论 剑

为黑客“正名”

提起黑客，总是令人感到神秘莫测。在人们眼中，黑客似乎是一群聪明绝顶、精力旺盛的年轻人，一门心思地破译各种密码，以便偷偷地、未经允许地打入他人的计算机系统,窥视其隐私。那么,究竟什么是黑客呢？

黑客(*Hacker*)，源于英语动词Hack,意为“劈，砍”,引申为“干了一件非常漂亮的工作”。在早期美国麻省理工学院的校园俚语中,“黑客”则有“恶作剧”之意，尤其是指手法巧妙、技术高明的恶作剧。在日本《新黑客词典》中,对黑客的定义是“喜欢探索软件程序奥秘，并从中增长了其个人才干的人。他们不像绝大多数电脑使用者那样，只规规矩矩地了解别人指定了解的狭小部分知识。”由这些定义中,我们还看不出过于贬义的意味。他们通常具有硬件和软件的高级知识,并有能力通过创新的方法剖析系统。“黑客”能使

更多的网络趋于完善和安全，他们以保护网络为目的，而以不正当侵入为手段找出网络漏洞。

另一种入侵者是那些利用网络漏洞破坏网络的人。他们往往做一些重复的工作（如采用暴力法破解口令），他们也具备广泛的电脑知识，但与黑客不同的是他们以破坏为目的。这些群体被称为“骇客”。当然也有一种人介于黑客与“骇客”之间。

一般认为，黑客起源于20世纪50年代美国麻省理工学院的实验室中，他们精力充沛，热衷于解决难题。60、70年代，“黑客”一词极富褒义，用于指代那些独立思考、奉公守法的计算机迷，他们智力超群，对电脑全身心投入，对电脑的最大潜力进行智力上的自由探索，为电脑技术的发展做出了巨大贡献。正是这些黑客，倡导了一场个人计算机革命，倡导了现行的计算机开放式体系结构，打破了以往计算机技术只掌握在少数人手里的局面，开了个人计算机的先河，提出了“计算机为人民所用”的观点，他们是电脑发展史上的英雄。现在黑客使用的侵入计算机系统的基本技巧，例如破解口令（Password Cracking）、开天窗（Trapdoor）、走后门（Backdoor）、安放特洛伊木马（Trojan Horse）等，都是在这一时期发明的。从事黑客活动的经历，成为后来许多计算机业巨子简历上不可或缺的一部分。苹果公司创始人之一乔布斯就是一个典型的例子。

在60年代，计算机的使用还远未普及，并没有多少存储重要信息的数据库，也谈不上黑客对数据的非法拷贝等问题。到了80、90年代，计算机越来越重要，大型数据库也越来越多，同时，信息越来越集中在少数人的手里。这样一场新时期的“圈地运动”引起了黑客们的极大反感。黑客认为，信息应共享而不应被少

数人所垄断，于是将注意力转移到涉及各种机密的信息数据库上 而这时,电脑化空间已私有化,成为个人拥有的财产，社会不能再对黑客行为放任不管，必须采取行动，利用法律等手段来进行控制。黑客活动受到了空前的打击。

但是，政府和公司的管理者现在越来越多地要求黑客传授给他们有关电脑安全的知识。许多公司和政府机构已经邀请黑客为他们检验系统的安全性，甚至还请他们设计新的保安规程。例如，在两名黑客连续发现网景公司设计 的信用卡购物程序的缺陷并向商界发出公告之后，网景修正了缺陷并宣布举办名为“ 网景缺陷大奖赛 ’的竞赛,那些发现和找到该公司产品中安全漏洞的黑客可获1000 美元奖金。无疑,黑客正在对电脑防护技术的发展做出贡献。

黑客攻击术

一些黑客往往会采取几种攻击方法，但是我很想说的是，一个优秀的黑客绝不会随便攻击别人的。

1、一般黑客攻击术

攻击术之一：获取口令

这又有三种方法：一是通过网络监听非法得到用户口令,这类方法有一定的局限性,但危害性极大,监听者往往能够获得其所在网段的所有用户账号和口

令，对局域网安全威胁巨大；二是在知道用户的账号后（如电子邮件@前面的部分）利用一些专门软件强行破解用户口令，这种方法不受网段限制，但黑客要有足够的耐心和时间；三是在获得一个服务器上的用户口令文件（此文件成为 Shadow 文件)后,用暴力破解程序破解用户口令，该方法的使用前提是黑客获得口令的 Shadow 文件。此方法在所有方法中危害最大，因为它不需要像第二种方法那样一遍又一遍地尝试登录服务器，而是在本地将加密后的口令与 Shadow 文件中的口令相比较就能非常容易地破获用户密码，尤其对那些弱智用户（指口令安全系数极低的用户，如某用户账号为 zys ,其口令就是 zys666、666666 、或干脆就是 zys 等),更是在短短的一两分钟内,甚至几十秒内就可以将其干掉。

