第3章 终端安全威胁

随着互联网的普及和新技术、新业务的快速发展与应用，终端作为信息系统中重要组成部分所面临的安全问题日益复杂。这些安全问题的来源多种多样，有终端所处的周边环境带来的威胁，也有终端自身硬件、软件的缺陷带来的隐患，还包括终端所处的网络环境带来的网络安全威胁。因此，了解终端面临的安全威胁是十分必要的。

3.1 环境方面的安全威胁

3.1.1 自然灾害

自然灾害是由于自然因素造成的人类生命、财产、社会功能和生态环境等受损害的事件或现象。在由大气圈、岩石圈、水圈、生物圈共同组成的地球上，人类生存的周边环境时刻在变化，当这种变化给人类社会带来危害时，就构成自然灾害。重大的突发性自然灾害包括旱灾、洪涝、台风、风暴潮、冻害、雹灾、海啸、地震、火山、滑坡、泥石流、森林火灾、农林病虫害、宇宙辐射、赤潮等。

中国常见的自然灾害种类繁多，主要包括以下几类：洪涝、干旱、台风、冰雹、暴雪、沙尘暴等气象灾害；火山、地震、山体崩塌、滑坡、泥石流等地质灾害；风暴潮、海啸等海洋灾害；森林草原火灾；重大生物灾害；等等。图 3-1 所示的 2008 年在我国南方发生的冰灾就是其中一种。

图 3-1　2008 年发生于我国南方的冰灾

自然灾害的特点归结起来主要表现在 6 个方面：

(1) 自然灾害具有广泛性与区域性。一方面，自然灾害的分布范围广。处于自然环境中，无论是海洋还是陆地，地上还是地下，平原还是山地，自然灾害都有可能发生，并不以是否有人类活动为转移。另一方面，自然地理环境的区域性又决定了自然灾害的区域性，例如，在多山、多雨的地区容易发生山洪、滑坡等自然灾害。区域性的气候也会导致灾害发生，例如，我国冬季西北地区多雪灾，夏季南方地区多洪水。

(2) 自然灾害具有频繁性和不确定性。例如，我国华北地区、青藏高原地区、四川盆地都属于典型的地震带，自 20 世纪以来，共发生 6 级以上地震 700 余次，地震灾害频繁发生。而 2008 年在我国南方发生的突发性冰冻天气灾害在南方是很罕见的自然灾害。

(3) 自然灾害具有一定的周期性和不重复性。主要自然灾害中的地震、干旱、洪水、台风等灾害的发生都呈现出一定的周期性。通常描述某种自然灾害达到“十年一遇”或“百年一遇”的说法，就是对自然灾害周期性的一种通俗描述。自然灾害的不重复性主要是指灾害过程、损害结果的不重复性，这主要因为自然灾害受很多不确定因素影响，这些因素所引发的“蝴蝶效应”是无法重现的。

(4)自然灾害具有关联性。自然灾害的关联性表现在两个方面。一方面是区域之间具有关联性。例如，南美洲西海岸发生的厄尔尼诺现象就以一定的概率表明全球气候会发生紊乱；美国排放的污染物至少有 60％的概率会在加拿大境内形成酸雨。另一方面是灾害之间具有关联性。也就是说，某些自然灾害可以互为条件，形成灾害群或灾害链。例如，火山活动就是一个灾害群或灾害链，火山活动可以导致地震、泥石流、大气污染、海啸等一系列灾害。灾害链中最早发生的、起作用的灾害称为原生灾害，而由原生灾害所诱导而发生的灾害则称为次生灾害，自然灾害发生之后产生的一系列其他灾害泛称为衍生灾害。

(5) 自然灾害所造成的危害具有严重性。例如，全球每年发生可记录的地震约 500 万次，其中有感地震约 5 万次，造成破坏的近千次，而里氏 7 级以上、足以造成惨重损失的强烈地震每年约发生 15 次；干旱、洪涝两种灾害造成的经济损失也十分严重，全球每年因此遭受的损失可达数百亿美元。

(6) 自然灾害具有不可避免性和可减轻性。自然灾害不可能消失，是不可避免的。随着科技的发展，人类可以在越来越广阔的范围内进行防灾减灾，通过采取避害趋利、除害兴利、化害为利、害中求利等措施，最大限度地减轻灾害损失。

由于信息系统的终端所处的地点不可避免地处于自然的大环境之中，因此由自然环境中的自然灾害引发的安全威胁不可避免。由于自然灾害的不确定性，其安全威胁具有低概率、高损失的特点，即遭受自然灾害的概率通常很小，但一旦发生，造成的损失非常巨大。

3.1.2　运行环境中的安全威胁

终端运行环境中蕴含的安全威胁包括技术因素和人为因素。

1. 技术因素

终端运行环境中的安全威胁的技术因素主要指由于终端所处的环境以及组成终端的软

硬件引发的故障，或终端周边的电子元器件因缺陷、使用寿命等原因而带来的安全威胁。

如果一个机房无法实现对温度的调节，终端运行产生的热量无法有效排除，当温度超过终端可以承受的限度时，宕机、蓝屏的风险就会大大提高。不当的或者恶劣的使用环境同样威胁着计算机终端的物理安全。例如，在计算机终端中广泛使用的机械硬盘，其读取、存储数据的过程是由一组机械磁头装置读取、更改磁盘扇区上的磁极信息（N 极或 S 极），磁盘的旋转速度非常快（常见的硬盘转速为 5400 转/分、7200 转/分等），如果硬盘在读写过程中由于某些原因发生震动，磁头与盘面发生物理接触，就会引发磁头和磁盘的物理损伤，从而导致硬盘出现无法存取数据、数据损坏等情况。

终端的硬件包括主板、内存、硬盘、风扇等。这些硬件通常都由各类集成电路和芯片组成。随着电子技术的发展，集成电路的工艺水平和使用寿命得以大幅度提高，构成计算机终端的各种元器件的性能和寿命也都得到很大提高。尽管在电子产品的生产过程中可以通过良品率来控制产品质量，但由于电子产品的高度集成化和复杂的工艺环境，在实际使用过程中，还是会有一定概率出现产品失效，引发计算机终端失效或部分失效，如图 3-2 所示。在 2018 年 4 月，由于气体火灾报警系统释放灭火气体，导致瑞典 Digiplex 数据中心磁盘损坏，引发近 1/3 的服务器意外关机，进而中断了整个北欧范围内的美国证券交易商协会（National Association of Securities Dealers Automated Quotations，NASDAQ）业务，这是一起典型的由运行环境造成的安全事件。

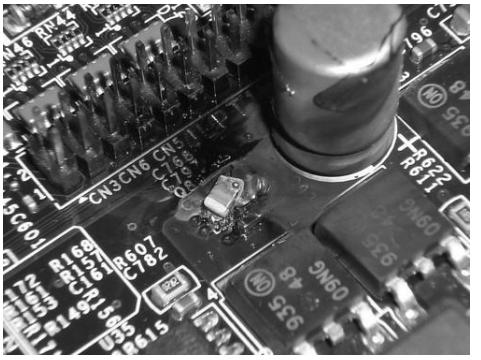

图 3-2　主板电子元器件损坏

电磁泄漏是电子设备无法避免的电磁学现象。由于终端设备工作时使用的模拟或数字信息的变化会引起电流、电压的变化，从而产生电磁泄漏，由此导致的 CPU 功率变化示例如图 3-3 所示。任何处于工作状态的电子设备都会或多或少地产生电磁泄漏。在电磁泄漏研究中，“红信号”是指与敏感信息有关的电信号，其他信号称为黑信号。

