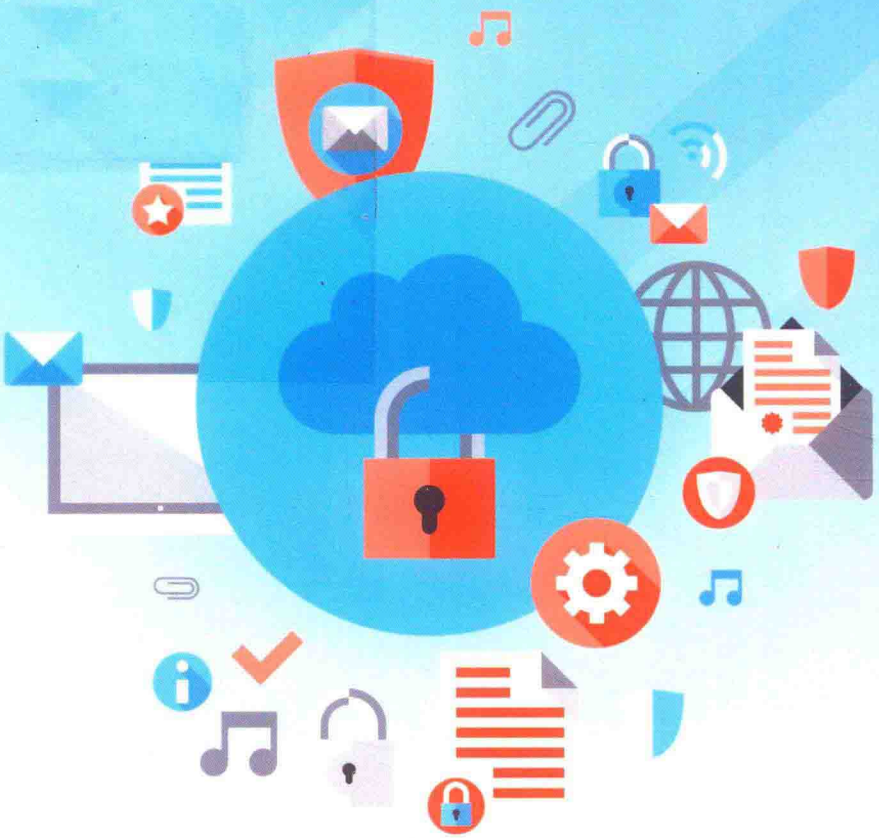

网络安全与云计算

安　庆　廖倬跃　刘　杰◎著

燕山大学出版社
YANSHAN UNIVERSITY PRESS

网络安全与云计算

安　庆　廖倬跃　刘　杰◎著

燕山大学出版社
·秦皇岛·

图书在版编目（CIP）数据

网络安全与云计算 / 安庆，廖倬跃，刘杰著 . — 秦皇岛：燕山大学出版社，2022.6
ISBN 978-7-5761-0358-8

Ⅰ . ①网… Ⅱ . ①安…②廖… ③刘… Ⅲ . ①计算机网络—网络安全—研究②云计算—研究
Ⅳ . ① TP393.08 ② TP393.027

中国版本图书馆 CIP 数据核字（2022）第 080223 号

网络安全与云计算

安　庆　廖倬跃　刘　杰　著

出 版 人：陈　玉
责任编辑：王　宁　　策划编辑：吴　波
责任印制：吴　波　　封面设计：星辰创意
出版发行：燕山大学出版社 YANSHAN UNIVERSITY PRESS　　电　话：0335-8387555
地　址：河北省秦皇岛市河北大街西段 438 号　　邮政编码：066004
印　刷：英格拉姆印刷(固安)有限公司　　经　销：全国新华书店

开　本：170mm × 240mm　1/16　　印　张：12.75
版　次：2022 年 6 月第 1 版　　印　次：2022 年 6 月第 1 次印刷
书　号：ISBN 978-7-5761-0358-8　　字　数：221 千字
定　价：52.00 元

前　言

网络以其丰富的信息资源和灵活的服务方式正越来越广泛地覆盖人们的生活，依赖网络的各种应用及信息共享服务已经非常普及。在错综复杂的网络环境中，信息的传递和共享使安全问题也变得越来越突出，网络安全问题在整个网络应用中不容回避，对网络安全相关知识的学习和研究已经成为人们生活和工作中非常重要的组成部分。

