软件安全—恶意代码机理与防护

C8 网络蠕虫

武汉大学国家网络安全学院 彭国军

guojpeng@whu.edu.cn

本讲提纲

- 8.1 网络蠕虫的定义
- 8.2 网络蠕虫的分类
- 8.3 网络蠕虫的功能模块
- 8.4 网络蠕虫的检测与防治

8.1 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
  - Fingerd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”
  - “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”

Fred Cohen(1984)

“计算机病毒是一种程序，它可以感染其它程序，感染的方式为在被感染程序中加入计算机病毒的一个副本，这个副本可能是在原病毒基础上演变过来的”。

http://spaf.cerias.purdue.edu/tech-reps/823.pdf

2. Terminology

There seems to be considerable variation in the names applied to the program described in this paper. I use the term *worm* instead of *virus* based on its behavior. Members of the press have used the term *virus*, possibly because their experience to date has been only with that form of security problem. This usage has been reinforced by quotes from computer managers and programmers also unfamiliar with the terminology. For purposes of clarifying the terminology, let me define the difference between these two terms and give some citations to their origins:

A *worm* is a program that can run by itself and can propagate a fully working version of itself to other machines. It is derived from the word *tapeworm*, a parasitic organism that lives inside a host and saps its resources to maintain itself.

A *virus* is a piece of code that adds itself to other programs, including operating systems. It cannot run independently—it requires that its ‘‘host’’ program be run to activate it. As such, it has a clear analog to biological viruses — those viruses are not considered alive in the usual sense; instead, they invade host cells and corrupt them, causing them to produce new viruses.

The program that was loosed on the Internet was clearly a worm.

Fred Cohen(1984)

A Computer Virus

We define a computer 'virus' as a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself. With the infection property, a virus can spread throughout a computer system or network using the authorizations of every user using it to infect their programs. Every program that gets infected may also act as a virus and thus the infection grows.

蠕虫和计算机病毒的定义2

1. *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…

2. *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

其他蠕虫定义

- 2003年，Kienzle 和 Elder 从破坏性、网络传播、主动攻击和独立性4 个方面对网络蠕虫进行了定义：网络蠕虫是通过网络传播，无须用户干预能够独立地或者依赖文件共享主动攻击的恶意代码。
  - 根据传播策略,他们把网络蠕虫分为 3 类:Email 蠕虫、文件共享蠕虫和传统蠕虫.

Kienzle DM, Elder MC . Recent worms: A survey and trends. In: Staniford S, ed. Proc. of the ACM CCS Workshop on Rapid Malcode (WORM 2003). Washington, 2003.

其他蠕虫定义

- 南开大学郑辉博士认为，蠕虫具有主动攻击、行踪隐蔽、利用漏洞、造成网络拥塞、降低系统性能、产生安全隐患、反复性和破坏性等特征，并给出相应的定义：“网络蠕虫是无须计算机使用者干预即可运行的独立程序，它通过不停地获得网络中存在漏洞的计算机上的部分或全部控制权来进行传播”。
  - 该定义包含了 Kienzle 和 Elder 定义的后两类蠕虫,不包括 E-mail 蠕虫.

郑辉. Internet蠕虫研究[博士学位论文].天津:南开大学信息技术科学学院,2003.

