

<<手机病毒大曝光>>

图书基本信息

书名：<<手机病毒大曝光>>

13位ISBN编号：9787560532202

10位ISBN编号：7560532209

出版时间：1970-1

出版时间：西安交大

作者：王继刚

页数：178

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<手机病毒大曝光>>

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！”

<<手机病毒大曝光>>

内容概要

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。

<<手机病毒大曝光>>

书籍目录

基础篇第1章 走近手机病毒1.1 手机病毒的出现1.2 定义手机病毒1.3 手机病毒的运行原理1.4 手机病毒的特点1.4.1 体积小、功能专一1.4.2 多种传播方式1.4.3 基于无线网络的灵活性1.5 手机中毒的一般表现1.5.1 系统反应缓慢1.5.2 莫名的短信或者彩信消息1.5.3 自动联网1.5.4 通话质量下降或者延迟1.5.5 耗电量增加1.6 手机病毒的危害1.6.1 直接性破坏1.6.2 剧增的话费1.6.3 窃密与监听1.6.4 欺骗与敲诈1.7 手机病毒大事记1.8 手机病毒的发展趋势1.8.1 多样化1.8.2 隐蔽化1.8.3 底层化1.8.4 顽固化1.8.5 反杀毒化第2章 手机结构的基本知识2.1 嵌入式系统与嵌入式操作系统的概念2.2 智能与非智能手机2.3 ROM与RAM2.4 SMS与MMS2.5 红外与蓝牙2.6 CMNET与CMWAP2.7 智能手机系统2.7.1 Symbian2.7.2 Windows Mobile2.7.3 Linux2.7.4 线程与任务认识篇第3章 手机缺陷与病毒攻击3.1 手机系统性缺陷的概念3.2 实例分析：短消息死锁漏洞3.2.1 漏洞细节分析3.2.2 漏洞利用过程3.2.3 防范该漏洞攻击的方法3.3 手机功能性缺陷的概念第4章 可怕的手机木马4.1 “木马”的来源4.2 木马病毒的危害性4.2.1 远程窃密4.2.2 通话监听4.2.3 信息截获4.2.4 伪造欺骗4.3 手机木马实现原理4.3.1 自启动式的激活方式4.3.2 自身隐藏技术4.3.3 后台运行的实现4.3.4 控制命令的接收4.3.5 命令执行过程4.3.6 结果回馈4.4 实例分析：多种手机木马病毒的识别与清除4.4.1 flocker手机木马病毒4.4.2 Pbbstealer手机木马病毒4.4.3 Commwarrior手机木马病毒4.4.4 Cardtrap手机木马病毒4.4.5 RommWar手机木马病毒4.4.6 Doomboot.A手机木马病毒4.5 手机木马的基本识别手段第5章 随网蔓延的蠕虫病毒5.1 什么是蠕虫病毒5.2 手机蠕虫病毒的出现背景5.2.1 蓝牙技术的不可靠性5.2.2 蠕虫病毒传播5.3 第一个手机蠕虫病毒——“卡波尔”5.3.1 病毒的发作现象5.3.2 病毒的处理方法5.4 Mibir蠕虫病毒简介5.5 Skulls系列病毒简介5.6 实例分析：手机蠕虫病毒的基本原理5.6.1 背景介绍5.6.2 编写蠕虫的工具及使用5.6.3 Symbian应用程序初始化过程5.6.4 源代码讲解5.6.5 病毒清除的基本方法第6章 危险的刷机与手机升级6.1 刷机的概念6.2 刷机带来的隐患6.3 手机系统升级的概念6.4 升级出来的隐患6.5 实例分析：手机刷机实验6.5.1 实验工具6.5.2 实验过程第7章 绵里藏针的捆绑型手机病毒7.1 什么是文件捆绑7.2 SIS格式的初步认识7.3 拆解SIS文件7.4 SIS捆绑病毒的基本实现7.5 捆绑型病毒的特点及危害7.6 捆绑型病毒的识别与防范第8章 手机流氓软件的出现8.1 流氓软件背景介绍8.2 流氓软件分类及其恶意行径8.3 流氓软件的危害8.4 实例分析：一个典型的流氓软件分析8.4.1 流氓软件感染过程8.4.2 流氓软件清除方法第9章 手机上的Rootkit9.1 Rootkit技术9.2 文件隐藏9.3 任务/线程隐藏9.4 驱动层次的Rootkit9.5 躲藏在硬件中的恶魔9.6 手机Rootkit未来发展趋势分析防范篇第10章 发现手机病毒的方法10.1 手机自启动方式检查10.2 手机文件系统检查10.3 手机运行任务检查10.4 手机联网检查10.5 手机功能检查第11章 手机病毒的逆向分析11.1 逆向工程技术简介11.2 ARM汇编语言11.2.1 ARM公司与ARM式嵌入式系统11.2.2 ARM编程模型11.2.3 ARM体系结构的存储器格式11.2.4 ARM状态下的寄存器使用11.2.5 ARM指令体系与寻址方式11.3 IDA Pro11.4 对卡波尔病毒的逆向分析第12章 主流手机反病毒软件介绍12.1 F-Secure12.2 卡巴斯基杀毒软件12.3 Symantec手机杀毒软件12.4 麦咖啡手机杀毒12.5 小红伞AntiVirMobile12.6 BitDefender Mobile Security12.7 网秦手机杀毒软件12.8 瑞星杀毒软件12.9 金山毒霸手机版12.10 江民杀毒软件12.11 光华手机杀毒软件12.12 手机杀毒软件的弊端

