12 网络蠕虫

周威

weizhou_sec@hust.edu.cn

本讲提纲

- 12.1 网络蠕虫的定义
- 12.2 网络蠕虫的分类
- 12.3 网络蠕虫的功能结构与关键技术
- 12.4 网络蠕虫的检测与防治

12.1 网络蠕虫的定义

- 蠕虫这个生物学名词在1982年由Xerox PARC（Xerox Palo Alto Research Center） 的John F. Shoch等人最早引入计算机领域，并给出了计算机蠕虫的两个最基本特征：
  - “可以从一台计算机移动到另一台计算机”
  - “可以自我复制”
- 蠕虫最初目的：分布式计算的模型试验
  - 利用网络主机的空闲资源
  - 破坏性和不可控性

第一个进入互联网的蠕虫－莫里斯蠕虫

- 1988年11月2日，导致大约6000台机器瘫痪［当时互联网主机的1/10］
- 利用的漏洞类型
  - Rsh/rexec：用户的缺省认证
  - Sendmail 的debug模式
  - Finger的缓冲区溢出
- 惩罚：
  - 3年缓刑、400小时社区服务及10,000美元罚金

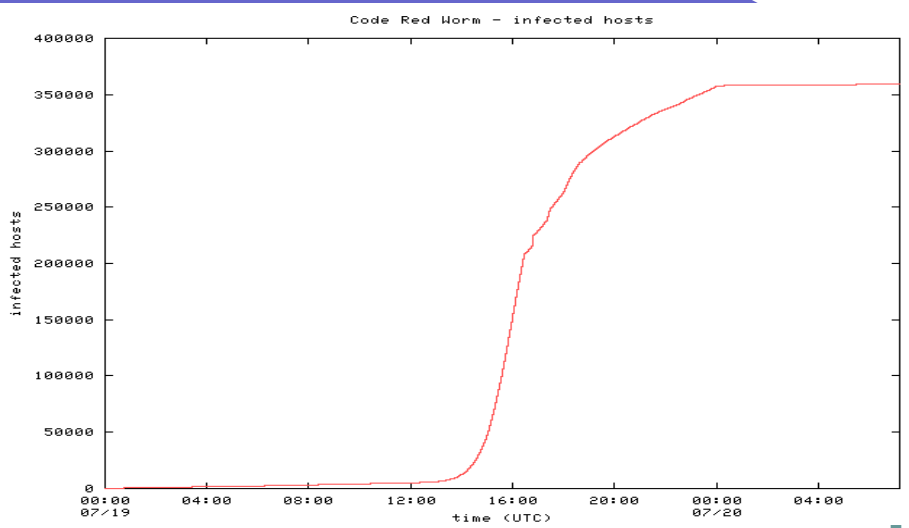
Robert Tappan Morris
当时为美国康奈尔大学大一研究生，
前国家安全局科学家罗伯特.莫里斯之子

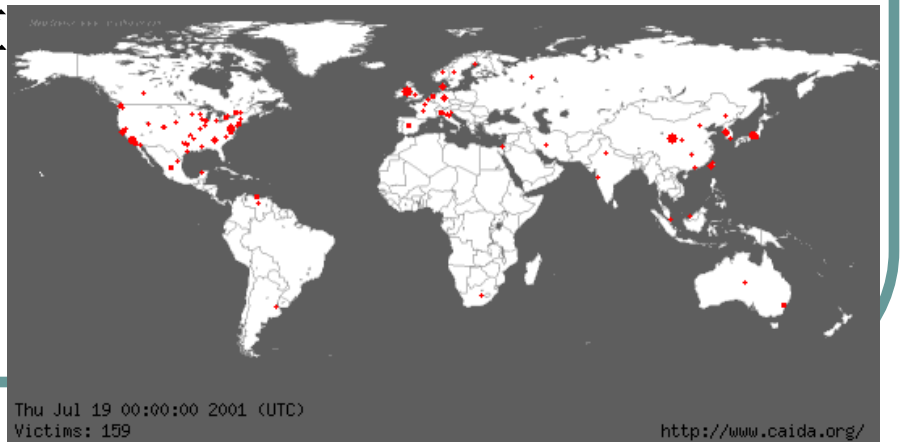
蠕虫和计算机病毒的重新定义

- 1988年Morris蠕虫爆发后，Eugene H. Spafford 为了区分蠕虫和病毒，给出蠕虫和计算机病毒的定义：
  - “计算机蠕虫可以独立运行，并能把自身的一个包含所有功能的版本传播到另外的计算机上”
    - Is a standalone malware computer program that replicates itself in order to spread to other computers.
  - “计算机病毒是一段代码，能把自身加到其他程序包括操作系统上；它不能独立运行，需要由它的宿主程序运行来激活它”

