第5章 恶意代码的定义及分类

随着计算机的普及和网络的迅速发展，计算机安全问题也随之产生并越来越突出。恶意代码是网络安全问题的主要威胁之一。本章将给出各类恶意代码的定义，并对它们进行简要介绍。

5.1 恶意代码的定义

恶意代码(Malicious Code)是指为达到恶意目的而专门设计的程序或代码，即一切旨在破坏计算机或网络系统可靠性、可用性、安全性和数据完整性或消耗系统资源的恶意程序。


C5.1

恶意代码可能通过软件漏洞、电子邮件、存储媒介或其他方式植入到目标计算机，并随着目标计算机的启动而自动运行。目前发现的恶意代码主要的存在形态是内存代码、可执行程序和动态链接库。

5.2 恶意代码的分类


C5.2

恶意代码可以分为计算机病毒、蠕虫、木马、后门、Rootkit、流氓软件、僵尸(Bot)、Exploit等。在各类恶意代码的具体定义上，部分定义已经约定俗成，并在实践中得到普遍认同，但随着网络及其应用技术的快速发展，恶意代码传播与攻击技术也在不断推进，部分恶意代码的定义也在逐渐发生变化，并出现了新的观点，本节主要从上述的几个类别对恶意代码进行介绍。

5.2.1 计算机病毒

计算机病毒是最常见的恶意代码类型之一。

1984年，计算机病毒的定义由美国计算机病毒研究专家Fred Cohen博士在“Computer Viruses-Theory and Experiments”一文[①]中提出：计算机病毒是一种寄生在其他程序之上，能够自我繁殖，并对寄生体产生破坏的一段可执行代码或程序。计算机病毒的独特感染传播能力使得它可以很快地蔓延，并且常常难以根除。它们能将自身附在各种类型的文件上，

① 具体可访问：Computer Viruses - Theory and Experiments，http://web.eecs.umich.edu/~aprakash/eecs588/handouts/cohen-viruses.html。

当文件被复制或从一个用户传送到另一个用户时,它们就随同文件一同被传播。

我国公安部 2000 年 4 月 26 日发布的《计算机病毒防治管理办法》对计算机病毒也进行了定义:计算机病毒,是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据,影响计算机使用,并能自我复制的一组计算机指令或者程序代码。

可见,计算机病毒与生物病毒一样,有其自身的病毒体(病毒程序)和寄生体(宿主),感染是其主要行为特征。所谓感染或寄生,是指病毒将自身嵌入宿主指令序列中。宿主是合法程序(也可能是操作系统本身),它为病毒提供了生存环境。当病毒程序寄生于合法程序后,病毒就成为程序的一部分,并在程序中占有合法地位。这样合法程序就称为病毒程序的寄生体,或称为病毒程序的载体(宿主)。病毒可以寄生在合法程序的任何位置。病毒程序一旦寄生于合法程序后,就随原合法程序的执行而执行,随它的生存而生存,随它的消失而消失。为增强活力,病毒程序通常寄生于一个或多个被频繁调用的程序中。

计算机病毒技术从其产生发展至今渐渐发生了非常大的变化,如今的计算机病毒结合各类技术向多方面发展,其边界也越来越泛化。

因此,关于计算机病毒定义的另外一种重要观点是,计算机病毒早已突破主机内程序代码感染的局限,而将感染传播目标延伸到其他主机,其已经从程序寄生为主发展为主机寄生为主。如按此观点,下面提到的"漏洞利用类蠕虫与口令破解类蠕虫"之外的其他几类蠕虫都应属于计算机病毒范畴。

5.2.2 网络蠕虫

1982 年,Shoch 和 Hupp 根据 *The Shockwave Rider* 一书中的概念提出了"蠕虫"(Worm)程序的思想,其主要用于寻找空闲主机资源进行分布式计算。这种"蠕虫"程序常驻于一台或多台计算机中,并有自动重新定位的能力。如果它检测到网络中的某台主机未被感染,它就把自身的一个副本发送到那台主机。每个程序都能把自身的副本重新植入另一台主机中,并且能识别那台主机。

