第一章 恶意代码概述

恶意代码的特征：

目的性，传播性，破坏性

恶意代码的种类：

1. 普通计算机病毒
2. 蠕虫
3. 特洛伊木马

   一个完整的木马系统由硬件部分，软件部分，连接部分组成
4. Rookit 工具

   一个典型的 Rootkit 包括以下内容：

   网络嗅探程序，特洛伊木马程序，隐藏攻击者的目录和进程的程序，日志清理工具
5. 流氓软件
6. 间谍软件
7. 恶意广告
8. 逻辑炸弹
9. 后门
10. 僵尸网络
11. 网络钓鱼
12. 恶意脚本
13. 垃圾信息
14. 勒索软件
15. 移动终端恶意代码

恶意代码传播途径：

软盘，光盘，硬盘，Internet，无线通信系统

恶意代码命名规则：

平台名.家族名.组名.变种号

恶意代码最新趋势：

1. 网络化
2. 专业化
3. 简单化
4. 多样化
5. 自动化
6. 犯罪化

第二章 恶意代码模型及机制

计算机模型：

随机访问计算机模型（Random Access Machine，RAM）:2/14/1946,ENIAC，这种模型无法感染病毒

随机访问存储程序模型（Random Access Stored Program Machine，RASPM）：具有 RAM 的所有特性，程序可以自我修改，不需要间接寻址

带后台存储的 RASPM 模型(Random Access with Attached Background Storage,RASPM_ABS)：带后台存储（外存）

Internet 蠕虫传播模型：

SIS、SI、SIR 模型是传染病传播模型中常用的三种模型。其中，S 表示易感者，I 表示感染者，R 表示移除者。具体解释如下：
SIS 模型：SIS 模型是一种简单的传染病模型，其中易感者可以被感染，感染者可以恢复并重新变为易感者。该模型假设人口总数不变，即不考虑人口迁移、出生和死亡等因素
SI 模型：SI 模型是一种比较早期的传染病模型，其中易感者可以被感染，感染者不会恢复并变为易感者。该模型同样假设人口总数不变
SIR 模型：SIR 模型是传染病模型中最经典的模型，其中易感者可以被感染，感染者可以恢复并变为移除者，移除者不会再次感染。该模型同样假设人口总数不变

恶意代码预防理论模型：

Fred Cohen”四模型”理论：
基本隔离模型
分隔模型
流模型
限制解释模型

传统计算机病毒结构和机制：

运行顺序：重定位->获取 API->感染文件->返回宿主程序
计算机病毒主要模块：
1. 引导模块（驻留在内存中，窃取系统控制权，恢复系统功能）
2. 感染模块
3. 破坏模块
4. 触发模块

引导型病毒：

引导型病毒首先感染软盘的引导区，然后蔓延至硬盘并感染硬盘的主引导记录（Main Boot Record，MBR）。一旦 MBR 被病毒感染，病毒就试图感染软驱中的软盘引导区。病毒隐藏在软盘的第一扇区，使它可以在系统文件装入内存之前先进入内存，从而活得对操作系统的完全控制。

第三章 传统计算机病毒

16 位可执行文件病毒：

COM 格式（最大 64KB，内含 16 位程序的二进制代码绝对映像，无重定位信息，不需要重定位）
MZ 格式（COM 发展而来，内含 16 位代码，具有文件头，文件头中包含文件入口点、堆栈位置、重定位表等，需要重定位）
NE 格式（Win3.X 时加入，保留 MZ 的头，加入 NE 的头，包括 EXE、DLL、DRV、FON 等，实现运行时动态链接）

32 位可执行文件病毒：

PE 格式（Portable Executable，可移植的执行体，重定位->获取 API->感染文件->返回宿主程序）

宏病毒：

只感染文档文件，包括：
Microsoft: Word,Excel,Access,Powerpoint,Project,Visio,
Inprise: Lotus Amipro
其他：AutoCAD，CorelDRAW，PDF
Word 宏病毒：