由于因特网本身安全性设计的缺陷及其开放性的应用环境，网络安全变得十分脆弱。一些黑客正是利用网络存在的安全漏洞向网络系统不断发起攻击。不管黑客或网络攻击者出于何种目的，目前一些黑客的恶意攻击正成为全球新的公害。因此，我们应该认识黑客、了解黑客、防御黑客的入侵，从技术上剖析黑客的种种攻击手段，让普通网民，特别是大学生及网络管理人员对黑客技术和网络安全漏洞有一个大致的了解，从而把因网络安全问题引起的损失降到最低。

随着网络用户的逐渐增多，传统的计算网络平台已无法满足实际需求，故云计算应运而生。云计算离不开计算机网络，计算机网络也是云计算的基础。作为一种商业计算模型，云计算是基于网络将计算任务分布在大量计算机构成的资源池上，使用户能够借助网络按需获取计算力、存储空间和信息服务。云计算融合了大量革新技术，它不仅是技术革新驱动商业模式变革的产物，也是用户需求驱动的结果。

随着互联网的不断发展和海量数据处理需求的增加，云计算技术成为当前最热门的 IT 技术，被视为 IT 业的下一次革命。云计算是在传统的数据存储、分布式计算和网络技术等计算机技术的基础之上发展而来的，它增强了分布式存储和处理海量数据的能力，以方便人们按需及时获取相应服务。在当今这个数据信息大爆炸的时代，云计算的实现和发展日益显现出了它的强大存储计算能力和广泛应用前景。随着计算机网络技术不断走进我们的工作和生活，其安全性一直是社会关注的重点。网络信息的安全问题会导致一系列的严重后果，为用户带来不可

估量的损失。在网络环境不断发展的同时，加强网络安全应用的研究已经成为计算机网络发展必须关注的重点问题。

目录

第一章　网络安全概述

第一节　网络安全概念及现状

随着信息技术的迅速发展，网络已成为重要的信息传播工具。而随着互联网技术的飞速发展，网络安全问题也受到越来越广泛的关注，各种病毒花样繁多、层出不穷，系统、程序、软件的安全漏洞越来越多，黑客们常通过不正当的手段侵入他人计算机，非法获得用户的信息资料，给正常使用互联网的用户带来不可估计的损失。因此，网络安全越来越引起人们的重视。

一、网络安全的概念

人们在享受信息化带来的众多好处的同时，也面临着日益突出的信息安全与保密问题。计算机网络信息安全技术经过多年的发展，在信息安全技术的研究基础上形成了两个完全不同的角度和方向：一个是从正面防御角度考虑，研究加密、鉴别、认证、授权和访问控制等；另一个是从反面攻击角度考虑，研究漏洞的扫描评估、入侵检测、紧急响应和病毒预防。网络安全从其本质上来讲就是网络上的信息安全，它涉及的领域相当广泛，这是因为在目前的公用通信网络中存在着各种各样的安全漏洞和威胁。下面给出网络安全的一个通用定义：网络安全就是网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然或者恶意的原因而遭到破坏、更改、泄露，系统能连续、可靠、正常地运行，保证网络服务不中断[①]。

广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论，都是网络安全研究的领域。

网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两者相互补充，缺一不可。技术方面主要侧重于防范外部非法用户的攻击，管理方面则侧

① 李剑 . 计算机网络安全 [M]. 北京：机械工业出版社，2019.

重于内部人为因素的管理。网络安全要考虑以下几个方面的内容。

（一）网络系统的安全

网络系统的安全主要包括以下几方面的问题：第一，网络操作系统的安全性。比较流行的操作系统（UNIX、Windows7/8/10 等）均存在网络安全漏洞。第二，来自外部的安全威胁。第三，来自内部用户的安全威胁。第四，通信协议软件本身缺乏安全性（如 TCP/IP 协议）。第五，计算机病毒感染。第六，应用服务的安全，许多应用服务系统在访问控制及安全通信方面考虑不周全。