电磁信号一般通过两种方式泄漏：一种是以电磁波的方式向周围空间辐射，称为辐射泄漏，这是由终端内部的电子电路、线缆等产生的；另一种是电磁能量通过传导线路传递，称为传导泄漏。利用特殊的电子装置捕获泄漏的电磁辐射或电磁能量，通过特定的算法转换就可以还原传输的数据，从而造成信息泄漏。侧信道攻击（又称边信道攻击）就是针对加密电子设备在运行过程中的时间消耗、功率消耗或电磁辐射对加密设备进行攻击的方法，由此可以获取终端相关的密钥、信息，给终端带来安全威胁。图 3-4 为 2016 年 2

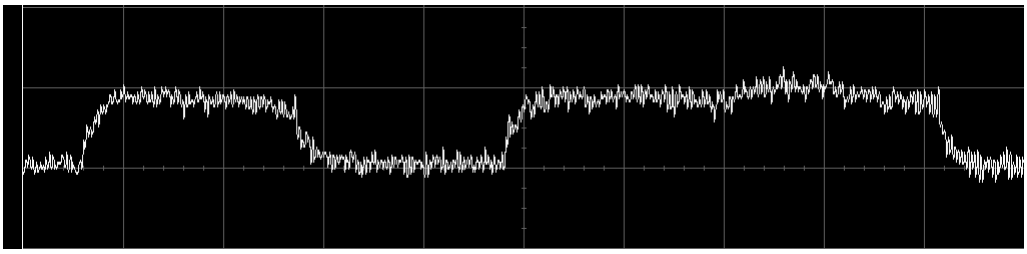

图 3-3　CPU 功率变化示例

月以色列特拉维夫大学和以色列理工学院利用侧信道攻击技术对隔壁房间中运行的笔记本电脑进行攻击的实验环境。

图 3-4　侧信道攻击实验环境

侧信道攻击技术发不仅可以用于攻击计算机终端，还可以攻击很多设备。在 2017 年 7 月 28 日在美国拉斯维加斯举行的 Black Hat 2017 安全会议上，阿里巴巴公司安全部门的研究人员演示了用声音和超声波攻击智能设备的技术（本质上属于一种结合了侧信道攻击的故障攻击方法），包括大疆无人机、iPhone 7、三星 Galaxy S7、虚拟现实显示器等产品均可被攻击和劫持。

由于电磁现象而引起的设备、传输通道或系统性能的下降称为电磁干扰（Electromagnetic Interference，EMI）。电磁干扰是人们早就发现的电磁现象，它几乎和电磁效应的现象同时被发现。

电磁干扰分为传导干扰和辐射干扰两种。传导干扰是指通过导电介质把一个电网络中的信号耦合到另一个电网络中。辐射干扰是指干扰源通过空间把其信号耦合到另一个电网络中。在高速印制电路板设计中，高频信号线、集成电路的引脚、各类接插件等都可能成为具有天线特性的辐射干扰源，能够发射电磁波并影响其他系统或本系统内其他子系统的正常工作。

一般来说，电磁干扰源分为两大类：自然干扰源与人为干扰源。

自然干扰源主要来源于大气层的天电噪声、地球外层空间的宇宙噪声，例如闪电、静电放电、日冕物质喷射都会产生干扰噪声。它们既是地球电磁环境的基本组成部分，同时又是对无线电通信和空间技术造成干扰的电磁干扰源。自然噪声会对通信网络的运行产生干扰，也会对电力网络产生干扰。

人为干扰源是能产生电磁能量干扰的机电或其他人工装置。其中一部分是专门用来发射电磁能量的装置，例如广播、电视、通信塔、雷达站和导航台等无线电设备，这些称为

有意发射干扰源；另一部分是在完成自身功能的同时附带产生电磁能量的发射，如交通车辆、架空输电线、照明器具、电动机械、家用电器以及工业、医用射频设备等，这些称为无意发射干扰源。

电磁干扰与电磁泄漏产生的后果不同。前者的影响是造成敏感设备的性能降低，甚至引发元器件损坏而使之无法工作，危害设备的物理安全；后者则造成源设备信息外泄，破坏信息的机密性，危害信息安全。

2. 人为因素

人员作为信息系统的使用者、管理者，是信息系统管理不可分割的重要组成部分。一方面人员是企事业单位的重要资产；另一方面人员也是信息系统最大的威胁来源，甚至从某些角度来说，人为因素给信息系统带来的安全威胁超过其他因素造成的安全威胁。例如，信息系统的运维人员没有定期对机房中的 UPS(Uninterruptible Power Supply，不间断电源)进行巡检，导致 UPS 系统中的电池漏液，引发火灾，使信息系统终端被毁；运维人员对信息系统电力供应配电盘配置不熟悉，导致信息系统意外断电，致使信息系统对外服务中断；为了获取地下埋藏的自然资源(例如地下水、矿产)，利用工程机械采挖自然资源，导致地质结构被破坏，引发地表塌陷，造成环境安全威胁。

3.2 存储介质方面的安全威胁

3.2.1 来自固定存储介质的安全威胁

如果对固定存储介质(如固定硬盘、磁带、光盘等)的存放环境、使用、维护和销毁等方面没有合理、完善的处置方式，在介质处置过程中，可能由于处置不当导致介质损伤、灭失、数据泄漏等安全威胁。例如，将存储重要数据的介质带出工作环境，因保管不善，导致介质损伤或丢失；由于介质的组成材料不尽相同，使用寿命也各不相同，对达到使用寿命的介质进行报废、销毁时，如果没有对介质进行专门的数据擦除处理，那么利用专业数据恢复设备甚至是常用的数据恢复软件就可以对介质中残留的数据进行恢复，就有信息泄漏的可能性，如图 3-5 所示。

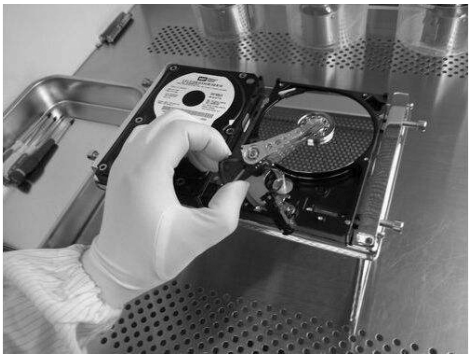

图 3-5　硬盘数据恢复

3.2.2　来自移动存储介质的安全威胁

由于终端对移动存储介质接入缺乏管控手段，终端中存储的敏感数据可以随意被复制，造成敏感数据泄漏。同时，由于缺乏相关的审核功能，无法通过操作记录、访问记录等进行责任追查。而且移动存储介质携带便利、使用方便，极易在安全性未知的使用环境中感染病毒、木马。当携带恶意代码的移动存储介质接入内网终端时，对内网会造成极大的安全隐患。移动存储介质带来的威胁主要表现在以下几个方面：

