计算机网络风险及其安全防范方式分析

武亚宏
（中泰证券股份有限公司，山东 济南 200120）

摘 要 当前国民经济与网络技术的关联性越来越大，网络正在国民经济中发挥着越来越大的作用。那么保证网络的安全性，遏制黑客的猖狂与攻击，对国民经济的健康发展以及社会的稳定和谐都有非常重要的意义。近年来，由于计算机网络技术的发展以及其对网络环境影响的两面性，一方面为我们带来了更多便利的工具以及技术；另一方面也造成了越来越多的计算机网络安全漏洞，无论是对于企业还是个人用户而言都是如此。计算机病毒、黑客疯狂的攻击手段，已经令许多企业和个人蒙受损失。本文分析了网络条件下的各种风险，并提出相应的解决策略和预防措施，旨在解决企业或个人网站中存在的安全问题，为我国人民目前工作、生活及经济发展的需要提供助益。

关键词 网络风险 计算机病毒 黑客攻击 网络钓鱼
中图分类号：TP39 **文献标识码**：A **文章编号**：1007-0745(2022)03-0098-05

人们将计算机病毒称之为“21 世纪最大的隐患”“不流血的致命武器”，在国际上还没有一套成熟的法律体系来制约网络犯罪，它的出现完全有可能改变人类的未来，因此网络风险防范的任务就更加艰巨了。随着计算机网络技术的发展，网络风险如黑客、病毒、钓鱼邮件等对信息安全的威胁日益严重。我们必须从自身做起，一方面要认真了解网络风险的本质，另一方面要加强网络风险防范策略的研究，真正做到防患于未然，提前做好风险防范策略上的准备，严阵以待，保障我们的信息安全。本文的研究旨在分析网络条件下的各种风险，如黑客攻击、病毒感染等网络攻击形式，从而针对性地提出网络攻击的预防及解决措施。

1 网络风险的主要形式和组成

1.1 网络病毒

网络病毒在网络中赫赫有名，即使是不常使用计算机的人，也都听过病毒的厉害。

网络病毒并不是现实生活中的病毒生物，他不会对人体产生伤害，它是人为创造的一段程序代码，刻意地对计算机进行破坏或偷窃数据信息。最初的网络病毒出自一些电脑高手如高级程序员等人之手，是用于提高信息共享度的一种模式与手段。而到今天，病毒已经改头换面，呈现多样化的形式，随着互联网技术的持续发展，病毒技术的使用开始带有不正当的目的，病毒的制造者也已经发展成网络上的一个独特的群体，被称之为黑客。他们有着与常人不同的理想和追求，有着自己独特的行为模式，并开始呈现组织化、团体化的趋势，危害也日益增强了。网络在持续复杂化，而黑客开始使用病毒持续攻击电脑用户的终端或者企业的服务器，攻击技术也层出不穷，病毒开始被定义为人类的公敌，人人得而诛之。同时网络病毒还有很多特点如：感染速度极快、扩散面极广、传播形式多元化、无法彻底清除等等，每次新的网络病毒爆发，都会造成大量的经济损失。图 1 是主要网络病毒类型的统计。

1.2 黑客攻击

黑客英文为 Hacker，他们通常精通计算机技术，出于炫技或者是其他扭曲心理，通过其精湛的硬件知识进行程序的编制，实现计算机病毒的散播。一部分黑客仅仅是出于猎奇心理，无意贻害公众，但是其所制造的程序的散播，还是会造成社会危害。还有一部分黑客本身就仇视社会，那么其编制的黑客程序或者病毒危害性就很大了。例如，曾经发生在美国的一起恶劣事件，一家知名计算机公司辞退了一名程序员，导致该程序员心生不满，决定对公司进行报复，在离开前设计了一个病毒程序，并植入了公司计算机系统里，结果这个病毒潜伏了 5 年多才发作，造成该公司整个计算机系统的紊乱，导致了巨大的经济损失，对该公司的经营造成了非常严重的危害。现实中存在各种各样的黑客，我们可以从表 1 的统计了解主要的黑客类型。