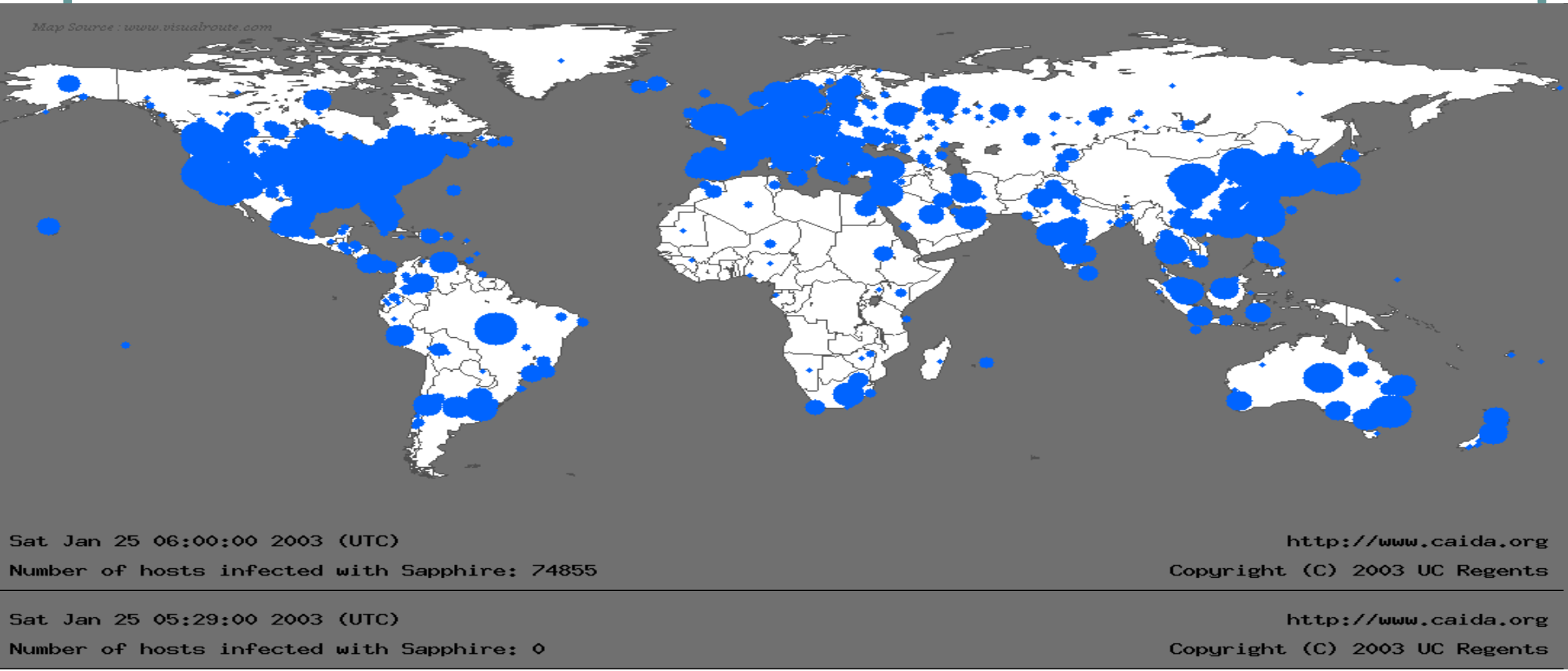
CodeRed—红色代码

- 2001年7月19日爆发，主要针对Windows NT和Windows 2000系统。
- 主要特征
  - 搜索与感染：
    - 1个线程：IP地址计算
    - 99个线程：感染
  - 利用漏洞：IIS的Index服务的缓冲区溢出漏洞（2001年6月18日发布）
  - 破坏：
    - 修改主页，主要针对英文系统。
    - DDoS攻击：白宫网站。