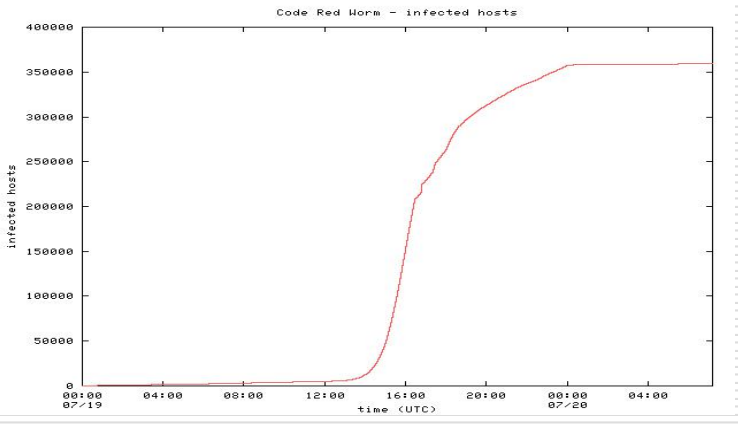
其他蠕虫定义

- 中科院文伟平博士等认为，“网络蠕虫是一种智能化、自动化，综合网络攻击、密码学和计算机病毒技术，不需要计算机使用者干预即可运行的攻击程序或代码。它会扫描和攻击网络上存在系统漏洞的节点主机，通过局域网或者国际互联网从一个节点传播到另外一个节点。
  - 该定义体现了新一代网络蠕虫智能化、自动化和高技术化的特征，是对郑辉网络蠕虫定义的扩展。

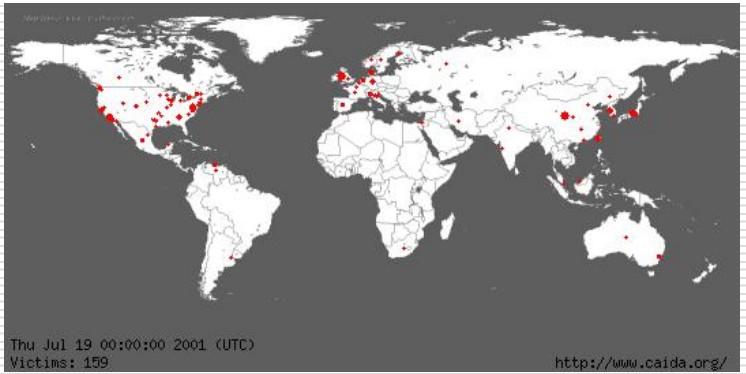
文伟平 等:网络蠕虫研究与进展. 软件学报，2004,15(8)：1208-1219 。