这段对蠕虫的描述给出了在当时发展环境下蠕虫最重要的两个特征:"可以从一台计算机移动到另一台计算机",以及"可以自我复制"。但此时人们并未对蠕虫与病毒作出严格区分。

在 1988 年莫里斯蠕虫爆发后,Eugene H. Spafford 在"*The Internet worm program: An analysis*"一文[①]中对蠕虫作出了重新定义以区分计算机病毒和蠕虫,他认为"蠕虫是一类可以独立运行、并能将自身的一个包含所有功能的版本传播到其他计算机上的程序"。而与此对应,他对计算机病毒的定义是"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,需要由宿主程序运行来激活它"。

该定义主要将独立性(即是否可以独立运行、是否为独立个体)作为区分计算机病毒和网络蠕虫的主要依据。按此定义,网络蠕虫又可分为漏洞利用类蠕虫、口令破解类蠕虫、电子邮件类蠕虫、即时通信工具类蠕虫、IRC 类蠕虫、P2P 类蠕虫,以及本地蠕虫(如利用本地复制及可移动存储设备进行传播)等。

① Spafford EH. The Internet worm program: An analysis. Technical Report, CSD-TR-823, West Lafayette: Department of Computer Science, Purdue University, 1988. 1~29.

例如，卡巴斯基对蠕虫进行命名分类[①]时，主要分为 Net-Worm、Email-Worm、IM-Worm、IRC-Worm、P2P-Worm 等，在威胁程度上，Net-Worm ＞ Email-Worm ＞ IM-Worm、IRC-Worm、P2P-Worm。

但是对这些不同类别的蠕虫而言，口令破解类与漏洞利用类蠕虫与其他类别蠕虫在传播特征上存在重大差异，前两者利用系统的缺陷和漏洞进行自主传播，其传播过程不需要计算机使用者进行干预，而其他类别蠕虫在往其他主机传播的过程中都需要计算机使用者的干预（如选择邮件正文或打开附件、单击网址链接、单击文件接收按钮、使用或双击可移动存储设备等），方能在目标主机得到再次执行和继续传播的机会。而是否具备这种主动攻击特征，导致不同的蠕虫在传播特性上存在很大区别，在对应的防护措施上，也存在较大不同。

自莫里斯蠕虫爆发以来，随着各类漏洞的不断爆出，漏洞利用类蠕虫事件不断，如 2001 年红色代码（CodeRed）和尼姆达（Nimda）、2003 年蠕虫王（Slammer）、冲击波（MSBlaster）、2004 年震荡波（Sasser）、2005 年极速波（Zotob）、2006 年魔波（MocBot）、2008 年扫荡波（SaodangBo）、2009 年飞客（Conficker）、2010 年震网（StuxNet）等。2003 年爆发的口令蠕虫则是口令破解类蠕虫的典型代表。

并且，部分蠕虫（如 Slammer，其为 376 字节的 UDP 数据包）仅存在于内存中，其并不产生任何独立的文件，也无法独立运行；如果按照 Spafford 的定义，这部分蠕虫可能还不能归于蠕虫之列。

因此，在计算机病毒与蠕虫的分类上，目前也存在不同的观点。

2003 年，南开大学郑辉博士在其博士论文“Internet 蠕虫研究”[②]中对蠕虫是这样定义的：“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。”他认为，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。2004 年，在此基础之上，中国科学院文伟平博士等在“网络蠕虫研究与进展”一文[③]中，也给出了相应的定义：“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。”

这一观点更加凸显了蠕虫的“攻击主动性”，并且可以将 Slammer 等这类无独立文件、不能独立运行的蠕虫纳入蠕虫范畴。可见，以此观点来看，独立性作为蠕虫区别于计算机病毒的重要依据已经不够准确，而是否需要人工干预来触发执行，是否通过漏洞获取网络中目标计算机的控制权进行自动传播，应当作为区分蠕虫与计算机病毒的重要依据之一。笔者对这一定义也表示认同。

---

① 卡巴斯基对恶意代码进行分类时，其按照威胁程度高低构建了恶意软件分类树（The malware classification tree），并以此制定其命名和分类规则。具体请访问：Types of Malware，http://usa.kaspersky.com/internet-security-center/threats/malware-classifications。

② 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.