（二）局域网安全

局域网采用广播方式，在同一个广播域中可以侦听到在该局域网上传输的所有信息包，这是一个不安全的因素。

（三）因特网互联安全

非授权访问、冒充合法用户、破坏数据完整性、干扰系统正常运行、利用网络传播病毒等都是在因特网上经常遇到的问题。

（四）数据安全

事实上，无论因特网还是其他专用网络，都必须注意数据的安全性问题，以保护本单位、本部门的信息资源不受到外来因素的侵害。

从根本意义上讲，绝对安全的计算机是不存在的，绝对安全的网络也是不可能有的。只有存放在一个无人知晓的密室里而又不通电的计算机才可以称得上安全。计算机只要投入使用，就或多或少地存在着安全问题，只是程度不同而已。因此，在探讨网络安全的时候，实际上指的是一定程度上的网络安全。而到底需要多大的安全性，要依据实际需要及自身能力而定。网络安全性越高，也就意味着网络的管理越复杂。网络的安全性与网络管理的便利性是相互矛盾的关系。

二、网络安全模型

信息需要从一方通过网络传送到另一方，在传送过程中居主体地位的双方必须相互合作以便进行交换，通过通信协议（如 TCP/IP）在两个主体之间可以建立一条逻辑信息通道。

为防止对手对信息机密性、可靠性等造成破坏，需要保护传送的信息。保证安全性的所有机制包括以下两部分。

第一，对被传送的信息进行与安全相关的转换。加密消息使对手无法阅读，补充代码可以用来验证发送方的身份。

第二，两个主体共享不希望对手得知的保密信息。例如使用密钥链接，在发送前对信息进行转换，在接收后再转换回来。为了实现安全传送，可能需要可信任的第三方。例如第三方可能会负责向两个主体分发保密信息，而向其他对手保密，或者需要第三方对两个主体间传送信息可靠性的争端进行仲裁。这种通用模型指出了设计特定安全服务的四个基本任务：第一，设计执行与安全性相关的转换算法，该算法必须使对手不能对算法进行破解以实现其目的。第二，生成算法使用的保密信息。第三，开发分发和共享保密信息的方法。第四，指定两个主体要使用的协议，并利用安全算法和保密信息来实现特定的安全服务。

三、计算机安全的分级

计算机操作系统的安全级别在美国国防部发表的橘皮书——《可信计算机系统评估准则》中被分为四个等级、七个级别，即 D（最低保护等级）、C（自主保护等级）、B（强制保护等级）、A（验证保护等级）四等，细分为 D、C1、C2、B1、B2、B3、A1 七级。D 级——计算机安全的最低一级。不要求用户进行登录密码保护，任何人都可以使用，整个系统是不可信任的，硬件和软件都易被他人侵袭。C1 级——自主安全保护级。要求硬件有一定的安全级（如计算机带锁），用户必须通过登录认证方可使用系统，并建立了访问许可权限机制。C2 级——受控存取保护级。比 C1 级增加了几个特性，即引进了受控访问环境，进一步限制了用户执行某些系统指令；授权分级使系统管理员为用户分组，授予他们访问某些程序和分级目录的权限；采用系统审计，跟踪记录所有安全事件及系统管理员的工作。B1 级——标记安全保护级。对网络上每个对象都实施保护；支持多级安全，对网络、应用程序工作站实施不同的安全策略；对象必须在访问控制之下，不允许拥有者自己改变所属资源的权限。B2 级——结构化保护级。对网络和计算机系统中所有对象都加以定义，分配给一个标签；为工作站、终端等设备分配不同的安全级别；按最小特权原则取消权力无限大的特权用户。B3 级——安全域级。要求用户工作站或终端必须通过可信任的途径链接到网络系统内部的主机上；利用硬件来保护系统的数据存储区；根据最小特权原则，增加了系统安全员，将系统管理员、系统操作员和系统安全员的职责分离，将人为因素对计算机安全的威胁降至

最小。A1 级——验证设计级。这是计算机安全级别中最高的一级，本级包括了以上各级别的所有措施，并附加了一个安全系统的受监视设计；合格的个体必须经过分析并通过这一设计；所有构成系统的部件来源都必须有安全保证；这一级还规定了将安全计算机系统运送到现场安装所必须遵守的程序。