CodeRed—红色代码

- 2001年7月19日爆发，主要针对Windows NT和Windows 2000系统。

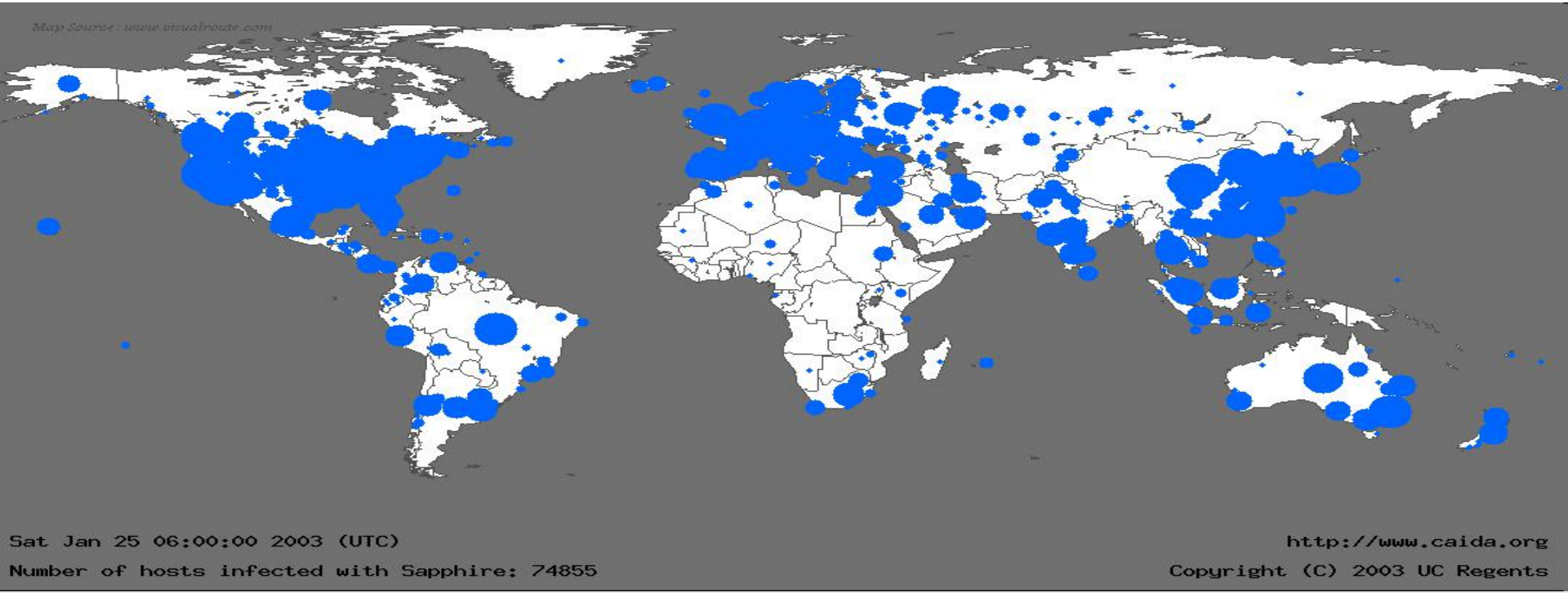


- 主要特征
  - 搜索与感染：
    - 1个线程：IP地址计算
    - 99个线程：感染
  - 利用漏洞：IIS的Index服务的缓冲区溢出漏洞（2001年6月18日发布）
  - 破坏：
    - 修改主页，主要针对英文系统。
    - DDoS攻击：白宫网站。



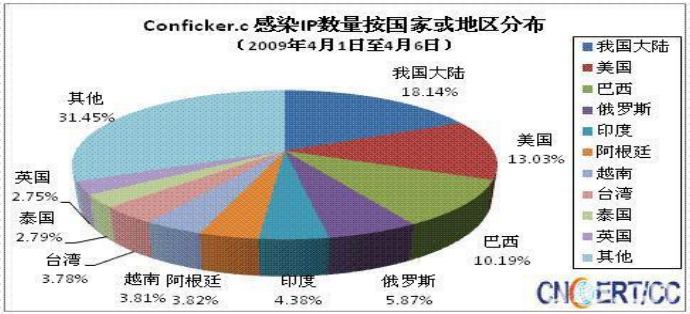
2003年一蠕虫王（slammer）

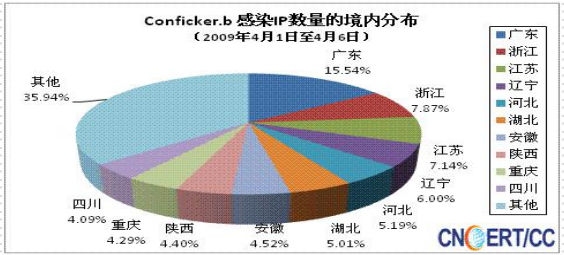
－376字节，仅存在于内存之中



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。





本讲提纲

- 8.1 网络蠕虫的定义
- 8.2 网络蠕虫的分类
- 8.3 网络蠕虫的功能模块
- 8.4 网络蠕虫的检测与防护

8.2 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”
- 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
- 冲击波-msblast（2003年8月11日）
  - MS03-026
- 震荡波-sasser（2004年5月1日）
  - MS04-011
- 极速波-Zotob（2005年8月14日）
  - MS05-039
- 魔波-MocBot（2006年8月13日 ）
  - MS06-040
- 扫荡波-saodangbo（2008年11月7日）
  - MS08-067
- 飞客-conficker（2008年11月） / Stuxnet（2010年）
  - MS08067