<<手机病毒大曝光>>

章节摘录

插图：以往我们买的一部手机，其固有的手机存储空间一般可以用兆字节来计算。

虽然使用兆字节来计算，但是往往也是在几兆字节空间左右。

这些存储空间最主要的用途是用来存放用户手机上的电话号码簿以及短消息之类的关键信息。

有时候，手机的制造商也会在手机的这些空间中存放一些图片或者小的音乐文件，其作用是为了让用户可以美化自己手机的背景桌面、个性化自己的手机来电铃声等等。

当这些基本的文件占据到手机的存储空间上时，几兆字节的大小就所剩无几了。

手机自身也会带上一两个小的游戏文件，用来丰富手机的使用功能。

这样的话，手机制造商给手机用户留下的可用空间就屈指可数了。

所以，如果用户想要在手机上安装某个程序，那么这个程序的文件所占存储空间就一定要小，也就是我们常说的文件要尽量小。

不然程序文件将无法存储到手机上，更不要谈论什么运行了。

但是，你一定会说，现在很多手机都支持扩展内存，也就是说手机可以单独配上一张存储卡，这些存储卡小的几百兆字节，大的可以上吉字节，不要说程序，就是电影、音乐文件都敢往手机上存储。

你说的不错，大存储空间手机早已经成为现代手机市场的主流。

其目的就是为了能够让用户拥有更加多的选择机会来丰富手机的娱乐特性。

可是，从手机病毒这个角度来讲，如果我们设想一个手机病毒程序的文件大小是几十兆字节，那么当用手机启动这个程序的时候，手机势必会显的反应迟缓，甚至会长时间死机。

这就如同我们在计算机上运行一个大型程序一样，硬件的支持总有一定的范围，超出这个范围就会出现一些毛病。

手机病毒为了能够隐蔽地执行，怎么可能选择让自己运行的如此明显，这不是显然在告诉用户，你的手机不正常了吗？

还有，手机病毒为了隐蔽自己，也往往会将自己伪装在其他文件中，如果自己的本身文件就过大，那么再加上伪装文件，最终的文件大小就会显得过于庞大，与其他的手机程序大小相差悬殊。

对于一般的手机程序来说，它的大小也往往在一个兆字节以下，一般是十几千字节到几百千字节不等。

为此，手机病毒的制造者也会考虑这个情况从而降低病毒文件的体积大小。

<<手机病毒大曝光>>

编辑推荐

《手机病毒大曝光》：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>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>