在网络的具体设计过程中，应根据网络总体规划提出的各项技术规范、设备类型、性能要求及经费等，综合考虑来确定一个比较合理、性能较高的网络安全级别，从而实现网络的安全性和可靠性。

四、网络安全的重要性

在信息社会中，信息具有与能源、物源同等的价值，在某些时候甚至具有更高的价值。具有价值的信息必然存在安全性的问题，对于企业更是如此。例如在竞争激烈的市场经济驱动下，每个企业对于原料配额、生产技术、经营决策等信息，在特定的地点和业务范围内都具有保密的要求，这些机密一旦被泄露，不仅会给企业带来损失，甚至会给国家造成严重的经济损失。

经济社会的发展要求各用户之间的通信和资源进行共享，这就需要将一批计算机联成网络，如此一来便隐藏着很大的风险，包含了极大的脆弱性和复杂性。特别是当今最大的网络——互联网，很容易遭到别有用心者的恶意攻击和破坏。随着国民经济信息化程度的提高，大量有关的情报和商务信息都高度集中地存放在计算机中。随着网络应用范围的扩大，信息泄露问题也变得日益严重。因此，计算机网络的安全性问题就越来越重要。

五、网络安全的现状

互联网与生俱有的开放性、交互性和分散性特征，使人类憧憬的信息共享、开放、灵活和快速等需求得到满足。网络环境为信息共享、信息交流和信息服务创造了理想空间，网络技术的迅速发展和广泛应用，为人类社会的进步提供了巨大推动力。正是由于互联网的上述特性，产生了许多安全问题：第一，黑客（Hacker）问题。黑客是指在因特网上一批熟悉网络技术的人，经常利用网络上现存的一些漏洞，设法进入他人的计算机系统。有些人只是好奇，而有些人则是心怀不良动机侵入他人的计算机系统。他们偷窥机密信息，或破坏其计算机系统，这部分人就被称为“黑客”。尽管人们在计算机技术上作出了种种努力，但这种攻击却愈演愈烈。从单一地利用计算机病毒和用黑客手段进行入侵攻击，转变为使用恶意代

码与黑客攻击手段相结合，使得这种攻击具有传播速度迅猛、受害面惊人和穿透深度高的特点，往往一次攻击就会给受害者带来严重的破坏和损失。第二，信息泄露、信息污染、信息不易受控。例如资源未授权侵用、未授权信息流出现、系统拒绝信息流和系统否认等，这些都是信息安全的技术难点。第三，在网络环境中，一些组织或个人出于某种特殊目的，进行信息泄密、信息破坏、信息侵权和意识形态的信息渗透，甚至通过网络进行政治颠覆等活动，使国家利益、社会公共利益和各类主体的合法权益受到威胁。第四，网络运用的趋势是全社会广泛参与，随之而来的是控制权分散的管理问题。由于人们的利益、目标及价值观产生分歧，信息资源的保护和管理出现脱节和真空，从而使信息安全问题变得广泛而复杂。第五，随着社会重要基础设施的高度信息化，社会的命脉和核心控制系统有可能面临恶意攻击而导致损坏和瘫痪，包括国防通信设施、动力控制网、金融系统和政府网站等。

近年来，人们的网络安全意识逐步提高，很多企业根据核心数据库和系统运营的需要，逐步部署了防火墙、防病毒和入侵检测系统等安全产品，并配备了相应的安全策略。虽然有了这些措施，但并不能解决一切问题。我国网络安全问题日益突出，其主要表现在以下几个方面。

（一）安全事件不能及时、准确发现

网络设备、安全设备、计算机系统每天生成的日志可能有上万条甚至几十万条，利用人工对多个安全系统的大量日志进行实时审计、分析的工作通常都流于形式，再加上误报（如网络入侵检测系统 NIDS、互联网协议群 IPS）、漏报（如未知病毒、未知网络攻击、未知系统攻击）等问题，造成不能及时、准确地发现安全事件。