③ 文伟平，等.网络蠕虫研究与进展. 软件学报，2004，15(8)：1208-1219.

5.2.3 网络木马

特洛伊木马(Trojan horse)的故事是在古希腊传说中,希腊联军围困特洛伊久攻不下,于是假装撤退,留下一具巨大的中空木马,特洛伊守军不知是计,将木马运进城中作为战利品。夜深人静之际,木马腹中躲藏的希腊士兵打开城门,特洛伊沦陷。

在古希腊传说中,特洛伊木马表面上是"礼物",但实际上藏匿了袭击特洛伊城的希腊士兵。现在,特洛伊木马(以下简称木马)是指表面上有用的软件,实际目的却是危害计算机安全并导致严重破坏的计算机程序,是一种附着在正常应用程序中或者单独存在的一类恶意程序。木马程序通常是目标用户被欺骗后自己触发执行的。与计算机病毒和网络蠕虫相比,木马不能进行自我传播。木马具有隐蔽性和非授权性的特点。

按照木马的行为特征,木马又可以分为多种,如远程控制型木马、信息窃取型木马、破坏型木马等。

卡巴斯基在对木马进行命名分类[①]时,按照木马行为采用 Trojan-Bank、Trojan-DDoS、Trojan-Downloader、Trojan-Dropper、Trojan-FakeAV、Trojan-GameThief、Trojan-IM、Trojan-Ransom、Trojan-SMS、Trojan-Spy、Trojan-Mailfinder、Trojan-ArcBomb、Trojan-Clicker、Trojan-Notifier、Trojan-Proxy、Trojan-PSW 等命名方式,同时将后门、Exploit、Rootkit 进行了单独命名,但依然归在木马之列。其中,远程控制型木马被归为后门。

在所有的木马种类中,远程控制型木马给用户带来的威胁最为巨大。它可以利用网络远程控制位于网络另一端的被植入木马程序的目标计算机,实现对目标计算机的控制、监视和数据窃取。

远程控制型木马一般都有客户端和服务端两个执行程序,其中客户端用于攻击者远程控制已植入木马的计算机,或者获取来自被植入木马的主机的数据,服务端程序就是在用户计算机中的木马程序。通过远程控制型木马,黑客可以远程管理目标主机的文件系统、服务、注册表,也可以进行屏幕控制、摄像头监视、麦克风监听、键盘记录,还可以通过远程 Shell 进行命令操作或进一步植入功能更加强大的第三方恶意软件等。黑客通过远程计算机控制植入木马的计算机,就像使用自己的计算机一样,这对于网络计算机用户来说是极其可怕的。

典型的远程控制型木马有冰河、网络神偷、广外女生、网络公牛、黑洞、上兴、彩虹桥、Posion Ivy、PCShare、灰鸽子、Cobalt Strike Beacon、Galileo RCS 等。

5.2.4 网络后门

后门是指绕过系统中常规安全控制机制而获取对程序或系统访问权限的程序,它按照攻击者自己的意图提供通道。"后门"一般是攻击者在获得目标主机控制权后,为今后能方便地进入该计算机而安装的一类软件。

而广义上的"后门"不仅仅指这一类软件,也可以是软件或操作系统的开发者故意留下的一串特殊操作或口令,甚至可能是一个故意留下来的可被利用的漏洞。一切故意为之的可以使攻击者绕过系统认证机制而直接进入一个系统的方法或手段都可以称为"后门"。

