课程名称：计算机病毒分析及治理防范实践

课程目标：

本课程全面地介绍了各种病毒的原理，以操作系统的发展为主线，结合病毒的发展过程来综合分析病毒。在分析工具上，较多地利用了脚本语言、C++和汇编语言，注重理论与实践相结合，每介绍一种类型的病毒，均以实例阐述。

在深入分析和全面阐述之后，本课程将向学员揭示，病毒只不过是利用了系统或应用软件提供的某些功能，利用漏洞来进行破坏的一段代码而已。基于此，病毒并不可怕，病毒是可以清除的，同时和病毒的斗争也将是长期的。

适用学员：从事集团客户维护人员、客户端销售、VIP 营销的社区经理、客户经理、宽带后台支撑（市场、后台、增值服务等线条）。

课程设计：

授课课时:	2 天
授课条件：	学员必须具有基本的通信技术基础知识
内容摘要：	**一、计算机病毒概述** ◇ 计算机病毒的产生与历史 ◇ 病毒产生的原因 ◇ 病毒的发展过程 ◇ 病毒的发展趋势 **二、引导型病毒分析** ◇ 引导型病毒 ◇ 系统引导过程与扇区分析 ◇ 实验 1：引导程序设计 ◇ 实验 2：接管中断程序设计 ◇ 清除病毒程序设计原理 **三、PE 文件病毒** ◇ PE 文件结构 ◇ PE 病毒常用技术 ◇ 添加节方式修改 PE

◇ 加长最后一节修改 PE

◇ 插入节方式修改 PE

四、网络蠕虫病毒

◇ 网络蠕虫综述

◇ 案例：利用 Unicode 漏洞

◇ 蠕虫与溢出

◇ 防范网络蠕虫病毒

五、木马病毒

◇ 木马技术揭露

◇ 木马程序的安装

◇ 木马的隐藏技术分析

◇ 木马清除方法

授课语言：	中文