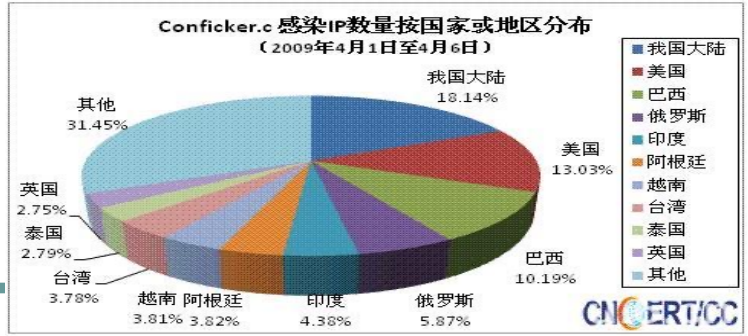


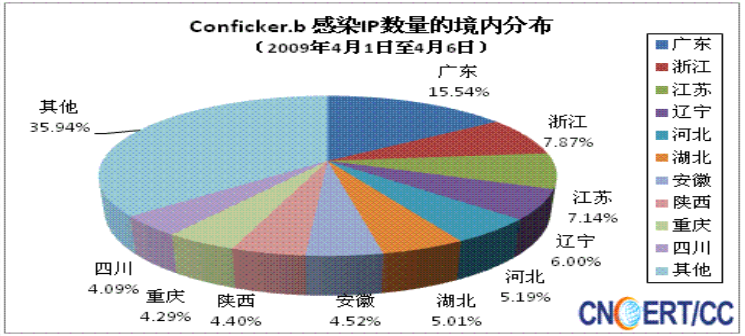
2003年一蠕虫王（slammer）
—376字节，仅存在于内存之中



可用于信息战的蠕虫－飞客(conficker)

- 时间：最早出现在2008年11月，之后相继在12月、次年2月、3月出现变种。
- 传播方式：MS08-067漏洞，局域网、U盘；感染上千万台电脑。
- 攻击程序传输：创建HTTP服务器。
- 控制命令接收方式:随机域名（250随机，500/50000）、P2P网络





12.2 网络蠕虫的分类—产业界通用分类标准

- 漏洞利用类蠕虫-ExploitWorm
  - Slammer、MsBlaster、Sasser、StuxNet等
- 口令破解类蠕虫-PassWorm
  - —通过弱口令进入目标系统，如2003年“口令蠕虫”
  - 2016年Mirai
- 邮件传输类蠕虫—MailWorm
  - Sobig、Mydoom、@mm类
- 即时通信类-IMWorm
  - QQ尾巴、MSN性感鸡等
- P2PWorm、IRCWorm、USBWorm等

按照传输渠道和控制权获取方法划分

典型漏洞利用类蠕虫示例

- 蠕虫王-slammer(2003年1月25日)
  - MS02-039 SQL
- 冲击波-msblast(2003年8月11日)
  - MS03-026 RPC
- 震荡波-sasser(2004年5月1日)
  - MS04-011 Winlogon
- 极速波-Zotob (2005年8月14日)
  - MS05-039 PNP
- 魔波-MocBot（2006年8月13日）
  - MS06-040 RPC
- 扫荡波-saodangbo（2008年11月7日）
  - MS08-067 RPC
- 飞客-conficker（2008年11月）/ Stuxnet（2010年）
  - MS08-067

关于恶意代码分类的差异性

- 计算机病毒：一组能够进行自我传播、需要用户干预来触发执行的破坏性程序或代码。
  - 如CIH、爱虫、美丽莎、新欢乐时光、求职信、恶鹰、rose、威金、熊猫烧香、小浩、机器狗、磁碟机、AV终结者、Flame…
- 网络蠕虫:一组能够进行自我传播、不需要用户干预即可触发执行的破坏性程序或代码。
  - 其通过不断搜索和侵入具有漏洞的主机来自动传播。
  - 如红色代码、SQL蠕虫王、冲击波、震荡波、极速波、魔波、震网…