(1) 无法保护终端数据私密性。由于普通 U 盘、移动硬盘是不受管控的存储介质，没有任何措施可以保证 U 盘、移动硬盘在可控的环境下使用，即 U 盘、移动硬盘可以不受控地在任何计算机上使用，这样，当员工在使用 U 盘、移动硬盘处理终端和相关业务数据时，就可能造成企业数据的无意外泄，或者员工故意窃取数据，而组织和管理者无法获知的情况。

(2) 无法保护移动存储介质数据的私密性和完整性。由于移动存储介质可能是一个不受保护的存储介质，对数据的访问并不会进行身份验证，数据也未进行加密处理。所以，在移动存储介质丢失、被他人冒用或被病毒、木马感染的情况下，容易造成其中保存的数据泄露、被篡改、丢失或损坏的情况。

(3) 容易造成内部病毒、木马传播。由于移动存储介质在内部网络、外部网络混用的情况非常普遍，移动存储介质极易成为病毒等恶意代码的载体。一旦将 U 盘、移动硬盘插入到其他计算机上，就极有可能造成计算机感染病毒，从而引发整个网络的病毒蔓延，造成系统损坏、数据丢失、死机，甚至网络瘫痪。

(4) 对于数据泄露的安全事件无法追踪。普通 U 盘、移动硬盘无论是在内网还是在互联网上使用，都无法对其进行有效的审核和取证。

(5) 容易成为某些特定攻击的载体。通过对 USB 设备的内部微控制器、USB 设备的固件等进行重新编程的方式，可以实施攻击，执行恶意动作，甚至可以通过 USB 触发电力过载，破坏终端设备。

在 2014 年美国黑帽大会上，柏林 SRLabs 的安全研究人员 JakobLell 和独立安全研究人员 Karsten Nohl 展示了称为 BadUSB(按照 BadBIOS 命名)的攻击方法，这种攻击方法让终端和与 USB 相关的设备(包括具有 USB 接口的计算机)都陷入了相当危险的状态。BadUSB 模拟键盘和鼠标的操作，通过执行特定的命令对主机进行操作，实现对主机的攻击，所以常规的防病毒软件无法防范其攻击行为。

BadUSB 主要依靠 USB 驱动器的构建方式进行攻击。USB 通常有一个大容量的可重写的存储芯片用于实际的数据存储，还有一个独立的控制器芯片负责与 PC 的通信和识别，如图 3-6 所示。控制芯片实际上是一个低功耗计算机，并且与笔记本电脑或台式机一样，它通过从存储芯片加载基本的引导程序来启动，类似于笔记本电脑的硬盘驱动器包含的主引导记录。闪存中有一部分区域是控制器固件，它的作用类似于操作系统，用于控制软硬件交互。固件无法通过普通手段读取。

BadUSB 对 U 盘的固件进行逆向重新编程，相当于改写了 U 盘的操作系统，进而发动攻击。

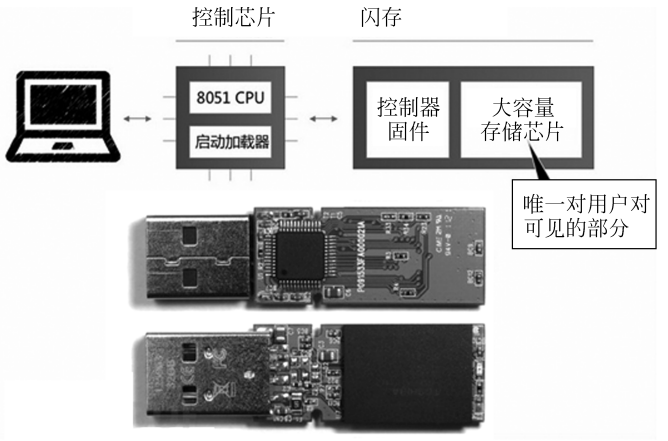

图 3-6　BadUSB 硬件架构

为什么重写固件即可实现进行攻击？这主要是因为 USB 协议中存在安全漏洞。

由于 USB 设备种类很多，例如音视频设备、摄像头等，因此要求操作系统提供最大程度的驱动程序兼容性，甚至免驱动程序使用。所以，在设计 USB 标准的时候，并没有要求每个 USB 设备像网络设备一样使用一个可识别的唯一 MAC 地址进行验证，而是允许一个 USB 设备具有多个输入输出设备的特征。这样，就可以通过重写 U 盘固件，将其伪装成一个 USB 键盘，并通过输入到 U 盘固件中的指令和代码进行攻击。

2018 年，IBM 公司发布了禁止全球所有员工使用可移动存储设备的公告，IBM 公司做出该决策的原因是“必须将错放、丢失或遭滥用的可移动便携式存储设备所带来的经济损失和名誉损失最小化”。由此可见，移动存储设备对组织机构安全有很大影响。

3.3 设备方面的安全威胁

由外部设备引发的安全威胁也是不容小觑的。信息系统中各种各样的外部设备都可能引发安全方面的问题。例如，笔记本电脑通常都配有摄像头，如果摄像头被远程控制，笔记本电脑使用者及其所在周边环境都可被控制者观察、记录下来。假设笔记本电脑使用者参加某个涉及商业秘密的会议，而摄像头面向的是涉密数据内容，可以想见会对数据安全和企业造成多大威胁。

在办公中不可或缺的打印机也有可能引发安全威胁。例如，在打印过程中，打印机周围的其他人员有可能会看到打印的内容，从而造成泄密；硒鼓在打印后，由于硒鼓表面的静电残留，打印的内容会残留在硒鼓表面，通过分析静电残留成像就可以恢复打印的内容，从而造成泄密；打印机通常都安装了内部存储器，用于存储打印任务的数据，只有新的打印数据进入后才会覆盖原有内容，在存储器更换或报废时，如果存储器中包含敏感数据，通过读取存储器中的内容就会造成泄密；网络打印机通过网络接收打印任务和打印内容，如果在这个过程中攻击者监听传入打印机的网络数据，或者打印机被病毒感染，通过网络将打印数据传输到外部网络攻击者指定的位置，都会造成数据泄密。

在海湾战争期间，美国利用打印机内嵌的病毒程序感染伊拉克连接打印机的终端，从而造成终端所在的信息系统失效，这是通过外部设备对终端进行篡改和破坏的典型案例。

扫描仪与打印机的安全威胁相似，在扫描敏感数据时，如果周边有其他人员，可能会造成敏感信息被窥视；敏感数据扫描后存储在扫描仪的存储器中，在存储器更换或报废时也会造成信息泄露。

键盘是终端非常重要的输入设备，任何与终端交互的信息，包括用户名、口令都需要通过键盘输入。2017 年曝光了某品牌的音频驱动程序中包含内置键盘记录器，会监控用户的所有按键输入。虽然该功能用于测试快捷键的有效性，但会在调试日志中记录所有的按键动作，导致用户的按键记录被日志文件留存。如果日志文件被恶意使用，就会引发安全威胁。

3.4　网络方面的安全威胁

3.4.1　非法终端

对于企业隔离内网用户，各类安全事件表明网络堡垒往往是从内部被攻破的。开放式的网络使得企业内部任何一个人都能够通过便携设备随意接入企业核心业务网络，访问企业的各种网络资源。如果携带恶意程序的终端一旦接入网络，随之而来的结果就是堡垒由内部被攻破。开放式的网络犹如企业没有门卫一样，任何人都可以随便进出，不受任何检查和限制。可以想象，这样的开放式网络为恶意访问提供了入侵的便利条件，采用非常简单的攻击技术便可造成巨大的破坏，不但给企业带来巨大的经济损失，更有可能使企业面临法律上的风险。