攻击术之二：放置特洛伊木马程序

特洛伊木马程序可以直接侵入用户的电脑并进行破坏，它常被伪装成工具程序或者游戏等诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载，一旦用户打开了这些邮件的附件或者执行了这些程序之后，它们就会像古特洛伊人在敌人城外留下的藏满士兵的木马一样留在自己的电脑中，并在自己的计算机系统中隐藏一个可以在 windows 启动时悄悄执行的程序。当您连接到因特网上时，这个程序就会通知黑客，来报告您的 IP 地址以及预先设定的端口。黑客在收到这些信息后，再利用这个潜伏在其中的程序，就可以任意地修改您的计算机的参数设定、复制文件、窥视你整个硬盘中的内容等，从而达到控制你的计算机的目的。

攻击术之三：WEB 的欺骗技术

在网上用户可以利用 IE 等浏览器进行各种各样的 WEB 站点的访问，如阅读新闻组、咨询产品价格、订阅报纸、电子商务等；然而一般的用户恐怕不会想到有这些问题存在：正在访问的网页已经被黑客篡改过，网页上的信息是虚假的！例如黑客将用户要浏览的网页的 URL 改写为指向黑客自己的服务器，当用户浏览目标网页的时候，实际上是向黑客服务器发出请求，那么黑客就可以达到欺骗的目的了。

攻击术之四：电子邮件攻击

电子邮件攻击主要表现为两种方式：一是电子邮件轰炸和电子邮件“滚雪球”，也就是通常所说的邮件炸弹，指的是用伪造的 IP 地址和电子邮件地址向同一信箱发送数以千计、万计甚至无穷多次的内容相同的垃圾邮件，致使受害人邮箱被“炸”，严重者可能会给电子邮件服务器操作系统带来危险，甚至瘫痪；二是电子邮件欺骗，攻击者佯称自己为系统管理员（邮件地址和系统管理员完全相同），给用户发送邮件要求用户修改口令(口令可能为指定字符串)，或在貌似正常的附件中加载病毒或其他木马程序（据笔者所知，某些单位的网络管理员有定期给用户免费发送防火墙升级程序的义务，这为黑客成功地利用该方法提供了可乘之机)。这类欺骗只要用户提高警惕，一般危害性不是太大。

攻击术之五：通过一个节点来攻击其他节点

黑客在突破一台主机后，往往以此主机作为根据

地,攻击其他主机(以隐蔽其入侵路径,避免留下蛛丝马迹)。他们可以使用网络监听方法,尝试攻破同一网络内的其他主机；也可以通过IP欺骗和主机信任关系,攻击其他主机。这类攻击很狡猾,但由于某些技术很难掌握,如IP欺骗，因此较少被黑客使用。

攻击术之六 网络监听

网络监听是主机的一种工作模式，在这种模式下，主机可以接受到本网段在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接受方是谁。此时，如果两台主机进行通信的信息没有加密，只要使用某些网络监听工具，例如NetXray for windows 95/98/nt, sniffit for Linux. solaries等就可以轻而易举地截取包括口令和账号在内的信息资料。虽然网络监听获得的用户账号和口令具有一定的局限性，但监听者往往能够获得其所在网段的所有用户账号及口令。

攻击术之七：寻找系统漏洞

许多系统都有这样那样的安全漏洞（Bugs),其中某些是操作系统或应用软件本身具有的，如Sendmail漏洞、win98中的共享目录密码验证漏洞和IE5漏洞等，这些漏洞在补丁未被开发出来之时一般很难防御黑客的破坏，除非你将网线拔掉；还有一些漏洞是由于系统管理员配置错误引起的，如在网络文件系统中,将目录和文件以可写的方式调出,将未加Shadow的用户密码文件以明码方式存放在某一目录下，这都会给黑客带来可乘之机，应及时加以修正。