① 具体可访问: What is a Trojan Virus? https://usa.kaspersky.com/internet-security-center/threats/trojans。

最初后门程序通常功能比较简单，随着其功能的日益丰富，其和木马变得非常相似。目前部分安全公司也直接将其与远程控制型木马一起列为木马下的一个子类。

5.2.5　僵尸程序与僵尸网络

僵尸(Bot)程序是 Robot 的缩写，是指实现恶意控制功能的程序代码。僵尸控制服务器通过对大量被植入僵尸程序的计算机进行组织和统一调度，便可以形成僵尸网络。

僵尸网络(Botnet)，是指采用一种或多种传播手段，将大量主机感染僵尸程序，从而在控制者和被感染主机之间所形成的一个一对多控制的网络。攻击者通常利用僵尸网络发起各种恶意行为，如对任何指定主机发起分布式拒绝服务攻击(DDoS)、发送垃圾邮件(Spam)、获取机密、滥用资源等。传统的恶意代码有后门工具、网络蠕虫和特洛伊木马等，僵尸网络来源于传统恶意代码，但又具有自身的特点。

僵尸网络的发展一般经历传播、加入和控制 3 个阶段，通过这 3 个阶段，僵尸程序会根据中心服务器的控制命令下载、更新僵尸样本。正因为僵尸网络能随时更新样本，僵尸程序能够保持良好的健壮性。

僵尸网络中心服务器通过命令与控制通道对网络内的僵尸主机进行控制，僵尸程序分类方法比较多样，但是一般以命令与控制机制作为分类标准。当前，僵尸网络的命令与控制机制主要有 3 种：基于 IRC 协议的命令与控制机制、基于 HTTP 的命令与控制机制和基于 P2P 协议的命令与控制机制。基于 IRC 协议和基于 HTTP 的命令与控制机制是 C/S 模式，存在一个集中控制服务器，并通过该服务器向网络内的各僵尸主机发送命令；基于 P2P 协议的命令与控制机制采用的是点对点的对等模式，网络内的各僵尸主机均可以作为僵尸网络的中心服务器。

5.2.6　Rootkit

Rootkit 是 20 世纪 90 年代出现的一种计算机技术。它最初被定义为由有用的小程序组成的工具包，可使得攻击者能够保持访问计算机上具有最高权限的用户“root”。从目前的发展看，Rootkit 是能够持久或可靠地、无法被检测地存在于计算机上的一组程序或代码。

Rootkit 技术的关键在于“使得目标对象无法被检测”，因此 Rootkit 所采用的大部分技术和技巧都用于在计算机上隐藏代码和数据。正因为 Rootkit 在隐藏上有如此优势，近些年很多木马程序纷纷利用 Rootkit 技术达到文件隐藏、进程隐藏、注册表隐藏、端口隐藏的目的。

最早的 Rootkit 产生于 UNIX 平台，随着 Windows 的普及，现在 Rootkit 在 Windows 平台上发展迅猛。Rootkit 分为用户模式 Rootkit 和内核模式 Rootkit。相比于用户模式的 Rootkit，基于内核模式 Rootkit 技术的恶意代码运行在操作系统的 Kernel Mode 下，可以进行所有权限的操作，所以对计算机安全构成更大的威胁。

5.2.7　Exploit

Exploit(漏洞利用程序)是针对某一特定漏洞或一组漏洞而精心编写的漏洞利用程序。通过精心构造的 Exploit，其可以触发目标系统的特定漏洞，从而获得目标系统的控制权，或者形成对目标程序或系统的拒绝服务。

目前,比较常见的 Exploit 如下。

主机系统漏洞 Exploit:针对目标主机系统,直接获取目标系统的控制权,如 MS03026(DCOMRPC 漏洞)漏洞利用程序,MS04011 等各类系统漏洞。这类漏洞利用程序通常可以给攻击者提供一个 Shell(正向或反向)、增加一个高权限系统账号、下载执行一个指定的恶意程序等。