3.4.2　非法外联

在终端计算机上使用移动通信设备（例如，利用运营商提供的移动上网卡，如图 3-7 所示）、USB 无线路由设备以及蓝牙、红外等外部通信设备，不受控的智能终端或其他无线设备可以任意接入终端，使终端暴露在不可控的无线网络空间中。而某些移动通信设备会在终端操作系统中配置非法代理服务器，使得内网终端暴露在外部网络空间中，引发

图 3-7　使用移动上网卡

信息泄露和暴露安全脆弱点，造成极大的安全隐患。

3.4.3 非法流量

信息系统通常连接的网络接口，无论是铜芯网线还是光纤接入，其带宽终究是有限的。组织机构通常会在网络边界部署流量控制或流量整形设备，并制定带宽限制策略，以便有效利用网络。但这种方法无法实现基于应用的流量限制，内网依然存在视频、P2P 等软件占用带宽、影响正常办公的情况。

在 2018 年召开的 RSA 安全大会中，安全软件开发商 Sophos 发布了该公司对全球防火墙行业状态的研究结果，此项调查对象是来自 10 个国家（包括美国、加拿大、墨西哥、法国、德国、英国、澳大利亚、日本、印度与南非）中型企业的 2700 多名 IT 管理者，其结论是：IT 管理者根本无法识别企业内近半数（约 45%）的网络流量。事实上，近 1/4 的 IT 管理者无法识别的网络流量比例高达 70%。

如果不具备识别网络上所运行内容的能力，就意味着 IT 管理者将对勒索软件、未知恶意软件、数据泄露以及其他高级威胁与潜在恶意应用/流氓用户视而不见。

3.5 系统方面的安全威胁

3.5.1 安全漏洞

在终端的安全性中，漏洞是一个比较宽泛的概念，可以涉及终端系统的方方面面：硬件、操作系统、应用软件等构成信息系统的组成元素都有可能包含漏洞。在 ISO 27005 标准中将漏洞定义为可被一个或多个威胁利用的资产或资产组的弱点（资产是对组织的商业运作及其业务连续性，包括支持该组织的使命有价值的任何信息资源）；NIST SP800-30 中给出了更广为使用的定义：漏洞是指在系统安全程序、设计、实施或内部控制中的缺陷或弱点，可能会被执行（被意外触发或被故意利用）并导致安全性被破坏或违反系统安全策略。

在终端系统中，漏洞是一个弱点，攻击者可以利用漏洞在终端系统中执行未经授权的操作。这是由于终端系统在需求、设计、实现、配置、运行等过程中会因人为因素有意或无意地产生缺陷。人为因素是其中最主要的原因，表现形式包括代码缺陷、逻辑缺陷、测试不足、权限泛滥、配置缺陷等。这些缺陷以不同形式存在于终端系统的各个层次和环节之中，一旦被攻击者利用，就会对终端安全造成威胁和损害，影响终端系统的正常运行。

需要说明的是，缺陷并不等同于漏洞，只有那些能够被利用且对终端安全造成损害的缺陷才能称为漏洞。漏洞的危害程度依据对终端的保密性、完整性、可用性 3 个方面的影响程度从高到低依次分为超危、高危、中危、低危 4 个等级，具体危害等级划分标准可参考《信息安全技术 安全漏洞等级划分指南》（GB/T 30279—2013）中的相关内容。

漏洞按照成因可分为以下几类：

（1）边界条件错误。由于程序运行时未能有效控制操作范围所导致的安全漏洞，例

如缓冲区溢出、格式串处理等。

(2) 数据验证错误。由于对携带参数或其中混杂操作指令的数据未能进行有效验证和正确处理导致的安全漏洞，例如命令注入漏洞、SQL 注入漏洞、XSS 注入漏洞、LDAP 注入漏洞等。

(3) 访问验证错误。由于没有对请求处理的资源进行正确的授权检查所导致的安全漏洞，例如远程或本地文件包含、认证绕过等。

(4) 处理逻辑错误。由于程序实现逻辑处理功能存在问题所导致的安全漏洞，例如程序逻辑处理错误、逻辑分支覆盖不全面等。

(5) 同步错误。由于程序对操作的同步处理不当所导致的安全漏洞，例如不合理的竞争条件、不正确的数据序列化等。

(6) 意外处理错误。由于程序对意外情况处理不当所导致的安全漏洞，例如泄露程序的某些结构或数据定义。

(7) 对象验证错误。由于程序处理使用对象时缺乏验证所导致的安全漏洞，例如资源释放后重利用、各类对象错误引用等。

(8) 配置错误。由于终端系统安全配置不当所导致的安全漏洞，例如默认配置、默认权限、配置参数错误。

漏洞按照其在终端系统中所处的层次可分为以下几类：

(1) 应用层漏洞。主要来自应用软件(例如 Web 程序、数据库软件、中间件、各种应用软件等)或数据的缺陷。

(2) 系统层漏洞。主要来自操作系统(例如视窗操作系统、服务器操作系统、嵌入式操作系统、网络操作系统等)的缺陷。

(3) 网络层漏洞。主要来自网络的缺陷，例如网络层身份认证、网络资源访问控制、数据传输保密与完整性、远程接入安全、域名系统安全和路由系统安全等方面的漏洞。

漏洞按照是否被发现可分为未知漏洞和已知漏洞。

未知漏洞是指那些系统中存在但还没有被发现的漏洞。这种漏洞的特征是它们没有被软件开发商、安全组织、黑客或黑客组织发现，但客观上是存在的。未知漏洞带给终端的是隐蔽的安全威胁。软件开发商、安全组织、黑客和黑客组织都在努力地挖掘漏洞，可以说，谁先发现了漏洞，谁就可以掌握主动权。如果是软件开发商、安全组织先发现了漏洞，在安全防护上就掌握了安全防护的主动权；如果是黑客或黑客组织先发现了漏洞，就会在攻击上掌握主动权。

已知漏洞从漏洞是否有相应修补措施的角度可以分为两种：0Day 漏洞和 NDay 漏洞。

0Day 漏洞(零日漏洞)是指已经被发现但还没有相应修补措施的漏洞。从信息安全的角度而言，0Day 漏洞的危害性极大，因为这种类型的漏洞有可能掌握在极少数人的手里。攻击者有可能在这种类型的漏洞的信息还没有公布，或者是公布后官方没有给出修补措施之前，利用这段时间差攻击包含 0Day 漏洞的终端。而对于管理终端安全的管理者而言，0Day 漏洞由于没有相应的防御方法，会造成巨大的安全隐患和可能的经济损失。近年来关注度非常高的 APT(Advanced Persistent Threat，高级持续性威胁)攻击就是利

用 0Day 漏洞实施攻击的典型方法。

NDay 漏洞是指已经被发现并有相应修补措施的漏洞。其特点是安全组织或厂商已经掌握了漏洞形成的原因和利用方法，产生漏洞的厂商依据漏洞形成的原因发布了相应的安全补丁程序用于修补相关漏洞，安全组织或厂商按照漏洞形成原因和利用方法，在安全防护产品中或安全服务项目已经加入针对相应类型漏洞的防护方法。而攻击者和黑客组织利用安全组织或厂商公布的漏洞形成原因编写具有针对性的漏洞利用程序文件，对包含漏洞而尚未安装补丁程序的终端进行攻击。