攻击术之八：利用账号进行攻击

有的黑客会利用操作系统提供的缺省账户和密码进行攻击,例如许多UNIX主机都有FTP和Guest等缺省账户（其密码和账户名同名），有的甚至没有口令。黑客用Unix操作系统提供的命令如Finger 和Ruser 等收集信息,不断提高自己的攻击能力。这类攻击只要系统管理员提高警惕，将系统提供的缺省账户关掉或提醒无口令用户增加口令，一般都能克服。

攻击术之九：偷取特权

利用各种特洛伊木马程序、后门程序和黑客自己编写的导致缓冲区溢出的程序进行攻击，前者可使黑客非法获得对用户机器的完全控制权，后者可使黑客获得超级用户的权限，从而拥有对整个网络的绝对控制权。这种攻击手段一旦奏效，危害性极大。

2、过去五种影响最大的攻击

红色代码：

2001年7月的某天,全球的IDS几乎同时报告遭到不明蠕虫攻击。信息安全组织和专业人士纷纷迅速行动起来，使用蜜罐(Honeypots)技术从因特网上捕获数据包进行分析,最终发现这是一利用微软IIS缓冲溢出漏洞进行感染的变种蠕虫。其实这一安全漏洞早在一个月以前就已经被eEye Digital Security 发现,微软也发布了相应的补丁程序，但是却很少有组织和企业的网络对其引起足够的重视，下载并安装了该补丁。在红色代码首次爆发的短短9个小时内,这一小小

蠕虫以迅雷不及掩耳之势迅速感染了25万台服务器，其速度和深入范围之广也迅速引起了全球媒体的注意。最初发现的红色代码蠕虫还只是篡改英文站点的主页，显示‘Welcome to http://www.wor.com! Hacked by Chinese! ’等信息。但是随后的红色代码蠕虫便如同洪水般在互联网上泛滥，发动DOS(拒绝服务)攻击以及格式化目标系统硬盘。随后,红色代码又不断的变种，其杀伤力也更强，在红色代码II肆虐时,有近2万服务器、500万网站被感染。从红色代码的影响中网络用户可以得到启示：只要注意及时更新补丁和修复程序，对于一般的蠕虫传播是完全可以避免的。因此作为系统管理员在平时应该多注意自己的系统和应用程序所出现的最新漏洞和修复程序，对于提供了修复程序和解决方案的应立即安装和实施；在网络遭到攻击时，为进行进一步的分析，使用蜜罐是一种非常行之有效的方法。

尼姆达(Nimda)：

尼姆达(Nimda)是在‘9.11 ’恐怖袭击整整一个星期后出现的，一些安全专家甚至喊出了“我们现在急需制定另一个‘曼哈顿计划’,以随时应对网络恐怖主义”的口号，由此可见尼姆达在当时给人们造成的恐慌。尼姆达病毒是在早上9:08 发现的，它明显地比红病毒更快、更具有摧毁功能，半小时之内就传遍了整个世界。随后在全球各地侵袭了830万部电脑,总共造成将近10亿美元的经济损失。同‘红色代码’一样‘,尼姆达’也是通过网络对Windows 操作系统进行感染的一种蠕虫型病毒。但是它与以前所有的网络蠕虫的最大不同之处在于‘,尼姆达’通过多种不同的途径进行传

播,而且感染多种Windows 操作系统。“红色代码”只能够利用IIS的漏洞来感染系统,而“尼姆达”则利用了至少四种微软产品的漏洞来进行传播。从Nimda蠕虫病毒播发的全程和特点来看，网络用户又可以深刻地认识到：对网络攻击事件的紧急响应能力以及和安全专家们建立良好的关系是非常重要的；为阻断恶意蠕虫的传播，往往需要在和广域网的接口之间设置过滤器，或者干脆暂时断开和广域网的连接；在电子邮件客户端和网络浏览器中禁止任意脚本的执行对网络安全性来说是很关键的。

Melissa(1999) 和 LoveLetter(2000)