文档类漏洞 Exploit:其通过利用数据文档编辑或阅读软件(如 MS Office、Adobe Acrobat Reader 等)的漏洞,将恶意程序与正常文档进行捆绑,生成一个恶意的文档文件。当目标用户使用带有漏洞的文档编辑或阅读软件打开时,则会触发漏洞,导致攻击代码获得控制权,进而可能进一步危害到系统的控制权。目前,比较常见的被利用文档类型包括 PDF、WRI、DOC、XLS、PPT 等。这类 Exploit 通常可以用来释放一个捆绑在文档中的恶意程序,或一个可以下载更强大功能恶意程序的一个恶意下载执行程序。

网页挂马类 Exploit:其主要利用当前浏览器或相关系统组件的漏洞,在网页文件中嵌入精心设计的 Exploit,当目标用户利用带有漏洞的浏览器打开这类挂马网页后,Exploit 被触发,将导致目标浏览器自动下载和执行指定的恶意软件。

除此之外,由于漏洞本身或者攻击者本身的技术原因,部分 Exploit 可能仅造成拒绝服务的效果,或虽然无法获得控制权,但可以改变或获取目标进程中的部分数据。

5.2.8 其他

在互联网上也会经常遇到其他一些类别的恶意程序,如下面介绍的几种。

勒索软件:通过加密用户数据资源或破坏系统功能,对用户进行钱财勒索的一类恶意程序。

挖矿软件:在目标系统进行非授权挖矿来获取虚拟货币盈利的一类恶意程序。

恶意广告软件(Adware):是指未经用户允许,下载并安装或与其他软件捆绑通过弹出式广告或以其他形式进行商业广告宣传的程序。

逻辑炸弹(Logic Bomb):它是合法的应用程序,只是在编程时被故意写入的某种“恶意功能”。例如,作为某种版权保护方案,某个应用程序有可能会运行几次后就在硬盘中将其自身删除。

黑客工具(Hack Tool):各类直接或间接用于网络和主机渗透的软件,如各类扫描器、后门植入工具、密码嗅探器、权限提升工具。

玩笑程序(Joke Program):其并不是恶意的,但它会改变或打断计算机的正常行为,一般会创建一个令人分心或令人讨厌的东西。


C5.3

5.3 恶意代码的发展阶段

5.3.1 单机阶段

在单机阶段,恶意代码主要以引导区病毒和文件感染型病毒为主,目标操作系统则主要聚焦在 DOS 操作系统。例如,全球第一款计算机病毒为引导区病毒 C-BRAIN(也称巴基斯坦智囊病毒),其寄生在磁盘主引导扇区,原本用意是保护以软磁盘为载体的软件版权。而

我国第一款计算机病毒为引导型病毒——小球病毒，病毒发作现象表现为一个小球在屏幕上不断地跳动和反弹，其感染技术是通过挂钩磁盘文件读写中断，在出现文件访问时进行代码寄生。

这一阶段的病毒感染方式单一，以寄生在磁盘引导区和目标 HOST 文件为主要技术手段，而传播扩散方式则主要依赖磁盘传播媒介（光盘、磁盘）。

这一时期的反病毒检测技术以特征值检测法为主，我国早期的反病毒厂商包括江民、金山、瑞星、北信源等。

5.3.2　网络传播阶段

随着互联网的普及，恶意代码的编写者开始利用网络的广泛连接性，使得恶意代码的传播速度和范围大大增加。这一时期，恶意代码的编写技术也在不断进步，开始出现能够自我复制和传播的复杂恶意软件。

并且在网络通信变得便捷后，开始出现很多自身并不具备自我复制与传播功能的恶意代码，这类恶意代码选择使用其他方式进行目标侵入，如网页挂马、文档捆绑等。它们因为自身没有传播能力，所以既不属于计算机病毒，也不属于网络蠕虫。这类典型的恶意代码有：网络木马、后门、僵尸、勒索软件、挖矿软件等。当然，复合型的恶意代码也在不断出现，如 Wannacry，其既可以通过漏洞进行自我传播，同时也具有勒索软件的功能。