关于恶意代码分类的差异性

1. *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…

2. *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

特点与防范区别

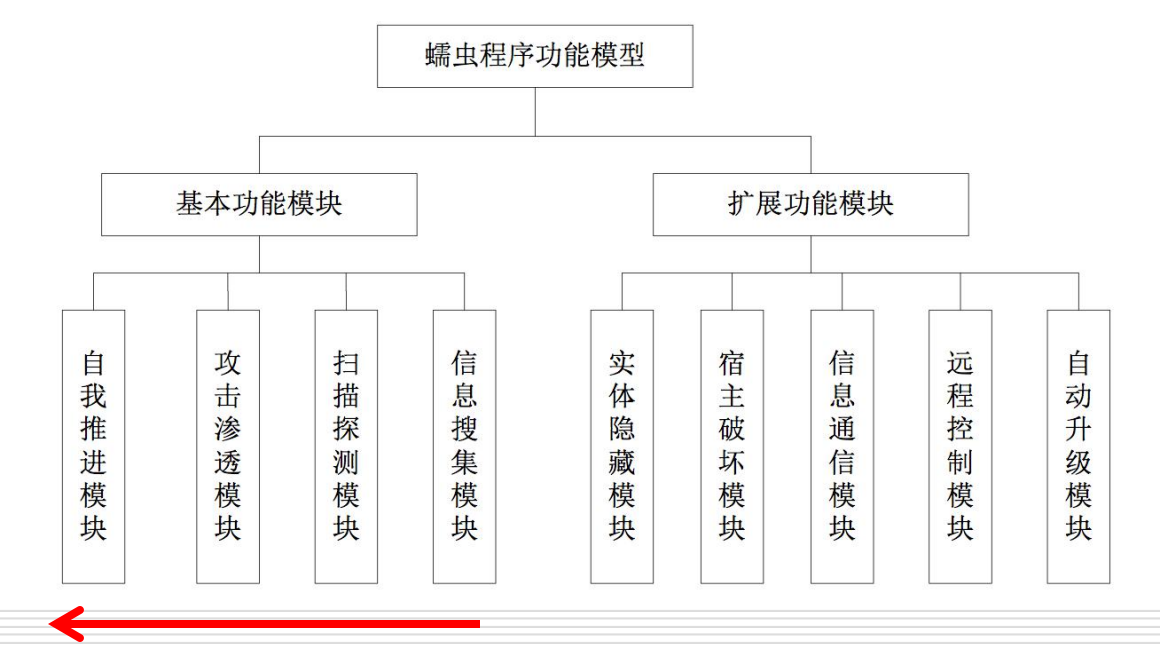
	感染型病毒	其他类蠕虫	漏洞利用类蠕虫［&口令破解类］
存在形式	寄生代码	独立个体	独立个体
传播方法	代码寄生	自我复制	自我复制
传播依赖因素	计算机用户	计算机用户	系统或程序漏洞
再次执行	宿主执行	系统自启动机制	系统自启动机制
传播目标	本地文件或系统	网络中其他主机	网络中存在漏洞的主机
影响重点	主机系统	主机系统、网络及系统性能	网络及系统性能
防范措施	反病毒软件、安全意识	反病毒软件、安全意识、流量阻断	流量阻断、修补补丁、反病毒软件
主要防范主体	计算机用户、反病毒厂商	计算机用户、反病毒厂商、应用服务商、网络管理人员、运营商	网络管理人员、运营商

本讲提纲

- 8.1 网络蠕虫的定义
- 8.2 网络蠕虫的分类
- 8.3 网络蠕虫的功能模块
- 8.4 网络蠕虫的检测与防治

8.3 网络蠕虫的功能模块

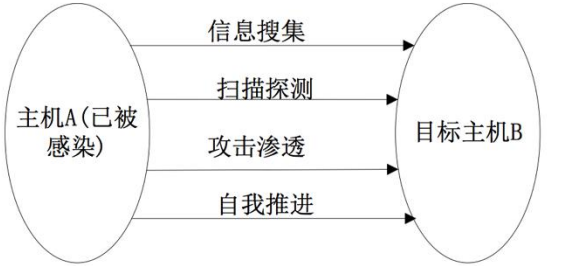
网络蠕虫程序的功能结构



注：后续提到的蠕虫，主要指漏洞利用型蠕虫

网络蠕虫基本功能

- 四个主要模块：
  - 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：发现易感染主机群体；
  - 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］。