（二）安全事件不能准确定位

信息安全系统通常是由防火墙、入侵检测、漏洞扫描、安全审计、防病毒、流量监控等产品组成的，但是由于安全产品来自不同的厂商，且没有统一的标准，所以安全产品之间无法进行信息交流，于是形成许多安全孤岛和安全盲区。由于事件孤立，相互之间无法形成很好的集成关联，因而一个事件的出现不能关联到真实问题。如入侵检测系统事件报警，就需关联同一时间防火墙报警、被攻击的服务器安全日志报警等，从而确定是真实报警还是误报。如是未知病毒的攻击，

则分为两类，即网络病毒和主机病毒。网络病毒大多表现为流量异常，主机病毒大多表现为中央处理器异常、内存异常、磁盘空间异常、文件的属性和大小改变等。要发现这个问题，就需要关联流量监控（网络病毒）、服务器运行状态监控（主机病毒）和完整性检测（主机病毒）。为了预防网络病毒大规模爆发，则必须在病毒爆发前快速发现中毒机器并切断源头。例如服务器的攻击可能是遭受病毒感染，分布式拒绝服务 DDoS（Distributed Denial of Service）攻击可能是服务器 CPU 超负荷，端口某服务流量太大、访问量太大等，必须将多种因素结合起来才能更好的分析，快速了解真实问题点并及时恢复正常。其中，DDoS 是一种基于 DoS 的特殊形式的拒绝服务攻击，是一种分布、协作的大规模攻击方式，主要瞄准比较大的站点，像商业公司、搜索引擎和政府部门的站点。DDoS 攻击是利用一批受控制的机器向一台机器发起攻击，这样来势迅猛的攻击令人难以防备，因此具有较大的破坏性。

（三）无法做集中的事件自动统计

这一问题涉及某台服务器的安全情况报表、所有机房发生攻击事件的频率报表、网络中利用次数最多的攻击方式报表、发生攻击事件的网段报表、服务器性能利用率最低的服务器列表等，需要管理员人为地对这些事件做统计记录，生成报告，从而耗费大量人力。

（四）缺乏有效的事件处理

查询没有对事件处理的整个过程做跟踪记录，信息部门主管不了解哪些管理员对该事件进行了处理，对处理过程和结果也没有做记录，使得处理的知识和经验不能得到共享，导致下次再发生类似事件时，处理效率仍然比较低。

（五）缺乏专业的安全技能

管理员发现问题后，往往因为缺乏安全知识导致事件迟迟不能被处理，从而影响网络的安全性，并且延误网络的正常使用。

第二节　计算机网络安全威胁

安全威胁是指某个人、物、事件或概念对某一资源的机密性、完整性、可用

性或合法性造成的危害。某种攻击就是某种威胁的具体实现。安全威胁可分为故意（如黑客渗透）和偶然（如信息被发往错误的地址）两类。故意威胁又可进一步分为被动攻击和主动攻击两类。

一、安全威胁

对于计算机或网络安全性的威胁，即安全攻击，一般是通过在提供信息时查看计算机系统的功能来记录其特性的，可分为中断、截获、篡改、伪造。中断，是指系统资源遭到破坏或变得不能使用，这是对可用性的攻击。例如对一些硬件进行破坏、切断通信线路或禁用文件管理系统。截获，是指未授权的实体得到了资源的访问权，这是对保密性的攻击。未授权实体可能是一个人、一个程序或一台计算机。篡改，是指未授权的实体不仅得到了访问权，而且还篡改了资源，这是对完整性的攻击。伪造，是指未授权的实体向系统中插入伪造的对象，这是对真实性的攻击[①]。

（一）被动攻击与主动攻击

上面提到的攻击类型可以分为被动攻击和主动攻击两种。第一，被动攻击的特点是偷听或监视传送，其目的是获取正在传送的消息。被动攻击有泄露信息内容和通信量分析等形式。可泄露的信息内容容易理解，包括电话对话、电子邮件消息以及可能含有敏感的机密信息。要防止对手从传送中获得这些内容，我们用某种方法将信息内容隐藏起来，常用的技术是加密，这样即使对手捕获了消息，也不能从中提取信息。对手可以确定位置和通信主机的身份，可以观察交换消息的频率和长度，这些信息可以帮助对手猜测正在进行的通信的特性。第二，主动攻击涉及修改数据或创建错误的数据流，它包括假冒、重放、修改消息、拒绝服务等。假冒，是指一个实体假装成另一个实体。假冒攻击通常包括一种其他形式的主动攻击。重放涉及被动捕获数据单元及其后来的重新传送，以产生未经授权的效果。修改消息意味着改变了真实消息的部分内容，或将消息延迟或重新排序，导致未授权的操作。拒绝服务，是指禁止对通信工具的正常使用或管理，这种攻击拥有特定的目标；另一种拒绝服务的形式是整个网络的中断，可以通过使网络失效而实现，或通过消息过载使网络性能降低。主动攻击具有与被动攻击相反的特点。虽然很难检测出被动攻击，但可以采取措施防止它的成功。相反，很难绝对预防主动攻击，因为这样需要随时对所有的通信工具和路径进行完全保护。防