计算机病毒 VS 网络蠕虫

差异性

计算机病毒 **VS** 网络蠕虫

代码感染类病毒

主机感染：

- 文件或引导区感染
- 寄生代码
- 用户对扩散起到关键作用

病毒or蠕虫？

网络传播：

- 自我复制
- 独立个体
- 用户对扩散起到关键作用
  - 邮件、IM、IRC、USB、P2P等

漏洞利用类蠕虫

网络传播：

- 自我复制
- 独立个体
- 用户对扩散无关键作用
  - 系统漏洞
  - 口令破解

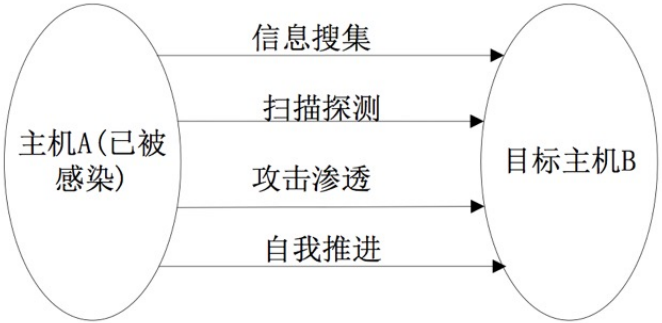
12.3 网络蠕虫的功能模块与关键技术

蠕虫程序的功能结构（主要以漏洞利用型）

- 基本模块：
  - 信息搜集模块
  - 扫描探测模块
  - 攻击渗透模块
  - 自我推进模块
- 扩展功能模块
  - 自动升级模块
  - 远程控制模块
  - 信息通信模块
  - 宿主破坏模块
  - 实体隐藏模块

漏洞利用类的网络蠕虫基本功能

- 四个主要阶段：
  - 信息收集：主要完成对本地和目标节点主机的信息汇集；
  - 扫描探测：发现易感染目标群体(主机服务漏洞的检测)；
  - 攻击渗透：利用已发现的服务漏洞实施攻击［控制权获取］；
  - 自我推进：完成对目标节点的感染［蠕虫主体程序传输（自我复制）］。



基本功能模块

- 信息搜集模块：为发现易感染目标提供支持，
- 搜集包括：
  - 本机系统信息、用户信息、对本机的信任或者授权的主机、本机所处的网络拓朴结构、边界路由信息等。

基本功能模块

- 扫描探测：目的完成特定目标的脆弱性检测，发现易感染目标；
- 影响蠕虫传播速度的主要因素
  - 漏洞主机发现的速度、漏洞主机总数、感染速度
- 主机发现的扫描方法（目标地址空间的选择方式）
  - 随机扫描、选择随机扫描、顺序扫描、
  - hit-list、分治扫描、
  - 路由、DNS
  - 更多的方法 <<网络蠕虫研究与发展>>

基本功能模块

- 攻击渗透模块：该模块利用安全漏洞建立获取目标的控制权
  - **Exploit(shellcode推送)**

基本功能模块

- 网络蠕虫通常利用的漏洞主要有：
  - 目标主机的系统或应用程序漏洞
  - 主机之间信任关系漏洞
  - 目标主机的默认用户和口令漏洞
  - 目标主机的客户端程序配置漏洞