随着技术的进步和黑客手段的不断演变，恶意代码的发展进入新的阶段。在这个阶段，恶意软件变得更加复杂和隐蔽，它们不仅具备自我复制和传播的能力，还开始利用操作系统和应用软件的漏洞进行攻击，甚至能够结束或绕过传统的安全防护措施。例如，求职信病毒利用 eml 漏洞进行自动触发，并能够直接结束反病毒软件。

还有一种显著的变化是，恶意代码开始向多态化和变形技术方向发展。这意味着每次恶意软件被检测到并被安全软件识别后，其编写者会迅速修改代码，甚至让恶意软件在每次传播时都改变自身，使其以不同的形式出现，从而避免被现有的防病毒软件识别。这种技术的出现，使得恶意软件的检测和防御变得更加困难。

随着对抗的持续升级，安全专家开始意识到，仅仅依靠传统的防病毒软件已经不足以应对日益复杂的网络安全威胁。因此，安全社区开始研究更为先进的防御机制，如行为监测、启发式分析等技术，以期能够更有效地检测和防御新型恶意代码。

5.3.3　混合攻击与对抗阶段

此外，随着云计算、物联网等新兴技术的兴起，恶意代码也开始向这些领域渗透。例如，针对云计算平台的攻击，恶意代码可能通过篡改云服务提供商的数据中心，窃取敏感信息或破坏服务；而在物联网领域，恶意代码可能通过控制智能家居设备、工业控制系统等，造成物理世界的破坏或损失，典型如 Mirai 蠕虫等。

为应对这些新的挑战，安全社区需要不断加强研究和创新。一方面，安全社区开始致力于提升防病毒软件的智能化水平，通过机器学习、人工智能等技术，实现对恶意代码的快速识别和拦截，同时还借助大数据、威胁情报等进行关联分析，推出 SIEM、EDR/XDR 等更加综合性的威胁检测系统，及时有效遏制了恶意软件的传播和破坏；另一方面，他们也积极推动网络安全标准和规范的制定，加强网络安全意识和教育，提高用户和企业对恶意代码的防范能力。

总之,恶意代码的发展历史是一个不断演进和变化的过程。随着技术的不断进步和黑客手段的日益复杂,我们需要保持警惕和创新精神,不断提升网络安全防护能力,确保网络空间的安全和稳定。


C5.4

5.4 恶意代码与网络犯罪

恶意代码与网络犯罪的快速发展对信息安全领域提出了新的挑战,也对掌握安全技术的人员提出了更高的法律与道德要求。对于信息安全专业的学生而言,随着专业知识的不断深入,编写软件或控制计算机系统的技术难度逐渐降低。然而,这种技术的易得性和操作的简便性也可能诱发滥用,甚至导致非法行为。因此,技术的使用必须受到法律约束,避免因追求利益或炫技而触犯法律,造成不可挽回的后果。

在我国早期的刑法中,针对计算机犯罪的打击力度较弱。根据《中华人民共和国刑法》(简称《刑法》)第 285 条第一款规定:“违反国家规定,侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的,处三年以下有期徒刑或者拘役。”该条款主要针对涉及国家安全和核心领域的信息系统,为此类系统提供更高层级的法律保护。然而,这一规定无法涵盖普通计算机信息系统的入侵或控制行为,也未能有效遏制病毒传播与恶意攻击的泛滥。例如,早期曾有黑客公然出售木马程序,而法律对此束手无策。

为完善法律体系,2009 年《中华人民共和国刑法修正案(七)》在第二百八十五条下新增第二款内容,将法律保护范围扩展到更广泛的计算机信息系统。第二款规定:“违反国家规定,侵入前款规定以外的计算机信息系统或者采用其他技术手段,获取该计算机信息系统中存储、处理或者传输的数据,或者对该计算机信息系统实施非法控制,情节严重的,处三年以下有期徒刑或者拘役,并处或者单处罚金;情节特别严重的,处三年以上七年以下有期徒刑,并处罚金。”这一规定有效打击了非法侵入计算机信息系统、非法获取数据以及非法控制系统等行为,使普通信息系统的安全得到法律保障。