未知漏洞和已知漏洞是动态变化的。未知漏洞可能会因其被产品厂商、攻击人员、安全人员等发现而转为已知漏洞。即使对于已知漏洞，大部分终端用户对终端中是否包含相关漏洞以及相关漏洞是否已经安装补丁程序并不了解，这种情况并不少见。这一方面是由于企事业单位中信息安全岗位人员的缺失，没有专业人员负责维护终端安全；另一方面是由于信息安全管理中制度或制度执行上的缺失，在实际管理中没有行之有效的技术手段和管理措施来保障终端安全。这说明，在终端发现漏洞的情况下，即使是已知并可以被修复的漏洞，仍有可能因为用户未及时安装补丁程序等原因导致终端漏洞仍受到攻击和利用。在前面提到的 APT 攻击中，对此类已知漏洞的利用也不占少数。

安全漏洞的表现形式多种多样，中国国家信息安全漏洞库将信息安全漏洞划分为 26 种类型，并将它们组织成漏洞分类层次树，如图 3-8 所示。

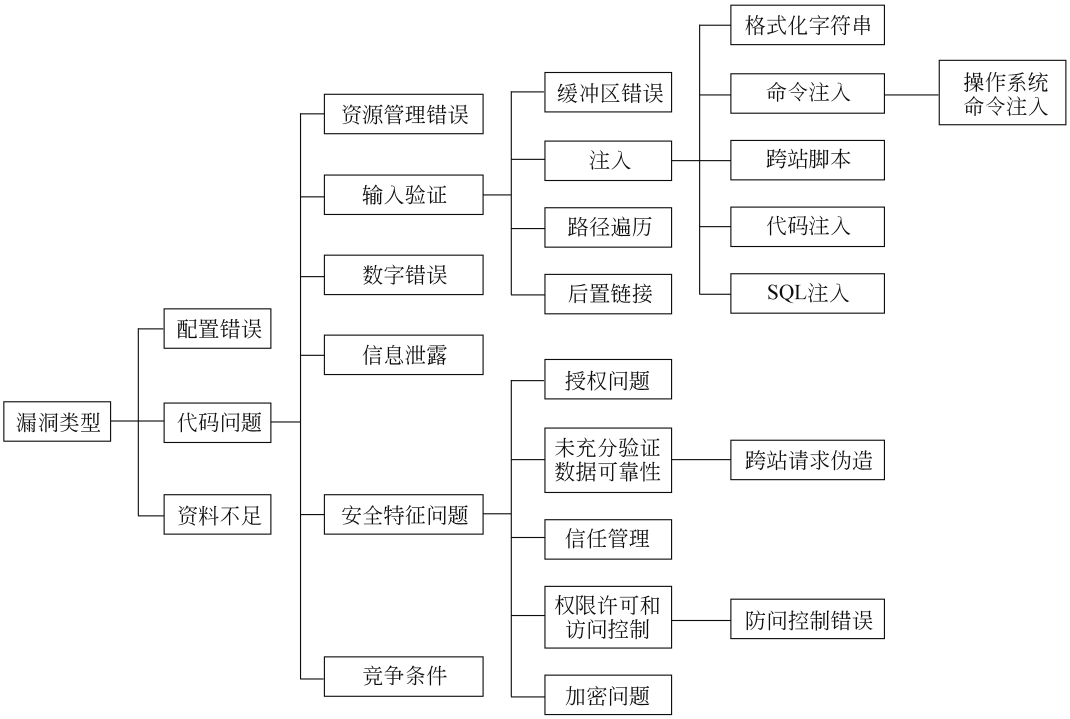

图 3-8　漏洞分类层次树

3.5.2　未定义安全基线

如果组织机构的信息系统网络对终端计算机没有定义标准的安全基线，就会使组织机构的安全管理人员对不符合安全基线的设备不能采取有效的隔离和修复措施，对漏洞、病毒的防护不能落实到位。一旦有终端发生病毒感染，往往很快扩散到全网络，轻则令网络陷于瘫痪，重则造成数据的丢失或损害，甚至造成业务中断，使正常工作无法进行。终端入网安全状况的不统一也会使得运维人员筋疲力尽，降低工作效率。这类安全威胁在实际中主要表现为以下几点：

（1）终端的使用者为便于登录系统，随意更改终端主机的密码，设置口令为弱口令，甚至不设置口令，或者设置的口令不符合强口令规则，使口令容易被暴力猜测破解。

（2）随意更改主机信息。随意更改主机名、IP 地址、MAC 地址等信息，给组织机构资产管理、网络审计等方面造成不便。

（3）随意安装和运行各种软件。由于终端使用者基本都具有信息系统本地管理员权限，可以安装和运行各种娱乐软件甚至是盗版软件，这些软件可能带有病毒、木马等恶意程序，给信息系统和组织机构带来声誉风险、版权风险和安全风险。

3.6　恶意软件

随着信息技术的不断发展，社会中各种业务的运作越来越依赖于计算机，而目前防不胜防的计算机恶意软件给计算机终端的正常运行造成了较大的威胁。互联网的普及也使得恶意软件大量出现。

图 3-9　存储 Morris 蠕虫源程序的磁盘

早期的恶意软件都是作为实验或恶作剧编写的，典型的例子是第一个互联网蠕虫 Morris，如图 3-9 所示。恶意软件从政府和企业网站收集受保护的信息，并且在一些关键基础设施中伺机进行破坏性操作（例如 3.6.5 节中的 APT 攻击）。恶意软件也可以用于获取个人信息，例如身份证号码、银行账号或信用卡号、密码等。

恶意软件被有意地设计成使计算机、服务器、客户端或计算机网络损坏的软件，被恶意攻击者广泛用于窃取个人、组织机构的财务、商业信息，攫取经济利益，窃取情报，发动网络战等。恶意软件在植入或以某种方式侵入目标终端后，采用可执行代码、脚本、活动内容和其他软件等多种形式对终端造成损害。可执行代码的表现形式可以是病毒、蠕虫、木马、勒索软件、间谍软件、广告软件等，并且可能不限于一种形式，往往是多种形式的混合体。在中国国家

标准《信息安全技术 病毒防治产品安全技术要求和测试评价方法》(GB/T 37090—2018)中,对恶意软件进行了定义:能够影响计算机操作系统、应用程序和数据的完整性、可用性、可控性和保密性的计算机程序或代码的软件。以下介绍恶意软件对终端安全产生影响的常见形式。

3.6.1 僵尸网络

僵尸终端是被恶意攻击者利用病毒、蠕虫、木马等恶意软件控制的,用于非法目的的终端,俗称"肉鸡"。僵尸终端可用于发送垃圾电子邮件、存储违禁数据(例如,色情内容)、发动分布式拒绝服务攻击(DDoS)等目的。僵尸网络(botnet)是此类僵尸终端的逻辑集合,僵尸终端可以是计算机终端、移动智能终端甚至是物联网设备终端等。例如,2016 年 10 月 21 日的 Dyn(达因公司,提供 DNS 服务)网络攻击事件是一起典型的由僵尸网络发起的分布式拒绝服务攻击,攻击导致欧洲和北美的大量用户无法使用主要的互联网平台和服务。此次事件主要是由于被感染 Mirai 恶意软件的大量物联网设备(例如网络摄像头、家庭网关等联网设备)组成的僵尸网络利用分布式拒绝服务攻击方式向 Dyn 域名解析服务器提交数以千万计的海量 IP 地址 DNS 查询请求,使 Dyn 域名解析服务器无法对外提供服务,导致互联网服务瘫痪。受网络攻击影响的北美和欧洲区域如图 3-10 所示,颜色深浅表明受影响的程度。