① 朱超军．网络安全与网络行为研究 [M]. 北京：北京理工大学出版社，2019.

止主动攻击的做法是对攻击进行检测，并从它引起的中断或延迟中恢复过来。因为检测具有威慑的效果，也可以起到预防作用。

（二）服务攻击与非服务攻击

从网络高层协议的角度，攻击方法可以概括地分为两大类。

1. 服务攻击（Application Dependent Attack）

服务攻击是针对某种特定网络服务的攻击，如针对 E-Mail 服务、Telnet、FTP、HTTP 等服务的专门攻击。目前因特网应用协议集（主要是 TCP/IP 协议集）缺乏认证、保密措施，是造成服务攻击的重要原因。现在有很多具体的攻击工具，如 Mail Bomb（邮件炸弹），可以很容易地实施对某项服务的攻击。

2. 非服务攻击（Application Independent Attack）

非服务攻击不针对某项具体的应用服务，而是基于网络层等低层协议而进行的攻击。TCP/IP 协议（尤其是 IPv4）自身的安全机制存在缺陷，从而为攻击者提供了方便。与服务攻击相比，非服务攻击往往利用协议或操作系统实现协议时的漏洞来达到攻击的目的，其更为隐蔽。而且目前非服务攻击也是常常被忽略的一个方面，因而被认为是一种更为有效的且更具危险性的攻击手段。

二、基本的威胁

网络安全的基本目标是实现信息的机密性、完整性、可用性和合法性。以下四个基本的安全威胁直接反映了这四个安全目标。

（一）信息泄露或丢失

信息泄露或丢失，是指敏感数据在有意或无意中被泄露或丢失，通常包括信息在传输中泄露或丢失、信息在存储介质中泄露或丢失、通过建立隐蔽通道等窃取敏感信息。

（二）破坏数据完整性

破坏数据完整性，是指以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加、修改数据，以干扰用户的正常使用。

（三）拒绝服务攻击

这一威胁主要是不断地对网络服务系统进行干扰，改变其正常的作业流程、

执行无关程序使系统响应减慢甚至瘫痪，影响用户的正常使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

（四）非授权访问

没有预先经过同意就使用网络或计算机资源，被看作非授权访问。如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。它主要有假冒身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等几种形式。

三、主要可实现的威胁

这些威胁可以使基本威胁成为可能，所以十分重要。它包括两类，即渗入威胁和植入威胁。

（一）渗入威胁的几种形式

主要的渗入威胁有：假冒、旁路控制、授权侵犯。假冒，是大多数黑客采用的攻击方法。某个未授权实体使守卫者相信它是一个合法的实体，从而攫取该合法用户的特权。旁路控制，攻击者通过各种手段发现本应保密却又暴露出来的一些系统特征，利用这些特征，攻击者绕过防线守卫者渗入系统内部。授权侵犯，也称为内部威胁，授权用户将其权限用于其他未授权的目的。

（二）植入威胁的主要形式

主要的植入威胁有特洛伊木马、后门。

1. 特洛伊木马

攻击者在正常的软件中隐藏一段用于其他目的的程序，这段隐藏的程序常常以安全攻击作为其最终目标。

2. 后门

后门是在某个系统或某个文件中设置的“机关”，当提供特定的输入数据时允许违反安全策略。

四、病毒

病毒是能够通过修改其他程序而“感染”它们的一种程序，修改后的程序里包含了病毒程序的一个副本，这样就能够继续感染其他程序。编制或者在计算机