通过 DOC 文档和 DOT 模板自我复制和传播
宏病毒特点：
1. 传播极快
2. 制作方便，变种多
3. 破坏可能性极大
4. 多平台交叉感染
5. 地域性问题
6. 版本问题
典型宏病毒：
梅丽莎（Melissa）
台湾 NO.1B
097M.Tristate.C
ILOVEYOU
Macro.Word97.Thus
Macro.Word97.Marker
Nuclear

第四章 Linux 恶意代码技术

第一个 Linux 恶意代码：Bliss（上天的赐福，1997 年 2 月）
第一个跨 Windows 和 Linux 平台的病毒：W32.Winux（又名 W32.Lindoes 或 W32.PEElf.2132）
Linux 系统恶意代码分类：
1. Shell 恶意脚本
2. 蠕虫
3. 基于欺骗库函数恶意代码
4. 与平台兼容恶意代码
Shell 恶意脚本：
以下是一个简单的 shell 恶意脚本

```
for file in ./infect/*       //遍历文件
do
cp $0 $file                  //自我复制
done
```

ELF 文件格式：
可执行链接格式（Executable and Linkable Format，ELF）是 UNIX 系统实验室作为应用程序二进制接口而研发的。
ELF 格式文件感染原理：
1. 无关 ELF 格式的感染方法
（1）覆盖式感染
有些病毒会强行覆盖执行程序的某一部分，将自身代码嵌入其中，以达到不改变被感染文件长度的目的，被这样的病毒覆盖的代码无法复原，从而这种病毒是无法安全杀除的。病毒破坏了文件的某些内容，在杀除这种病毒后无法恢复文件的原貌。
（2）追加式感染
同覆盖式感染方式不同的是，将病毒体直接追加到宿主文件中，或将宿主追加到病毒体之后，并不覆盖宿主文件，在病毒文件执行后将控制权交还给宿主文件。
2. 利用 ELF 格式的感染方法

（1）文本段之后填充
（2）数据段之后插入感染
（3）文本段之前插入感染
（4）利用函数对齐填充区感染
（5）利用 NOTE 段或者扩展.note 节
3. 高级感染技术
（1）LKM 感染技术
LKM 技术是 Linux 内核模块技术（Loadable Kernel Module），是一种可以在运行时动态地向 Linux 内核中插入或删除代码的技术。通过 LKM 技术，可以在不重新编译内核的情况下，向内核中添加新的功能或者删除某些功能，从而实现对 Linux 系统的动态修改。LKM 技术可以用于驱动程序的开发、系统调试、安全防护等方面。由于 LKM 技术具有动态修改内核的能力，也可能被黑客用于开发恶意软件，如 Rootkit 等。
（2）PLT/GOT 劫持实现
PLT/GOT 劫持实现技术用于修改程序的全局偏移表（GOT）和过程链接表（PLT），从而实现对程序的控制权劫持。在程序运行时，PLT/GOT 劫持实现技术常用于二进制漏洞利用、提权攻击、恶意代码注入等方面，是黑客攻击中的一种常见技术。

第五章 特洛伊木马（木马概述）

特洛伊木马得名于荷马史诗《伊利亚特》中的战争手段，信息安全中特洛伊木马是一种与远程计算机之间建立起连接,使远程计算机能够通过网络控制用户计算机系统并且可能造成用户的信息损失、系统损坏甚至瘫痪的程序。

木马的组成：

1. 硬件部分
（1）控制端
（2）服务端
（3）Internet
2. 软件部分
（1）控制端程序
（2）木马程序
（3）木马配置程序
3. 连接部分
（1）控制端 IP 和服务端 IP
（2）控制端端口和木马端口