8.3.1 信息收集

- **目的：**对本地或者目标网络进行信息搜集，为发现易感染目标提供支持。
- 搜集信息包括：
  - 本机系统信息、用户信息、对本机的信任或授权的主机、本机所处网络的拓扑结构、边界路由信息等等。

8.3.2 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（主机）。

- 影响网络蠕虫传播速度的主要因素：
  - 漏洞主机被发现的速度；
  - 漏洞主机的总数；
  - 网络蠕虫对目标的感染速度。

—相对恒定

—取决于蠕虫自身以及漏洞的利用机制。

扫描策略—如何更快地覆盖易感染群体。

- 按照蠕虫对目标地址空间的选择方式进行分类，扫描策略可分为：
  - 随机扫描、
  - 选择性随机扫描、
  - 顺序扫描、
  - 基于目标列表（hit-list）的扫描、
  - 分治扫描、
  - 基于路由的扫描、
  - 基于DNS扫描等。

文伟平 等:网络蠕虫研究与进展. 软件学报，2004,15(8)：1208-1219 。

8.3.3攻击渗透模块

- 目的：该模块利用安全漏洞建立获取目标系统的控制权。
  - Exploit（Shellcode推送）

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

8.3.4 自我推进［自我复制］

- 目的：该模块在本机与目标主机间完成蠕虫副本传递。
  - 文件直接传输
  - 搭建Web、FTP、tftp服务器
  - P2P等

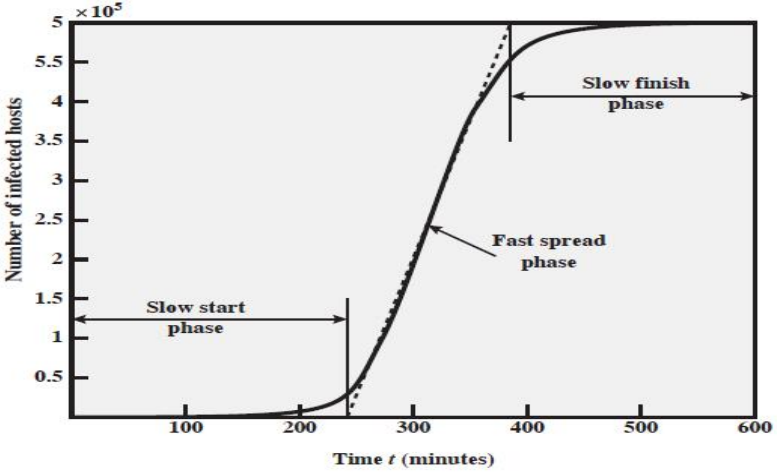
8.3.5 扩展功能模块—取决于攻击者目的

- 实体隐藏模块：包括对蠕虫各个实体组成部分的隐藏、加密、变形，主要提高蠕虫的生存能力。
- 宿主破坏模块：用于摧毁或破坏被感染主机，破坏网络正常运行，在被感染主机上留下后门等。
- 信息通信模块：能使蠕虫间、蠕虫同黑客之间进行通信。
- 远程控制模块：调整蠕虫行为，控制被感染主机，执行蠕虫编写者下达的指令。
- 自动升级模块：随时更新模块功能，实现持续攻击目的。

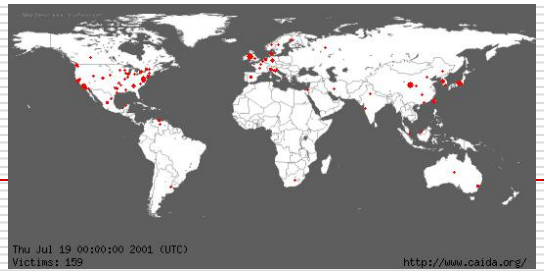
本讲提纲

- 8.1 网络蠕虫的定义
- 8.2 网络蠕虫的分类
- 8.3 网络蠕虫的功能模块
- 8.4 网络蠕虫的检测与防治

8.4 网络蠕虫的检测与防治



- 蠕虫传播的阶段：
  - 慢启动期
  - 快速传播期
  - 慢结束期
  - 被清理期



8.4.1 漏洞利用型蠕虫的行为特征

- 特点：
  - 利用系统、网络应用服务漏洞
  - 主动攻击、无需人为干预
  - 速度极其迅猛、
- 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