在1999年3月爆发的Melissa 病毒和2000 年5月爆发的LoveLetter 病毒因为它们能够迅速蔓延并造成极大的危害，也荣登了这次评选的五大宝座之一。Melissa 是Microsoft Word 宏病毒，LoveLetter 则是VBScript 病毒,二者除了都是利用Outlook 电子邮件附件进行传播外,另外恶意代码也都是利用Microsoft公司开发的Script 语言缺陷进行攻击，因此二者非常相似。用户一旦在Microsoft Outlook 里打开这个邮件，系统就会自动复制恶意代码并向地址簿中的所有邮件地址发送带有病毒的邮件。很快,由于Outlook 用户数目众多，其病毒又可以很容易地被复制，很快许多公司的邮件服务器就被洪水般的垃圾邮件塞满而中断了服务。一些公司在发现遭到攻击或可能遭到后立即将自己内部网络与因特网断开，在内部网将遭到蠕虫感染的机器清除或隔离，等病毒风暴过后才连接到internet 上,因此才免受其危害。当时的各大防病毒厂商在病毒爆发后不久立即向他们的客户分发病毒

签名文件，但是由于用户太多却要在同一时间下载和更新病毒库，使得要想及时更新签名文件变得非常困难，这无疑更加助长了病毒的肆虐。也正是因为这个原因使得Melissa 和 LoveLetter 病毒所产生的危害仅次于红色代码和尼姆达。Melissa 和 LoveLetter 的爆发可以说是信息安全的唤醒电话，它引起了当时人们对信息安全现状的深思，并无形中对信息安全的设施和人才队伍的发展起了很大的刺激作用：Melissa 和 LoveLetter 刺激了企业和公司对网络安全的投资，尤其是对防病毒方面的投入；许多公司对网络蠕虫病毒的紧急响应表现出来的无能刺激了专业的网络安全紧急响应小组的空前壮大。

分布式拒绝服务攻击

在2000 年新千年到来之际，信息安全领域的人们都以为可以集体地长长地嘘一口气了，因为他们以为由于存在千年虫的问题，在信息网络安全领域中应该暂时还不会出现什么波澜。然而，一月之后却来了一场谁也意想不到的大洪水：在全球知名网站雅虎第一个宣告因为遭受分布式拒绝服务攻击而彻底崩溃后，紧接着 Amazo.com、CNN、E*Trade、ZDNet、Bu.com、Excite 和 eBay 等其他七大知名网站也几乎在同一时间彻底崩溃。这无疑又一次为因特网敲响了警钟。其实，在这之前人们已经接触过来自数以百计的机器的flood 攻击，但是像针对雅虎这样大规模的攻击却从未目击过，甚至未曾想象过。DDoS 的闪击般攻击使人们认识到因特网远比他们想象的更加脆弱，分布式地拒绝服务攻击产生的影响也远比他们原来想象中的要大得多。利用因特网上大量的机器进行

DDOS ，分布式扫描和分布式口令破解等，一个攻击者能够达到许多意想不到的强大效果。从雅虎遭到强大的DDOS攻击中人们又获得了启示：要阻止这种攻击关键是网络出口反欺骗过滤器的功能是否强大。也就是说如果你的Web 服务器收到的数据包的源IP地址是伪造的话，你的边界路由器或防火墙必须能够识别出来并将其丢弃；网络安全事件响应小组们认识到他们必须和他们的ISP 共同去阻止数据包的 flood 攻击。如果失去ISP 的支持，即使你的防火墙功能再强大，你网络出口的带宽仍旧可能被全部占用。唯一有效的也是最快速的方法就是和 ISP 联手通过丢包等方法一起来阻挡这一庞大的Flood 攻击；不幸的是，DDoS 攻击即使在目前也仍旧是互联网面临的主要威胁，当然这主要是因为ISP 在配合阻断DDoS 攻击上速度太慢引起的，这无疑使事件紧急响应的效果大打折扣。

远程控制特洛伊木马后门（1998—2000）：

在1998年7月，黑客 Cult of the Dead Cow（CDC）推出的强大后门制造工具 Back Orifice （或称BO ）使庞大的网络系统轻而易举地陷入了瘫痪之中。安装BO主要目的是：黑客通过网络远程入侵并控制受攻击的Win95 系统，从而使受侵机器“言听计从”。BO 以多功能、代码简洁而著称，并且由于BO 操作简单，只要简单地点击鼠标即可，即使最不熟练的黑客也可以成功地引诱用户安装Back Orifice 。只要用户一安装了Back Orifice ，黑客几乎就可以为所欲为了，像非法访问敏感信息，修改和删除数据，甚至改变系统配置。如果仅仅从功能上讲，Back Orifice 完全