经典木马：

Back Orifice(BO)、Netspy、Picture、Netbus、Asylum、冰河、灰鸽子、网络神偷

木马的特点：

1. 欺骗性
2. 隐蔽性
3. 自动运行性
4. 自动恢复功能
5. 功能的特殊性

木马的分类：

1. 远程控制型木马
2. 发送密码型木马

3. 键盘记录型木马
4. 毁坏型木马
5. FTP 型木马

远程控制软件和木马的异同点：

远程控制软件和木马都是用于远程控制计算机的工具，但它们之间存在一些异同点。共同点包括：都可以通过网络远程控制计算机，都可以在计算机上执行恶意操作，如窃取敏感信息、植入后门等。不同点包括：远程控制软件通常是合法的，可以通过正常安装获取，而木马通常是通过潜在漏洞或者社会工程学手段进行传播；远程控制软件通常具有明确的功能和用途，而木马则通常是隐蔽的，具有多种恶意功能；远程控制软件通常有明确的使用者和被使用者，而木马则可以被任何人使用。

木马的技术发展：

1. 跨平台性
2. 模块化设计
3. 更新更强的感染模式
4. 即时通知
5. 更强更多的功能

第五章 特洛伊木马（木马程序的关键技术）

植入技术：

1. 常用植入手段
（1）邮件植入
（2）IM 传播
（3）下载传播
（4）漏洞植入
（5）网上邻居植入
（6）网页植入
2. 首次运行
（1）冒充为图像文件
（2）程序捆绑欺骗
（3）以 Z-file 伪装加密程序
（4）伪装成应用程序扩展组件
3. 网站挂马技术
（1）框架挂马
（2）Js 挂马
（3）图片伪装挂马
（4）网站钓鱼挂马
（5）伪装挂马

自启动技术：

1. 修改批处理
（1）Autoexec.bat（引导系统时执行）
（2）Winstart.bat（启动图形界面时执行）
（3）Dosstart.bat（进入 MS-DOS 时执行）
2. 修改系统配置
（1）System.ini

（2）Win,ini
3. 借助自动播放功能
4. 通过注册表中的 Run 来启动
5. 通过文件关联启动
6. 通过 API HOOK 启动
7. 通过 VxD 启动
8. 通过浏览网页启动
9. 利用 Java Applet
10. 利用系统自动运行的程序
11. 其他方法

隐藏技术：

1. 反弹式木马技术（网络神偷）
2. 用 ICMP 方法隐藏连接
3. 隐藏端口
4. Windows NT 系统下木马进程的隐藏
5. 远程线程技术

第六章 移动智能终端恶意代码

常见智能手机操作系统：

Android、IOS、Windows Phone、Symbian、Linux、WebOS、黑莓系统

手机操作系统的弱点：

1. 不支持任意的访问控制（不能区别不同用户的个人隐私数据）
2. 不具备审计能力
3. 缺少通过身份标识符或者身份认证进行重用控制的能力
4. 不对数据完整性进行保护
5. 即使部分系统有密码保护，恶意用户仍然可以使用调试模式轻易得到他人的密码，或者使用类似 PalmCtypt 这样的简单工具得到密码
6. 密码锁定情况下，移动终端操作系统仍然允许安装新的应用程序

移动终端恶意代码关键技术：

1. 移动终端恶意代码传播途径
（1）终端-终端
（2）终端-网关-终端
（3）PC-终端
2. 移动终端恶意代码攻击方式
（1）短信攻击
（2）直接攻击手机
（3）攻击网关
（4）攻击漏洞
（5）木马型恶意代码
3. 移动终端恶意代码的生存环境
（1）系统相对封闭
（2）创作空间狭窄
（3）数据格式单调
4. 移动终端设备的漏洞