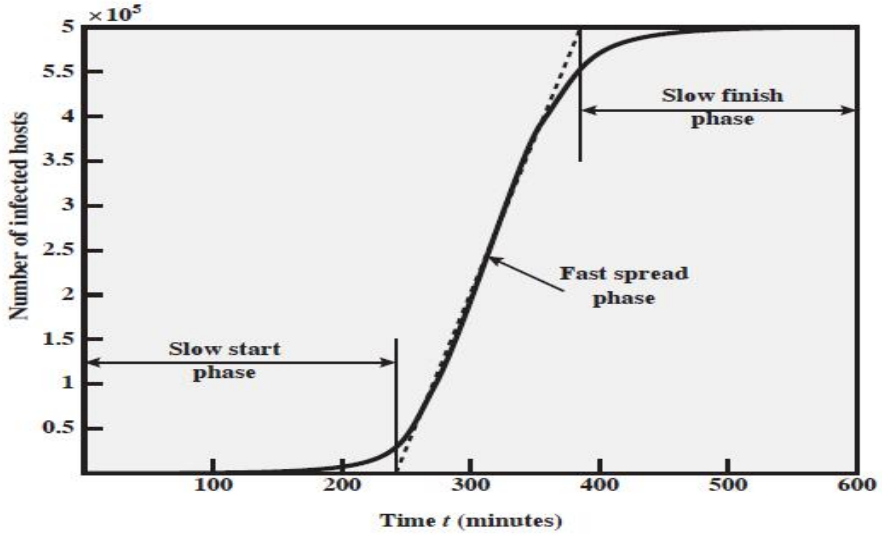
8.4.2 网络蠕虫与病毒防护的区别

	感染型病毒	其他类蠕虫	漏洞利用类蠕虫
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
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	网络中存在漏洞的主机
影响重点	主机系统	主机系统、网络及系统性能	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