可以和市场上最流行的商业远程控制软件媲美！

3、未来的几种攻击机制

超级蠕虫：

无论是手段的高明性，还是后果的危害性，计算机网络受到蠕虫的威胁都在激增。在我们的民意调查中显示人们仍旧将这一威胁看作是计算机网络将面临的最大威胁之一，有超过36%的人认为超级蠕虫的威胁应该摆在第一位。超级蠕虫一般被认为是混合蠕虫,它通常能自我繁殖,并且繁殖速度会变得更快,传播的范围会变得更广。更可怕的是它的一次攻击就能针对多个漏洞。例如,超级蠕虫潜入系统后,不是仅仅攻击某个漏洞，而是会尝试某个已知漏洞，然后尝试一个又一个漏洞。超级蠕虫的一枚弹头针对多个漏洞发动攻击，所以总有一个会有效果。如果它发现你未打补丁的地方，那你就在劫难逃了。而事实上没有哪家公司的系统完全打上了所有的补丁。很多安全专家逐渐看到的通过IM(即时消息)进行传播的蠕虫就可以说是一种超级蠕虫。黑客将一个链接发给IM用户后，如果用户点击链接，蠕虫就会传播给该用户的IM地址簿上的所有人。有了IM,用户将随时处于连接状态,所以也随时会受到攻击。(建议用户参考安络科技的专题文章:《八月震撼 点对点(p2p)通信对信息安全构成严重威胁》，并请关注前段段时间出现过的“MSN Messenger ”病毒)。

为对付未来的超级蠕虫我们所能做的将是：对外部可访问系统进行安全加固，像Web 服务器、邮件服务器和DNS服务器等，尽量将它们所需要开放

的服务减少到最小；给系统及时打上补丁、及时更新防病毒软件，对员工进行安全宣传和教育；使用基于主机的入侵检测系统和预防工具，例如 Symantec 的 Intruder Alert 3.6 可以阻断或迅速发现蠕虫的攻击。

隐秘攻击 (Stealthier Attacks)：

现在越来越多的黑客把攻击后成功地逃匿IDS的检测看作是一种艺术，有许多新工具将能使他们在攻击用户的系统后，不会留下任何蛛丝马迹，有多种高级黑客技术将能使之成为可能，而这些技术已经被广泛地为专业黑客和一些高级的脚本菜鸟（Scripts Kids)所采用。

多变代码：

这些恶意软件其本身可能是一种病毒，蠕虫、后门或漏洞攻击脚本，它通过动态地改变攻击代码可以逃避入侵检测系统的特征检测（Signature-based detection，也可称为模式匹配）。攻击者常常利用这种多变代码进入互联网上的一些带有入侵侦测的系统或IDSes入侵者警告系统。

Antiforensics：

攻击者可操作文件系统的特性和反侦测伎俩进行攻击来逃避 IDS的检测。例如通过利用像Burneye这样一个工具，可以掩盖黑客对系统的攻击企图，使用 Defiler的工具 Toolkit可以覆盖黑客对目标文件系统所做的修改留下的蛛丝马迹。

隐蔽通道：

为了和后门或者恶意软件进行通讯，攻击者必须建立一条非常隐蔽的通信通道。为此，攻击者常常将通讯端口建立在一些非常常用的通信协议端口上，像HTTPS或者SS。

内核级后门(Kernel-level root kits)：

通过从系统内核控制一个系统，攻击者获得对目标系统的完全控制权限，而对受害者来说却一切都似乎风平浪静。

嗅探式后门(Sniffing backdoors)：

通过将后门和用户使用的嗅探器捆绑在一起，攻击者能够巧妙地绕过用户使用的传统的通过查看正在监听的端口来发现后门的检测方法，使受害者被种了后门却还一直蒙在鼓里。

反射式／跳跃式攻击：

与其直接像目标系统发送数据，很多攻击者觉得还不如利用TCP/IP欺骗技术去以误导正常的检测，隐蔽攻击者的真实地址。像反射式D.o.S攻击就是例证。

针对以上这些诡秘的攻击，作为用户又该如何防范和阻止呢？

如果你的系统遭到这种攻击，你需要能够迅速地检测出来，而且要知道攻击者具体在你的系统上干了写什么。为了能够察觉出这种入侵，需要同时使用基于网络和基于主机上的入侵检测系统和防病毒产