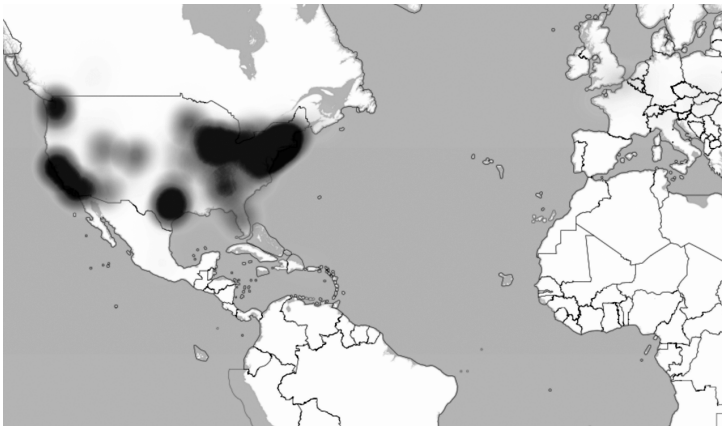

图 3-10　受网络攻击影响的北美和欧洲区域

僵尸网络的体系结构也在不断发展,除了传统的客户/服务器方式,还出现了点对点方式。这些僵尸网络的实际控制者通过 IRC、Telnet、P2P 等协议发动攻击,大型僵尸网络还采用了域的组织方式,僵尸网络通过这些协议完成命令和控制(Command and Control,简称 C&C 或 C2)的过程。攻击者通过隐蔽通道与僵尸终端上的客户端软件进行通信。僵尸网络除了常见的发送垃圾邮件和拒绝服务攻击、获取僵尸终端的用户个人敏感信息外,还被用于间谍活动、下载和安装流氓软件、网络欺诈、挖矿、APT 等恶意攻击行为中,参见后续章节相关内容的介绍。

僵尸终端的大多数所有者、使用者通常没有意识到终端被恶意利用。这些终端可以

是路由器、Web 服务器、物联网设备，僵尸恶意软件利用终端的漏洞（例如弱口令、安全漏洞等）对终端进行感染，使之成为僵尸网络的一员，并可能进一步感染其他终端，对终端安全和终端所在信息系统造成巨大的安全隐患。

3.6.2　软件供应链攻击

软件供应链攻击是指利用软件供应商与最终用户之间的信任关系，在合法软件正常传播和升级过程中，利用软件供应商的各种疏忽或漏洞，对合法软件进行劫持或篡改，从而绕过传统安全产品检查，以达到非法目的的攻击类型，如图 3-11 所示。

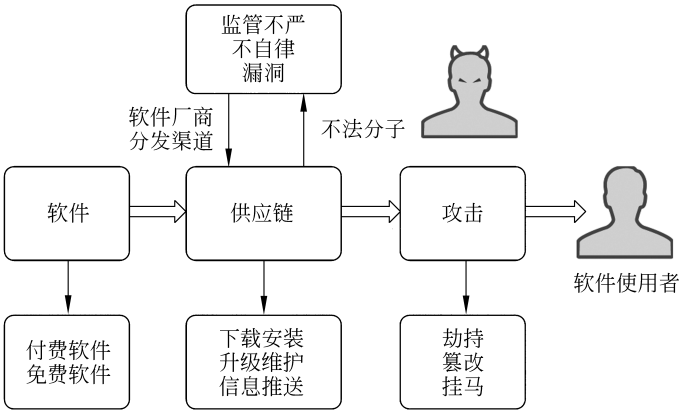

图 3-11　供应链攻击

在软件供应链中，软件通常可分为付费软件和免费软件。个人和政企用户通常认为付费软件在质量、安全性和服务等方面都会有很高的保障，遭遇供应链攻击的概率相对会低很多。也正是因为这种强信任关系，付费软件一旦遭遇软件供应链攻击，其破坏性也将是巨大的。免费软件通常都是个人自行从互联网上下载和安装的，软件本身的安全性参差不齐，组织机构对软件厂商也没有直接的约束，因此遭遇软件供应链攻击的风险非常高。通过下载安装、升级维护、信息推送等方式，利用软件厂商及其分发渠道监管不严、不自律、漏洞，通过劫持、篡改、挂马等方式对软件进行污染，达到其非法目的。

360 安全团队在 2017 年发布的《中国政企软件供应链攻击现状分析报告》中列举了多起软件供应链攻击的案例，其中比较著名的攻击事件发生在 2017 年 6 月 27 日，乌克兰、俄罗斯、印度、西班牙、法国、英国等欧洲多国遭受大规模 Petya 勒索病毒袭击，该病毒远程锁定设备，然后索要赎金。其中，乌克兰受灾最为严重，政府、银行、电力系统、通信系统、企业以及机场都不同程度地受到了影响，首都基辅的鲍里斯波尔国际机场、乌克兰国家储蓄银行、马士基船舶公司、俄罗斯石油公司和乌克兰部分商业银行、零售企业和政府系统遭到了攻击。有研究认为，这次攻击的目的是破坏而非敲诈，目标是破坏乌克兰的重点基础设施，只是伪装成 Petya 病毒攻击的样子来欺骗安全分析人员，因此有的安全公司称之为 NotPetya 攻击。

根据事后的分析，此次事件之所以能在短时间内肆虐欧洲大陆，就在于其利用了在乌

克兰流行的会计软件 M.E.Doc 进行传播。这款软件是乌克兰政府要求企业安装的，覆盖率接近 50%。更为严重的是，根据安全公司的研究，M.E.Doc 公司的升级服务器在问题爆发前 3 个月就已经被控制，换而言之，攻击者已经控制了乌克兰 50%的公司达 3 个月之久，Petya 攻击只是这个为期 3 个月的控制的最后终结，其目的就是尽可能多地破坏攻击线索，避免政府对攻击过程取证。在此过程中，攻击者采用的就是典型的软件供应链攻击方法。

3.6.3 勒索软件

2017 年 5 月，永恒之蓝勒索蠕虫病毒（WannaCry，也译作“想哭”病毒）肆虐全球，导致 150 多个国家、30 多万受害者遭遇勒索软件攻击，医疗、交通、能源、教育等行业领域遭受巨大损失。特别是在该病毒的攻击过程中，大量“不联网”的、一向被认为是相对安全的企业和机构的内网设备也被感染，这给全球所有企业和机构都敲响了警钟：没有绝对的隔离，也没有绝对的安全，不联网的不一定比联网的更加安全。该病毒的编写人员据称是美国国家安全局（National Security Agency，NSA）旗下方程式组织（Equation Group）。以永恒之蓝为代表的这一波漏洞利用武器库的大规模试水可以称为网络战的雏形，如图 3-12 所示。