（1）PDU 格式漏洞
（2）特殊字符漏洞
（3）vCard 漏洞
（4）Siemens 的“%String”漏洞
（5）Android 浏览器漏洞

经典移动终端恶意代码：

Cabir、CopyCat、Judy、X 卧底系列木马、白卡吸费魔木马、VBS.Timofonica、吞钱贪婪鬼、Skulls、Lasco

移动终端恶意代码的防范：

1. 注意来电信息
2. 谨慎网络下载
3. 不接收怪异短信
4. 关闭无线连接
5. 关注安全信息

第七章 蠕虫

蠕虫的分类：

1. 面向企业用户和局域网

红色代码、尼姆达、SQL 蠕虫王

2. 针对个人用户和网络

爱虫、求职信

蠕虫和传统病毒的区别：

存在形式：蠕虫（独立程序），传统病毒（寄存文件）
传染机制：蠕虫（主动攻击），传统病毒（宿主程序运行）
传染对象：蠕虫（计算机），传统病毒（本地文件）

蠕虫病毒的组成：

传播模块：负责寻找下一个满足感染条件的目标计算机，并将自身复制到目标计算机上，以实现蠕虫病毒的传播。
感染模块：负责感染目标计算机，并将自身复制到目标计算机上，以实现蠕虫病毒的传播。
控制模块：负责控制已感染的计算机，以实现蠕虫病毒的远程控制和操作。
负载模块：负责执行蠕虫病毒的恶意功能，如窃取敏感信息、植入后门等。

震网蠕虫的特点：

1. 攻击目标明确
2. 采用技术先进

蠕虫的特征：

1. 利用漏洞主动进行攻击
2. 与黑客技术相结合
3. 传染方式多
4. 传播速度快
5. 清除难度大
6. 破坏性强

经典蠕虫：

莫里斯蠕虫、红色代码、尼姆达、冲击波、震荡波、震网、求职信、情书、爱虫

第八章 勒索型恶意代码

勒索型恶意代码是一种以勒索为目的的恶意软件,是黑客使用技术手段劫持用户设备或数据资产，并以此为条件向用户勒索钱财的一种恶意攻击手段
勒索软件有两种形式，分别是数据加密和限制访问

典型勒索恶意代码：

WannaCry、Hidden-Tear

WannaCry：

1. 蠕虫模块
2. 漏洞利用模块（永恒之蓝漏洞，445+139 端口，SMB 服务）
3. 勒索模块

防范及应对策略：

1. 增强安全意识
2. 备份重要文件
3. 网络流量的检测
4. 网络隔离措施
5. 更新软件和安装补丁

应急策略：隔离感染主机，切断传播途径，查找攻击源，查杀病毒修复漏洞

第九章 流氓软件、邮件型恶意代码、WebPage 恶意代码、僵尸网络、Rootkit、APT

流氓软件特征：

1. 强迫性安装
2. 无法卸载或卸载困难
3. 干扰正常使用
4. 具有恶意代码和黑客特征

利用 Outlook 漏洞的恶意代码（邮件型恶意代码）的传播方式：

1. 附件方式
2. 邮件本身
3. 嵌入方式

WebPage 中的恶意代码：

1. 基于 JavaScript 的恶意脚本
2. 基于 VBScript 的恶意脚本
3. 基于 PHP 的恶意脚本
4. Shell 恶意脚本

典型 WebPage 恶意代码（万花谷）

僵尸网络（botnet）的特点：

1. 分布性
2. 恶意传播
3. 一对多控制

僵尸网络的工作过程一般包括传播、加入、控制三个阶段

僵尸网络传播手段：

即时通讯软件、邮件型恶意代码、主动攻击漏洞、恶意网站脚本、特洛伊木马

僵尸网络的危害：

1. DDoS

2. 发送垃圾邮件
3. 窃取秘密
4. 滥用资源

Rootkit 的概念：

Rootkit 是一种特殊的恶意软件，它的功能是在安装目标上隐藏自身及指定的文件、进程和网络链接等信息，使得攻击者可以在目标计算机上秘密地窥探敏感信息、植入后门等。Rootkit 的特点是具有隐蔽性、持久性和高级功能。它可以隐藏自己的存在，使得常规的杀毒软件和系统工具无法检测到它的存在;它可以在系统启动时自动运行,保证自身的持久性;它可以具有高级的功能，如修改系统内核、篡改系统日志、绕过安全防护等。Rootkit 一般都和木马、后门等其他恶意程序结合使用，以达到更加隐蔽和有效的攻击效果。