品，并仔细检查你的系统日志。一般用户可能不具备这种专业能力，可以寻找一家高专业水准的信息安全签约服务商，为您提供高水平的反入侵服务。

2 一旦你发现自己的系统有什么异常，你必须确保你的事件紧急响应小组在取证分析上有丰富的经验，能够熟练使用像@ stake 的免费TASK 工具或者 Guidance Software 的商业软件EnCase ,因为这两个工具都能非常仔细对系统进行分析，并且非常精确地隔离攻击者的真实破坏活动。重点部门的事件响应小组可以和专业安全服务商共建，明确分工，及时处理。

4、未来的网络恐怖主义

利用程序自动更新存在的缺陷：

主流软件供应商，像Microsoft 和Apple Computer 等都允许用户通过Internet 自动更新他们的软件。通过自动下载最新发布的修复程序和补丁，这些自动更新工具可以减少配置安全补丁所耽误的时间。但是程序允许自动更新的这个特征却好比一把双刃剑,有有利的一面,也有不利的一面。攻击者能够通过威胁厂商Web站点的安全性,迫使用户请求被重定向到攻击者自己构建的机器上。然后，当用户尝试连接到厂商站点下载更新程序时，真正下载的程序却是攻击者的恶意程序。这样的话攻击者将能利用软件厂商的自动更新Web 站点传播自己的恶意代码和蠕虫病毒。

在过去的岁月中，Apple 和 WinAmp 的Web站点自动更新功能都被黑客成功利用过，所幸的是发现及时(没有被报道)。Apple 和 WinAmp 后来虽然

修复了网站的缓冲溢出缺陷，并使用了代码签名(Code Signing)技术,但基于以上问题的攻击流一直没有被彻底清除。为了预防这种潜在的攻击威胁，需要严格控制和管理安装在你的内部网机器上的软件，禁止公司职员随意地安装任何与工作无关的应用软件。在这里,你可以使用软件管理工具来强迫执行,像Microsoft 的 SMS,LANDesk SOFTware 的LANDesk 这两个工具只要二者择其一，你就可以配置你的内部升级服务器，如通过在工具中对微软软件升级服务器相关选项进行配置，你可以具体选择哪个修复程序和补丁允许被安装。为保护你的网络，可使用sniffer 测试所有的补丁，如发现网络流量不正常或发现开放了陌生的端口则需引起警觉。

针对路由或DNS 的攻击：

Internet 主要由两大基本架构组成：路由器构成Internet 的主干,DNS 服务器将域名解析为IP 地址。如果一个攻击者能成功地破坏主干路由器用来共享路由信息的边界网关协议(BGP)，或者更改网络中的DNS 服务器,将能使Internet 陷入一片混乱。攻击者通常会从头到脚，非常仔细地检查一些主流路由器和DNS 服务器的服务程序代码，寻找一些能够使目标程序或设备彻底崩溃或者取得系统管理权限的缓冲溢出或其他安全缺陷。路由代码非常复杂，目前已经发现并已修复了许多重要的安全问题，但是仍旧可能存在许多更严重的问题，并且很可能被黑客发现和利用。DNS 软件过去经常发生缓冲溢出这样的问题，在以后也肯定还可能发生类似的问题。如果攻击者发现了路由或DNS 的安全漏洞，并对其进行大举攻击的

话，大部分因特网将会迅速瘫痪。为了防止遭到这种攻击，确保你的系统不会被作为攻击他人的跳板，应采取如下措施：对公共路由器和外部DNS 服务器进行安全加固，如果公司的DNS服务器是为安全敏感的机器提供服务,则应为 DNS 服务器配置防火墙和身份验证服务器 确保DNS 服务器安装了最新补丁，对DNS 服务器严格监控；如果你认为是由 ISP的安全缺陷造成的威胁，确保你的事件紧急响应小组能够迅速和你的ISP取得联系，共同对付这种大规模的网络攻击。

同时发生计算机网络攻击和恐怖袭击：

这可以说是一场双重噩梦：一场大规模的网络攻击使数百万的系统不能正常使用，紧接着，恐怖分子袭击了一个或者更多城市，例如一次类似“9.11 ”的恐怖爆炸！