此外,第二百八十五条第三款进一步明确了对工具提供者的惩罚:“提供专门用于侵入、非法控制计算机信息系统的程序、工具,或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具,情节严重的,依照前款的规定处罚。”这一条款将违法行为的处罚范围扩大到帮助犯罪实施的行为,对提供侵入工具的个人或单位施加同等刑责,强化了对犯罪工具传播的法律控制。

与第二百八十五条相对应,《刑法》第二百八十六条第三款对计算机破坏性程序的制作和传播作出了明确规定:“故意制作、传播计算机病毒等破坏性程序,影响计算机系统正常运行,后果严重的,依照第一款的规定处罚”。该条款不仅针对传统意义上的病毒程序,还在后续司法解释中进行了明确,将木马程序等虽然不能自我传播但具备破坏性的程序纳入处罚范畴,进一步强化了对恶意代码的打击力度。

2011 年,最高人民法院与最高人民检察院进一步出台司法解释,即《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》,细化了“情节严重”和“情节特别严重”的认定标准,即

第一条 非法获取计算机信息系统数据或者非法控制计算机信息系统,具有下列情形之

一的，应当认定为刑法第二百八十五条第二款规定的“情节严重”：

（一）获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的；

（二）获取第（一）项以外的身份认证信息五百组以上的；

（三）非法控制计算机信息系统二十台以上的；

（四）违法所得五千元以上或者造成经济损失一万元以上的；

（五）其他情节严重的情形。

实施前款规定行为，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节特别严重”：

（一）数量或者数额达到前款第（一）项至第（四）项规定标准五倍以上的；

（二）其他情节特别严重的情形。

明知是他人非法控制的计算机信息系统，而对该计算机信息系统的控制权加以利用的，依照前两款的规定定罪处罚。

从中可以看出，非法获取 10 组以上支付结算或金融交易身份信息，500 组以上其他身份认证信息，非法控制 20 台以上计算机，违法所得 5000 元以上，或造成 1 万元以上经济损失的行为均被认定为情节严重。而上述标准的 5 倍，即获取 50 组以上金融身份信息、2500 组以上普通身份认证信息，或控制 100 台以上计算机等情形，则被认定为情节特别严重。此外，恶意代码的定义也得到了扩展，木马程序等虽然不具备病毒的自传播性，但因其破坏性和隐蔽性，同样被纳入法律规制范围。

这些法律的完善不仅为打击网络犯罪提供了有力依据，也对网络安全领域的从业者和学习者提出了警示。技术是一把双刃剑，合理使用能够保护信息安全，滥用则可能导致法律制裁和道德谴责。现实中，恶意代码滥用的案例屡见不鲜。例如，“熊猫烧香”病毒的编写者，因编写病毒牟利被判刑入狱。其病毒图标形象鲜明，传播广泛，最终因对信息系统造成巨大破坏而引发社会广泛关注。

在当前互联网环境下，网络攻击和信息窃取手段层出不穷，而违法成本却相对较低，作为网络空间安全领域的学习者和从业者，技术能力与法律意识缺一不可。一方面，我们要树立服务国家网络安全战略，不断增强保护国家、社会及个人信息安全的使命感与责任感，维护网络空间的安全与秩序；另一方面，我们还必须时刻保持警觉，遵循法律规定，避免因一时疏忽而触犯国家法律。