图 3-12　WannaCry 攻击效果

360 互联网安全中心 2017 年 12 月发布的《2017 勒索软件威胁形势分析报告》中的数据表明，在 2017 年 1～11 月，360 互联网安全中心共截获计算机端新增勒索软件变种 183 种，新增控制域名 238 个。全国至少有 472.5 多万台用户计算机遭到了勒索软件攻击，平均每天约有 1.4 万台国内计算机遭到勒索软件攻击。2018 年，全国共有 430 余万台计算机遭受勒索软件攻击。勒索软件由 2017 年的撒网式无差别攻击逐步转向以服务器定向攻击为主、以撒网式无差别攻击为辅的方式。

根据 360 终端安全实验室《2018 年勒索病毒白皮书（政企篇）》的数据，勒索软件的传播方式分布如图 3-13 所示。勒索软件以某种方式影响受感染的计算机系统，并要求对方

付款以使系统恢复正常状态。例如，CryptoLocker 可以安全地加密文件，并且在支付勒索赎金后解密文件。

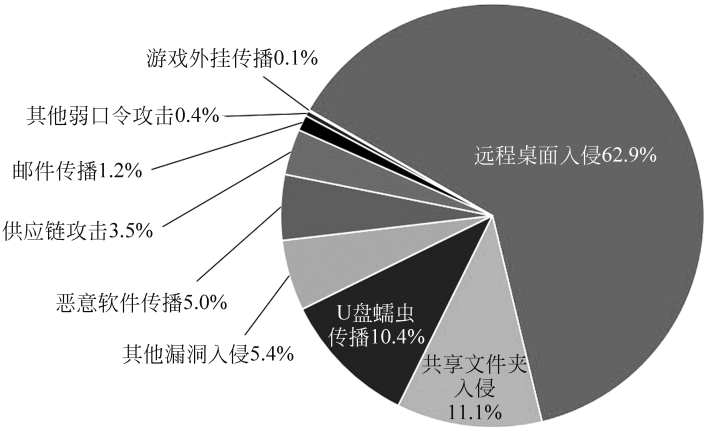

图 3-13　2018 年勒索软件传播方式分布

在被勒索软件攻击的政企终端中，金融行业终端最多，占攻击终端总数的 31.8%；其次是政府、能源行业终端，占比分别为 10.4%、9.0%，如图 3-14 所示。

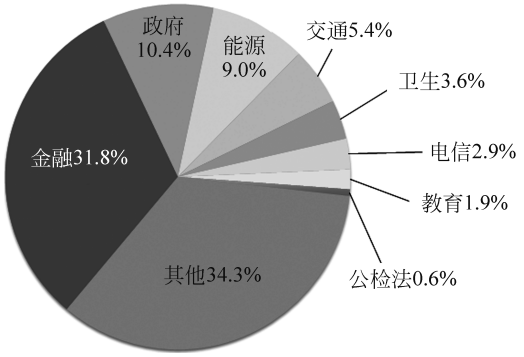

图 3-14　被勒索软件攻击的政企终端行业分布

勒索软件紧密跟踪漏洞，利用多种漏洞、多种方式进行传播；攻击面和目标继续扩大，除高价值个人目标外，还包括政企机构、关键基础设施等；被攻击的设备种类不断扩大，从个人主机到政企机构的服务器，从普通办公终端到专业生产设备；攻击目的也呈现多样化，不局限于勒索，还包括以营利为目的的组织化犯罪；勒索行为也不再是恶意攻击者个人的行为，已经呈现有计划、有组织、有目的的群体性行为特征。预计勒索软件在 2019 年仍将在恶意软件威胁排行榜上占有非常大的比重。

3.6.4　挖矿木马

挖矿木马是一类通过入侵计算机系统并植入挖矿机程序，以赚取加密数字货币（例如比特币、莱特币、门罗币等）的木马类恶意软件。被植入挖矿木马的计算机会出现 CPU、GPU（Graphics Processing Unit，图形处理器）使用率飙升、系统卡顿、部分服务无法正常

使用等情况。挖矿木马最早在2012年出现，并在2017年开始大量传播。

360安全卫士2019年1月发布的《2018年Windows服务器挖矿木马总结报告》中的数据表明：2018年，挖矿木马已经成为Windows服务器遭遇的最严重的安全威胁之一，挖矿木马攻击趋势由2017年的爆发式增长逐渐转为平稳发展的同时，挖矿木马攻击技术提升明显，恶意挖矿产业也趋于成熟。针对Windows服务器的挖矿木马除少部分利用Windows自身漏洞外，更多的是利用搭建在Windows平台上的Web应用或数据库的漏洞入侵服务器。2018年针对Windows服务器的挖矿木马攻击目标分布如图3-15所示。

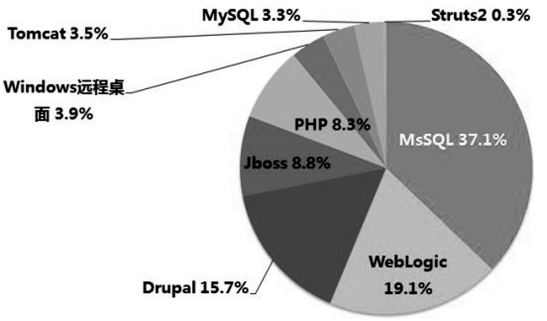

图3-15　2018年针对Windows服务器的挖矿木马攻击目标分布

常见的挖矿木马家族有WannaMine、Mykings、8220、MassMiner等。由于挖矿是一种几乎零成本的获利方式，恶意挖矿家族还进一步通过相互合作、各取所需，使受害计算机和网络设备的价值被更大程度地压榨。挖矿木马家族除了往终端中植入挖矿木马直接获利外，还会向其他黑产家族提供成熟的漏洞攻击武器与战术，或者将已控制的终端出售给其他黑产家族，造成终端安全威胁来源扩大化，给终端安全带来更多的安全隐患。

3.6.5　APT

高级持续性威胁(Advanced Persistent Threat，APT)是一类具有隐蔽性和持续性的黑客程序，通常针对商业、政府机构等目标，利用先进的攻击手段对特定目标进行长期持续性网络攻击，是近年来极具威胁性的攻击手段之一。由于网络“军火”民用化趋势的出现，越来越多的军火级网络漏洞利用工具被应用于攻击普通互联网目标。这使业界和公众进一步加深了对APT攻击与威胁的认识。APT的特点如下：

(1) 高级。攻击组织者通常拥有全方位的情报收集技术，包括计算机入侵技术、情报收集技术，甚至包括电话拦截和卫星成像技术。虽然攻击过程中采用的攻击技术可能不会被归类为高级，例如使用自动化的恶意软件生成工具包生成的攻击组件或易于获取的漏洞利用工具，但是，攻击团队通常可以根据攻击的需要设计和开发更高级的应用工具，通常结合多种攻击方法、工具和技术以达到并攻陷目标，保持对目标的访问。

(2) 持久性。攻击者通常有特定的目的和任务，而不是机会性地寻求财产信息或其他短期收益的信息。这意味着攻击者会受某些组织的指导，通过持续监测和互动，对目标进行跟踪，以实现既定攻击目的。这并不意味着对目标持续的攻击或者恶意软件更新，事实上，低速和慢速方法通常更为成功。与仅需要执行特定任务的威胁相比，攻击者的主要