口令破解类

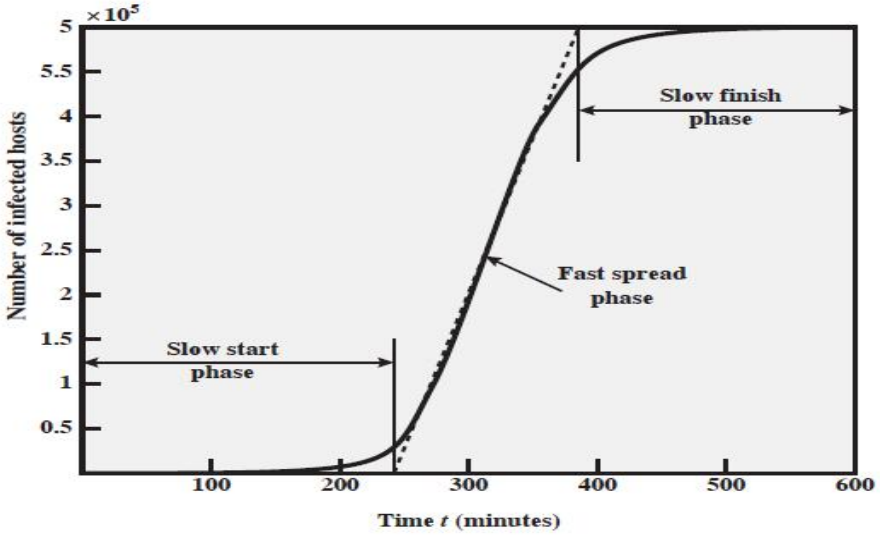
8.4.3 网络蠕虫的检测与防治

- 个人用户
  - 及时修补漏洞补丁
  - 使用防火墙软件阻断
  - 安全防护软件及时更新



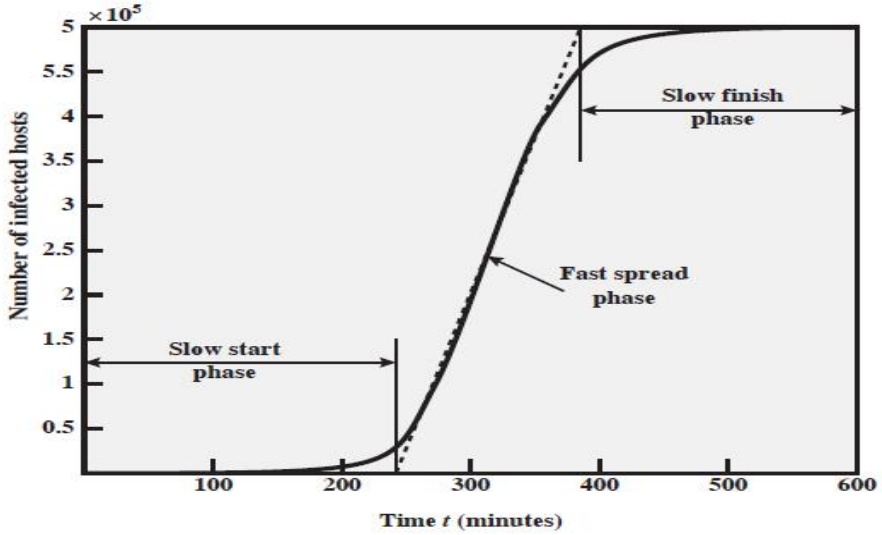
8.4.3 网络蠕虫的检测与防治

- 网络管理者
  - 网关阻断
  - 补丁下发



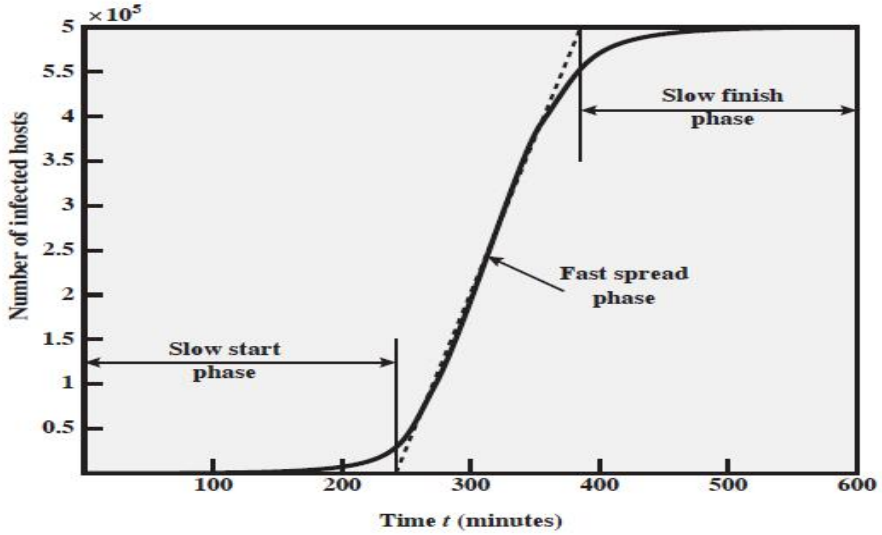
8.4.3 网络蠕虫的检测与防治

- 安全厂商
  - 网络流量特征分析与提取
  - 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，并进行补丁修补



8.4.3 网络蠕虫的检测与防治

- 网络应用厂商
  - 应用流量过滤与阻断
  - 补丁自动分发与修补



C8 课后思考

- 为什么网络蠕虫的传播速度要远远大于计算机病毒？
- 关于网络蠕虫与计算机病毒的定义和分类，目前存在不同的观点，请查阅资料并分析这种差异及其产生的原因？
- 网络蠕虫传播为什么会存在慢启动和慢结束阶段？通过何种方式可以增加慢启动阶段的速度？
- 网络蠕虫对用户上网速度产生明显影响，那么，增加网络带宽是否可以有效防止蠕虫攻击？