5.5　恶意代码与 APT 攻击中的武器

5.5.1　从恶意代码的发展看 APT 攻击


C5.5.1

在 20 世纪八九十年代，计算机病毒主要以 DOS 平台下的简单恶意代码为代表。这些病毒的编写动机多种多样，既有恶意破坏，也有炫技展示。然而，随着 DOS 病毒数量的不断增长，反病毒引擎也在不断完善升级并逐渐成熟，成为早期安全防御体系的核心，并引领了安全技术的发展方向。进入 20 世纪 90 年代中后期，信息高速公路的建设促进了网络互联互通，同时也为蠕虫病毒的大规模传播提供了土壤。21 世纪初，蠕虫作为恶意代码的重要形态，在短时间内迅速流行，推动了网络侧恶意代码监测技术的成熟，并催生了 UTM、NG-

FW 和 NTA 等一系列安全产品。

随着信息社会的快速发展和信息资产价值的显著增加,恶意代码的动机从单纯的技术探索逐渐转向经济利益驱动。从 2006 年开始,特洛伊木马数量急剧膨胀,这种数量级的增长使得依赖人工分析的恶意代码对抗模式难以为继,迫使安全厂商构建大规模自动化分析体系,以应对海量恶意代码带来的安全挑战。在反病毒引擎、端点防护、流量监测以及后端自动化分析技术逐步成熟的背景下,安全行业开始面临更为复杂和严峻的安全威胁,其中高级持续性威胁(Advanced Persistent Threat,APT)攻击成为关注的焦点。

典型的 APT 攻击案例——方程式组织对中东 Eastnets 金融机构的攻击过程,展现了其复杂性与隐蔽性。攻击者通过互联网 4 个跳板发动攻击,逐步击穿两层防火墙,并在防火墙上预置 Rootkit,随后利用多个 0-day 漏洞深入内网,成功控制多台业务服务器,并通过 SQL 查询提取账户名、密码和交易数据。这一过程不仅涉及多层渗透和漏洞利用,还依赖高效的插件式攻击平台和深度持久化木马组件,充分体现了 APT 攻击的高技术水平和战略意图。

APT 这一概念最早由美国空军信息作战中心于 2006 年提出,用于描述具备高级能力和持续作业意图的网络攻击者。“A”代表攻击者的能力,强调其技术水平与攻击工具的复杂性;“P”强调攻击的持续性,反映出攻击者在时间和资源上的长期投入;“T”则指威胁本身,体现出能力与意图的结合所带来的危害性。在 APT 攻击分析中,攻击者的意图往往是判断其性质与威胁等级的关键因素,即便攻击工具和技术手段并非总是处于高级水平,其战略目标和持续渗透能力仍然构成重大威胁。

表 5-1　不同层级的安全威胁

等级	攻　击　者	攻 击 目 的	攻击能力与资源
0 级	业余攻击者、业余内部泄密者	无特定目的	公开攻击技术与工具
1 级	黑产组织、有专业背景的内部泄密者	受商业利益驱动	公开攻击技术、工具与平台,部分专有攻击技术、工具与平台
2 级	网络犯罪团伙或黑客组织	受商业利益驱动,也可能受意识形态驱动,敢于造成较大破坏或影响	专有攻击技术、工具与平台,漏洞挖掘与利用技术开发能力
3 级	网络恐怖组织	受意识形态驱动,寻求破坏或影响的最大化	专有攻击技术、工具与平台,漏洞挖掘与利用技术开发能力,掌握少量 0-day 漏洞
4 级	一般能力国家/地区行为体	受国家/地区利益驱动,网络间谍与网络战一体化,寻求通过网络战获得政治、经济、军事优势	部分掌握自身国家/地区级网络基础设施的控制,专有攻击技术、工具与平台,具有漏洞挖掘与利用技术开发能力,掌握少量 0-day 漏洞
5 级	高级能力国家/地区行为体	受国家/地区利益驱动,网络间谍与网络战一体化,寻求通过网络战获得政治、经济、军事优势	部分掌握自身国家/地区级网络基础设施和外部国家/地区级网络基础设施的控制,专有攻击技术、工具与平台,跨维度高度集成的攻击利用手段,漏洞挖掘与利用技术开发能力,掌握较多 0-day 漏洞