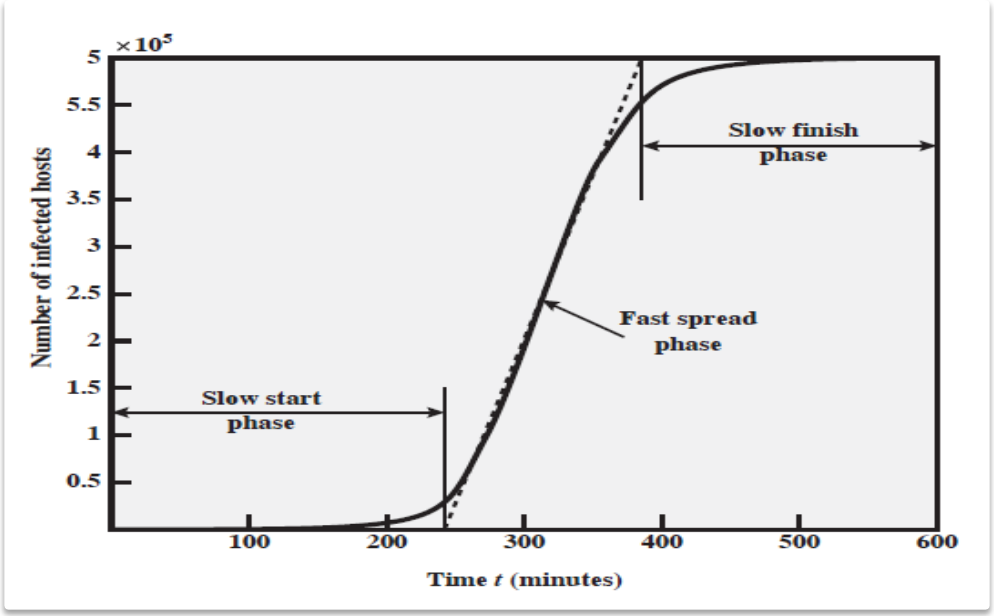
基本功能模块

- 自我推进（自我复制）：该模块在本机与目标主机之间完成蠕虫副本传递
  - （直接传送、**web/ftp/tftp**、**P2P**）

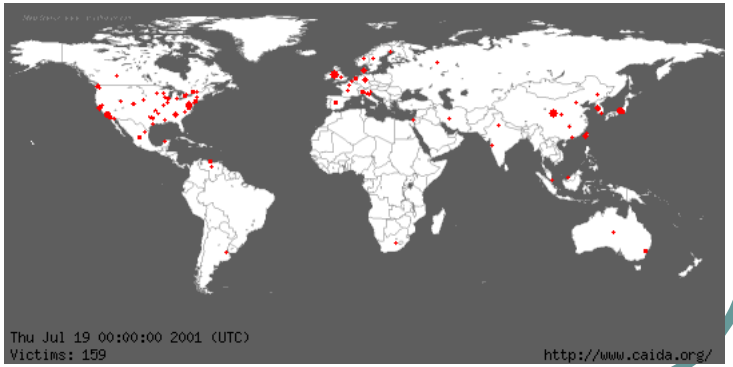
扩展功能模块-取决于攻击者目的

- 实体隐藏模块：对蠕虫实体组成部分隐藏、加密变形，提高蠕虫生存能力。
- 宿主破坏模块：摧毁或破坏被感染计算机；或在被感染的计算机上留下后门程序等等。
- 信息通信模块：使蠕虫间、蠕虫同黑客之间进行通信。
- 远程控制模块：调整蠕虫行为，控制被感染计算机，执行蠕虫编写者下达的命令。
- 自我升级模块：随时更新模块功能，实现持续攻击的目的。

12.4 网络蠕虫的检测与防治



- 蠕虫的传播阶段
  - 慢启动阶段
  - 快速传播阶段
  - 慢结束阶段
  - 被清理期



12.4.1 漏洞利用性蠕虫的特征

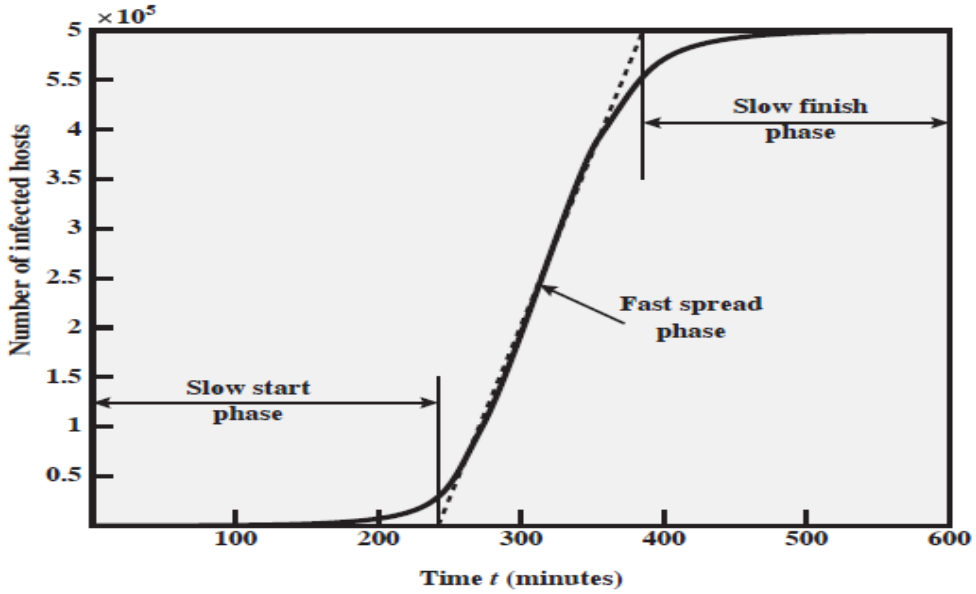
- 特点
  - 利用系统漏洞、网络应用服务漏洞
  - 主动攻击、无需人为干预
  - 速度及其迅猛
- 危害
  - 造成网络拥塞
  - 降低系统性能
  - 产生安全隐患
  - 反复性
  - 破坏性

