定购买一款手机，最后选定的手机是某制造商生产的 3×8i 型手机，它是当时新出来的一款非常不错的手机，在使用中没有觉得任何不妥的地方。直到有一天，我为了学习需要查阅一些国外的安全文档的时候，无意中看到一篇安全报告中声称该手机制造商生产的手机出现重大安全隐患。这篇报告引起了我的注意，仔细阅读后发现，原来该制造商生产的手机在发送短消息时采用的是 PDU 格式（注：在第 2 章第 4 部分将详细介绍这种特殊的短信格式），而如果利用这种格式创建一个包含特殊字符的短消息，将该短消息发送给该制造商生产的手机时，接收手机就会马上自动关机，同时将无法删除该条特殊短消息，从而造成接收手机瘫痪，拒绝正常服务。

很明显，一个恶意攻击者完全可以利用该安全隐患，编写出大量恶意短消息，然后利用这些短消息来攻击自己想要破坏的目标手机，这种行为完全类似计算机上一个黑客的所作所为。既然这样，如果恶意攻击者编写出一个程序，让这个程序自动完成编写恶意短消息，同时自动完成发送恶意短消息到被攻击手机的动作，此时，这个程序就像计算机病毒一样带有了恶意的破坏性质。

在随后的日子里，我利用 C 语言编写了一个测试程序，用我的手机作为被攻击目标，成功地触发了这个安全隐患。从那一刻我就认为，如果将这个测试程序变成一个能在手机上执行的程序，那么手机病毒就不再是神话了，而是一个真实存在的“恶魔”。

2004 年 6 月，一款中文名叫“卡波尔”，英文名为“Cabir”的手机病毒正式登上了历史舞台。这是一个真正运行在手机上的可以自我复制、传播感染的病毒。

卡波尔病毒运行在 S60（注：即 Symbian 系统，关于这个手机平台的具体内容，将在第 2 章第 6 部分讨论）手机平台上，它通过手机的蓝牙功能进行传播，一旦发现周围存在蓝牙开启的手机就会将自己通过蓝牙复制过去，接着在这部新的手机上再次运行，然后又查找开启蓝牙的手机再复制自己，如此不断循环下去。

所幸的是，卡波尔病毒并没有制造什么破坏性的结果，这是因为其制造者只是想为了能够证明手机系统可以被病毒攻击。但是它的出现却开启了手机病毒的全

面爆发!

在一些关于手机病毒的介绍资料上,常常将2000年的"Timofonica"骚扰短信事件称作第一个手机病毒,其实这是不准确的。如同我在大学中的那个测试程序,2000年一个攻击者编写的计算机程序通过西班牙电信公司的"Telefonica"移动系统向系统内的所有用户发送脏话等等大量骚扰短信,造成用户使用不便,这个程序还是一个在计算机上运行的程序,不能在手机上运行,单独从这一点讲,这个程序就不应该算为手机病毒。而且这个程序造成的影响更加类似于一个手机短信炸弹,而不像病毒那样有自我复制的功能。

自卡波尔病毒出现以后,各式各样的手机病毒逐步开始出现,这些病毒的开发者受到计算机病毒的启发,编写出的手机病毒功能完全模仿计算机病毒,破坏功能急剧加大。关于这些手机病毒的可怕危害,我将在本章的第5部分进行详细的讲解。

1.2 定义手机病毒

在前面,我一直在强调一个概念,就是一个程序要被认定为手机病毒程序,它最起码必须是一个运行在手机上的程序,而不是运行在计算机上的程序。这是手机病毒的一个必要条件,但是这个定义还不完整,为此让我们先来看看"计算机病毒"的一个较为准确的定义。《中华人民共和国计算机信息系统安全保护条例》明确定义,计算机病毒是指"编制或者在计算机程序中插入的破坏计算机功能或者破坏数据、影响计算机使用并且能够自我复制的一组计算机指令或者程序代码"。从中我们看到,定义主要突出了判断一个计算机程序是不是病毒的三个基本标准即:自我复制性、隐蔽性以及破坏性。

一般的计算机程序完全是为了计算机用户的某种正常需要使用来工作的,不会造成任何恶意的破坏行为,甚至程序的开发人员会更加细致开发程序,从而避免造成用户的使用不便。而对于病毒来说,它就像让我们得病的感冒病毒一样,被感染的计算机会出现系统反应缓慢、丢失数据,甚至会主动向外泄密。而被感染的计算机又成为一个新的病毒源,它会进而去感染其他的计算机。

手机程序也是如此。普通的手机程序完全是为手机使用用户服务,例如手机使用者可以利用该手机程序来备份短消息,或者来播放歌曲、视频文件。然而当一个手机程序在运行后,它首先利用手机系统的某种特性或者漏洞使得自己自动运行,接着开始复制自己到该手机的某个位置或者其他手机的某个位置上时,这个手机程序就具有了手机病毒的初期性质。