目标之一是保持对目标长达数年甚至数十年的长期访问。

(3) 威胁。APT 是一种安全威胁,因为攻击者具有专业能力和明确意图。APT 是有组织的行为,而不是无意识的随机行为,也不是自动化的恶意代码执行。攻击者有特定的目标,技术娴熟,积极主动,且攻击过程条理分明,不受资金条件的限制。

APT 攻击者通常会使用 0day、NDay 漏洞实现指定目标的攻击,攻击目标主要集中在政府、能源、金融、国防、互联网等领域,以获取目标的核心价值为导向,其核心价值可以表现为政治、经济、社会、军事、技术等方面的信息。例如,2010 年著名的震网攻击就是典型的 APT 事件,这次攻击利用相关工作人员的个人计算机作为第一道攻击跳板,进而感染相关人员的移动设备,病毒以移动设备为桥梁进入隔离内网内部,随即潜伏下来并很有耐心地逐步扩散,在特定条件下突然爆发进行破坏。这是一次十分成功的 APT,而其最为成功的地方就在于极为巧妙地控制了攻击范围,攻击十分精准。

APT 攻击者遵循的典型持续攻击过程如下:

(1) 选择攻击目标,通常针对特定的组织。

(2) 尝试在目标环境中建立立足点(常见攻击方法包括鱼叉式网络钓鱼电子邮件)。

(3) 使用受感染的系统访问目标网络。

(4) 部署有助于实现攻击目的的其他工具。

(5) 消除痕迹以保证未来可按计划访问。

2013 年,Mandiant 公司对在 2004—2013 年期间使用的 APT 方法进行研究,将其过程总结为类似生命周期的过程。下面简要介绍这一过程:

(1) 寻找切入点。通过电子邮件等方式,主要利用社会工程学和鱼叉式网络钓鱼(使用 0Day、NDay 漏洞);或者在目标组织的员工可能访问的网站上植入恶意软件,进行水坑攻击;或者通过感染病毒的移动存储设备进行摆渡攻击。寻找切入点的方法多种多样,其最终目的是切入目标网络。

(2) 建立立足点。在目标网络中安装远程管理软件,创建网络后门和隧道,允许攻击者隐形访问其基础设施。

(3) 提升权限。利用漏洞和密码破解方式获取受攻击计算机的管理员权限,并尽可能将其扩展到 Windows 域管理员账户。

(4) 内部侦察。收集有关基础设施、信任关系、Windows 域结构等相关信息。

(5) 横向移动。将控制扩展到其他工作站、服务器和基础设施元素,并对其进行数据收集。

(6) 保持存在。确保持续控制前面步骤中获取的访问通道和凭据。

(7) 完成任务。从受害者的网络中获取数据。

从近期 APT 事件中,可以总结 APT 技术热点和发展趋势如下:

(1) Office 0Day 漏洞成为焦点。Office 漏洞的利用,一直是 APT 组织攻击的重要手段。2017 年,先后又有多个高危的 Office 漏洞被曝出,其中很大一部分已经被 APT 组织使用。Office 0Day 漏洞已经成为 APT 组织关注的焦点。其中逻辑性漏洞、内存破坏性漏洞为主要类型,这类漏洞包括 CVE-2014-4114、CVE-2014-6352、CVE-2015-0097、CVE-2017-0262、CVE-2016-7255 等漏洞都曾名噪一时。

(2) 恶意代码复杂性显著增强。在 2017 年的 APT 技术领域中,被提及最多的病毒不是 WannaCry,而是 FinSpy(又名 FinFisher 或 WingBird)。CVE-2017-0199、CVE-2017-8759、CVE-2017-11292 等多个漏洞都被用来投递 FinSpy。FinSpy 的代码经过了多层虚拟机保护(如图 3-16 所示),并且还有反调试和反虚拟机等功能,复杂程度极高。

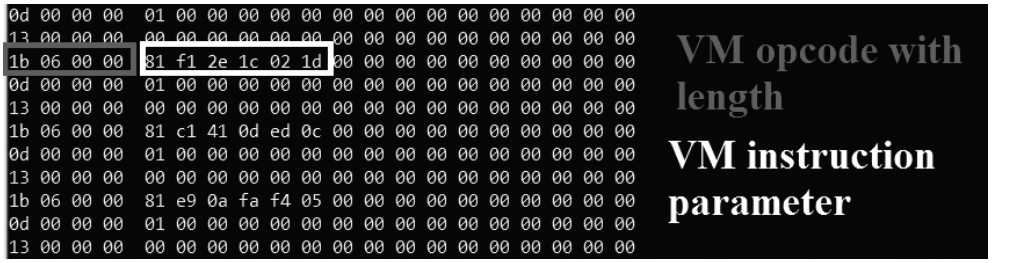

图 3-16 代码保护

(3) APT 已经影响到每一个人的生活。APT 和 APT 组织已经开始影响到每一个人的生活。APT 一般是针对重要的组织或个人发动的。然而在 2017 年,APT28 组织针对酒店行业进行了攻击。而乌克兰电网攻击事件以及席卷全球的 WannaCry 和类 Petya 背后也隐隐有 APT 组织的影子。

作为 APT 最直接的战场——终端,无论是被动防御攻击还是主动安全加固,其目的都是确保终端可以有效抵御 APT,从而保证信息系统基础设施的安全。

3.7 习题

1. 自然灾害有哪些特点?

2. 在电磁信号领域,主要由哪几种泄露数据信息的方式?又有哪几种方式可以降低系统传输性能?

3. 从终端所处的环境来看,设立终端机房时应考虑哪些因素?

4. 在终端系统中,移动存储设备带来的安全威胁有哪些?

5. 漏洞有哪些种类?其基本概念是什么?

6. 调研近年来的 APT 事件,简要描述其攻击原理。

第 4 章 终端安全管理概述

4.1 终端安全管理概念

4.1.1 个人终端安全与企业终端安全的区别

从安全管控范围来看，个人终端是信息系统的末端，个人终端安全只保护单点终端用户的安全，不能对整个信息系统终端形成有效的管理，也不能建立统一的安全基线，管理人员无法掌握全网的安全状况；而企业终端安全面对的是企业的信息系统，在单点终端安全的基础上又增加了全网统一管理、全网统一展示、全网统一策略等网络化管理能力。针对企业复杂的使用环境，还需要提供符合安全要求的定制化服务，对于重要基础设施领域的企业这类需要重点保护的单位（例如电信企业、金融企业等），还需要提供专人负责、定向解决企业用户问题的安全服务。而且，为应对越来越严峻的网络安全态势，很多企业级安全产品增加了与其他安全产品联动的功能，对信息系统的整体防护效果和防护效率高于个人安全产品。个人终端安全与企业终端安全功能的对比如表 4-1 所示。

表 4-1 个人终端安全与企业终端安全功能对比

功能分类	功能项	个人终端安全	企业终端安全
终端防护	终端扫描	√	√
	安全监控	√	√
	系统加固	√	√
网络管理	全网安全状况查看	×	√
	全网日志统一分析	×	√
	全网分级管理	×	√
	全网分组管理	×	√
集中管控	全网终端的统一升级	×	√
	全网终端的统一策略设置	×	√
	全网终端的统一部署	×	√
终端管控	远程终端信息查看	×	√
	远程终端设置更改	×	√
	远程终端行为控制	×	√

√为支持的功能，×为不支持的功能。