Rootkit 的组成：

1. 网络嗅探程序
2. 特洛伊木马程序
3. 隐藏攻击者的目录和进程的程序
4. 日志清理工具
5. FIX 程序　　...以及其他工具

高级持续性威胁（Advanced Persistent Threat，APT）：

APT 的攻击过程：

第一阶段 定向信息收集
第二阶段 单点攻击突破
第三阶段 构建通道
第四阶段 横向渗透
第五阶段 目标行动

APT 的特征：

1. 高级性
（1）高级的收集手段
（2）威胁高级的数据
（3）高级的攻击手法
2. 持续性
（1）持续潜伏
（2）持续攻击
（3）持续欺骗
（4）持续控制

第十章 恶意代码防范技术

恶意代码检测技术：

1. 特征码扫描技术
2. 启发式扫描技术
3. 完整性分析技术
4. 基于语义的检测技术
5. 行为监控分析技术
6. 代码仿真分析技术

恶意代码检测方法：

1. 手工检测

2. 自动检测

自动检测程序核心部件：

1. 特征码

特征码不应含有恶意代码的数据区，数据区是经常变化的。

特征码足以将恶意代码区别于其他恶意代码和该恶意代码的其他变种。

在保持唯一性的前提下，应尽量使特征码长度短些，以减少时间和空间开销。

特征码必须能将恶意代码与正常程序区分开。

2. 扫描引擎

数据备份与数据恢复：

存储备份技术：

1. 完全备份

对整个系统或用户指定的所有文件进行全面的备份。

2. 增量备份

只备份上一次备份操作以来新创建或更新的数据。

3. 差分备份

备份上一次完全备份后产生和更新的所有数据。

第十一章 常用杀毒软件和解决方案

杀毒软件选择参考：

1. 查杀能力
2. 防范新恶意代码的能力
3. 备份和恢复能力
4. 实时监控能力
5. 升级能力
6. 智能安装能力
7. 简单易用
8. 资源占用情况
9. 兼容性
10. 价格
11. 厂商的实力

恶意代码防范产品的地缘性：编制者的生活空间、特定操作系统及软件环境、定向性攻击和条件传播

第十二章 恶意代码防治策略

恶意代码防治策略的基本准则：

1. 拒绝访问能力
2. 检测能力
3. 控制传播的能力
4. 清除能力
5. 恢复能力
6. 替代操作

国家层面防治策略：

1. 完善相关法律法规及其贯彻落实工作
2. 在各主干网络建立恶意代码预警系统

3. 建立多层次恶意代码应急体系
4. 建立动态的系统风险评估措施
5. 建立恶意代码事故分析制度
6. 制定完备的备份和恢复计划
7. 提高国内运营商自身的安全性
8. 加强信息安全培训
9. 加强技术防范措施

单机用户防治策略：

1. 新购置的计算机第一时间进行系统升级，保证修补所有已知安全漏洞
2. 使用高强度口令
3. 及时安装系统补丁
4. 重要数据应当留有备份
5. 选择并安装经过权威机构认证的安全防范软件
6. 使用网络防火墙
7. 当不需要网络时就不要接入互联网，或断开网络连接
8. 设置杀毒软件的邮件自动杀毒功能
9. 正确配置恶意代码防治产品，发挥产品的技术特点
10. 充分利用系统提供的安全机制，正确配置系统，减少恶意代码入侵事件
11. 定期检查敏感文件，保证及时发现已感染的恶意代码和黑客程序

杂项：

《中华人民共和国网络安全法律》施行时间 6/1/2017。

《刑法》第 286 条规定：故意制作、传播计算机病毒后果严重的，处五年以下有期徒刑或拘役，后果特别严重的，处五年以上有期徒刑。

上世纪 90 年代末，中国公安部推出我国最早的杀毒软件 Kill 6.0。

参考文献

《计算机病毒与恶意代码-原理、技术及防范》（第四版） 刘攻申