蠕虫与病毒防护的区别

	文件感染型病毒	其他类蠕虫	漏洞利用和口令破解类蠕虫
存在形式	寄生代码	独立个体	独立个体
传播方法	代码寄生	自我复制	自我复制
传播依赖因素	计算机用户	计算机用户	系统或程序漏洞/弱口令
再次执行	宿主执行	系统自启动机制	系统自启动机制
传播目标	本地文件或系统	网络中其他主机	网络中存在漏洞/弱口令的主机
影响重点	主机系统	主机系统、网络及系统性能	主机系统、网络及系统性能
防范措施	反病毒软件、安全意识	反病毒软件、安全意识、流量阻断	流量阻断、修补补丁、反病毒软件
主要防范主体	计算机用户、反病毒厂商	计算机用户、反病毒厂商、应用服务商、网络管理人员、运营商	网络管理人员、运营商

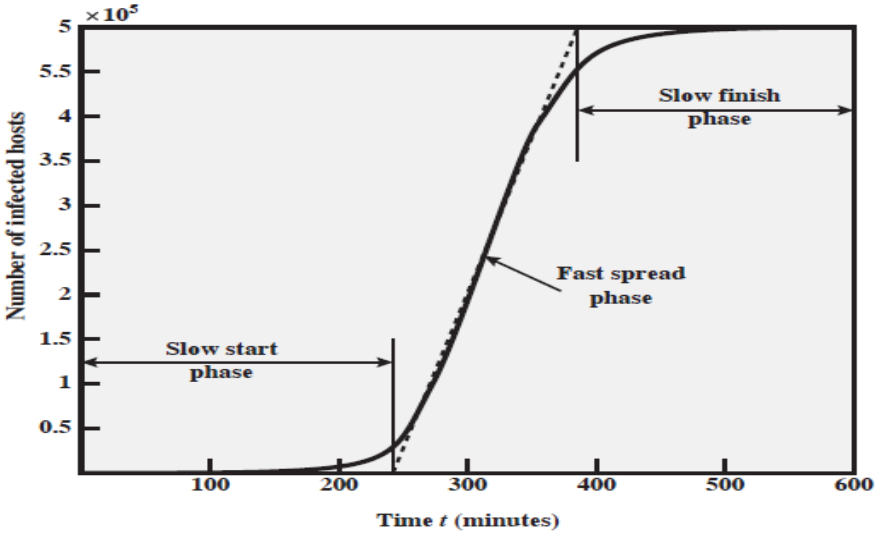
12.4 网络蠕虫的检测与防治

- 个人用户
  - 及时修补补丁
  - 使用防火墙软件
  - 关注流量的异常性
- 网络管理者
  - 网关阻断
  - 补丁下发



网络管理者蠕虫检测与防治

- 网络应用厂商
  - 应用流量过滤与阻断
  - 补丁自动分发与修补
- 安全厂商
  - 网络流量分析与提取
  - 网络安全设备快速阻断
  - 快速利用客户端安全软件清除蠕虫个体，进行补丁修补



思考题

- 1.为什么网络蠕虫的传播速度比计算机病毒要快的多？
- 2. 蠕虫存在慢启动阶段，有什么方法可以加快慢启动阶段的速度？
- 3. 蠕虫会影响用户上网速度，会影响网络带宽，那么提升网络带宽有利于防护蠕虫攻击吗？