之所以称这种自我复制的特性为手机病毒的初期性质,是因为对于任何一种

病毒程序来讲，它最原始的特性就类似于生物病毒一样，具有自我传播感染性。

接着当这个初期的手机病毒程序开始对手机系统或者手机使用者个人信息资料，如短消息等等内容进行破坏时，这个手机程序就在理论上真正成为了手机病毒。

1.3　手机病毒的运行原理

很多人都十分惊奇，为什么手机上也会感染病毒？其实，对于手机来讲，手机硬件平台就完全等效于一个小型的个人计算机，它有处理器、存储器等部件，而手机系统就是一个类似于 Windows 计算机操作系统一样的控制系统程序，只不过它有一个特殊的名字叫做“嵌入式操作系统”（嵌入式操作系统的具体概念我们放在第 2 章的第 1 部分进行讲解，这里我们可以暂时理解它为一个缩小版本的计算机操作系统）。

一般来讲，我们平时使用的手机所带的系统都是完全固化的。也就是说，我们不能随意在这种手机上安装软件。这些手机系统在固化到手机上之前，将手机用户基本所需的功能都已经实现，如语音通话、拨打电话、接听电话、发送短消息，等等。这些基本功能是手机系统必须实现的。

我们拿大家熟知的 Windows 操作系统来作一个比较。当我们在个人计算机上安装完 Windows 操作系统后，就可以通过这个系统的图形界面或者控制命令来使用计算机内部的任意一个硬件设备。可以通过系统提供软件来播放音乐，而系统则控制声卡硬件设备发出声音。Windows 操作系统最基本的功能就是将计算机中的硬件设备全部变得可用起来，同时为用户提供一个简单易操作的交互界面。前面讲到的固化手机系统也就是这样的。

与此同时，很多手机用户可能对手机有着额外的需求。例如一位十分喜欢看电影的人，他在选择一部手机的时候，他就期待这部手机能够具有播放电影的功能，这样他就可以随时随地享受影视节目。用户的这种特殊需要决定了手机制造厂商需要在手机系统中加入满足这些特殊需要的功能实现部分。这一部分程序的实现完全可以也直接固化进入手机系统，成为手机系统的一个部分。就如同 Windows 系统自带了用来播放视频的软件 Windows Media Player 一样。

但是手机制造厂商发现，随着越来越多的手机用户使用量，手机使用者对于手机功能的需求越来越复杂，如果完全要将这些用户的需求同时装进一个手机系统，显然那将使手机系统变得十分庞大繁琐，不稳定，容易引发问题。同时，手机系统的开发者不可能为了某一个用户的需要来单独制造一个手机系统，而为了满足另

外一个用户的需要又单独制造一个手机系统，这样手机系统的成本将变得十分昂贵，不利于手机市场的销量。于是，手机系统的设计者开始允许手机自身带有一定的软件安装功能。也就是说，一个手机系统可能支持某种类型的安装程序文件，允许手机用户将符合自己需要的安装程序文件直接运行在手机上。这样一来，手机的系统还是提供那些原始基本的功能，而这些来自系统外部的软件将服务于用户的额外需求。我们平时听到的某某手机支持 Java 功能，其作用就是这个意思。这类手机就允许用户在手机上安装 Java 编写的手机程序，这些程序可以是提供某种功能的软件，也可以是某个经典的游戏等等。

当手机系统开始支持用户安装软件的时候，就引入了一个不安全的因素。因为手机本身无法得知用户安装的这个手机软件是不是一个“安全”的软件。虽然说用户自己不可能主动安装一个不安全的软件在自己的手机上，但是伪装了的一些恶意软件却可以轻易骗过用户的信任，从而被用户安装在手机上，一旦这些程序成功运行起来，破坏结果就随之而来了。

如果说扩展功能支持是手机的一个质的升级，那么智能手机则是更加接近于我们平时使用的个人计算机系统。关于智能手机的具体含义我们将在第 2 章中进行讨论，这里我们只需要知道一点，智能手机的系统完全类似于 Windows 操作系统，这样你就可以想象为什么手机上会出现与计算机一样的病毒程序了。

手机病毒一般采用高级语言编写，例如我们熟知的 Java 语言。高级语言的好处在于编程的时候会比较简单，减小了开发难度。但是底层语言，如汇编语言同样可以开发手机病毒程序，甚至编写出来的程序会更加具有破坏性质，更加隐蔽。

手机病毒在采用高级语言开发的同时，必须紧密与手机系统开发平台结合。就像我们平时在编写 Windows 下的程序一样，如果我们使用 VC++6.0（VC++6.0 是微软公司开发的一个集成开发环境）来编写出一个程序，那么它只可能运行在 Windows 下面而不会运行在 Linux 这样的操作系统上，因为我们选择的开发语言只适用于 Windows 操作系统。为此，我们常常需要使用手机系统开发者提供的开发环境（这里的开发环境包括编程开发工具，编程开发语言，编程开发所需的文件库等等）来进行相应手机系统下的病毒开发。在本书的第 6 章里，我将会较为详细地演示一个手机病毒的基本开发过程来帮助大家理解手机病毒的编程过程。

但是，并不是说一个恶意编程人员没有办法开发出具有通用性质的手机病毒。Java 手机病毒就是这样一种可以运行在多种手机系统上的手机病毒，因为一般的手机系统都支持 Java 环境，所以一个由 Java 程序编写出来的手机病毒就可以感染并运行在很多类型的手机上，如诺基亚、索尼爱立信、三星等。

手机病毒具有其独特的地方。由于手机平台的特殊设计，手机病毒一般只能

此为试读，需要完整PDF请访问：www.ertongbook.com