黑客攻击一般分为破坏性攻击和非破坏性攻击两

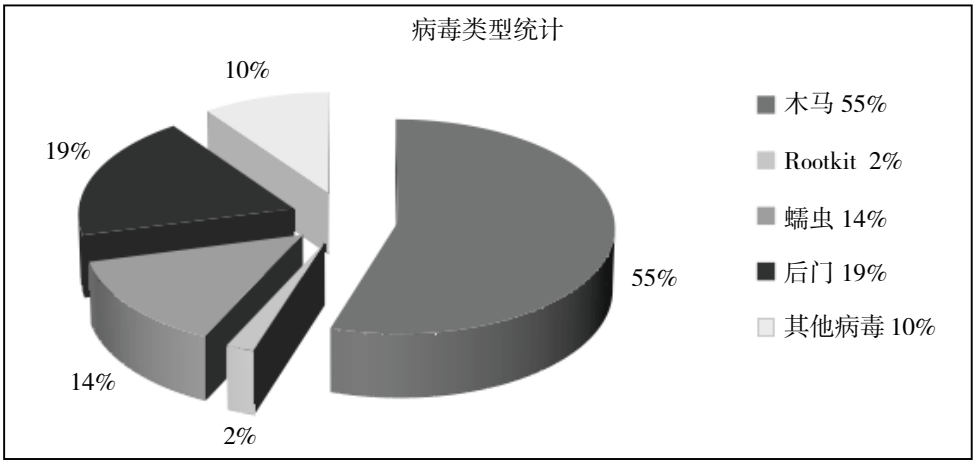

图 1 主要网络病毒分类及比例

表 1 黑客主要种类汇总

黑客种类	具体行为
白帽黑客	实施渗透测试，识别网络安全漏洞。
黑帽黑客	未经授权访问电脑系统和重要数据。
灰帽黑客	利用自己的技能谋取私利。
脚本小子	使用其他黑客提供的脚本或下载工具进行黑客攻击。
绿帽黑客	业余爱好者，关心黑客行为。
蓝帽黑客	黑客领域的新手，偶有报复行为。
红帽黑客	阻止黑帽黑客，处理恶意软件。
国家资助黑客	政府指定的为其提供网络安全并从其他国家获取机密信息。
黑客主义者	未经授权访问政府的电脑文件和网络，以达到社会或政治目的。
恶意内部人或举报人	公司或政府机构雇员，利用所获得的信息实施敲诈行为。

类，破坏性攻击一般指黑客创造的病毒破坏计算机设备或使计算机设备无效运作，消耗计算机设备的寿命，另外盗取保密信息等行为也被视为破坏性攻击。非破坏性攻击一般指黑客的攻击行为不对系统进行破坏、不盗取保密信息，但是它扰乱系统的正常工作，阻止系统对外提供正常服务，使系统瘫痪，我们常说的 DOS 攻击就是属于这种类型。无论是破坏性攻击还是非破坏性攻击，都会给我们正常的工作生活带来极大的困扰，甚至造成重大的损失。

1.3 网络钓鱼

有一种网络仿冒形式，国际上称为 Phishing，也就是我国统称的网络欺诈、网络仿冒或者钓鱼。网络钓鱼是网络攻击者传播网络病毒的一种流行方法，通过网络邮件、聊天工具让受害者下载一个文件或访问一个链接，从而植入木马恶意软件、勒索软件或进行破坏性攻击。用户的个人信息、银行账户和密码口令等信息在不知情的情况下被这些钓鱼软件或仿冒网站套取。或者是遭遇在计算机当中植入的木马，该类木马通过假网页或者诱骗邮件等等形式传播，植入恶意代码，骗取个人信息。网络钓鱼是在电子商务交易中最为普遍的一种安全漏洞攻击方式，通过某调查显示，有大约九成网购爱好者在与电商进行网络交易的时候遭遇过网络钓鱼，其发生率在近几年已经超过木马，由于网络钓鱼是十分隐蔽的，普通电脑用户在触发钓鱼程序时毫不知情，甚至一些警惕性不高的用户通常在账户内的资金数目发生了较大的改变时才会察觉，而此时所遭受的经济损失已经十分严重。由此不仅为淘宝、京东、拼多多等电商集团的经营操作带来许多买卖纠纷，也为这些电商集团的品牌形象带来了很大

的负面影响，在一定程度上扼制了其电子商务规模的扩展[1]，对其企业经营的负面影响可想而知。

还有一些更复杂的网络钓鱼方式，它需要漫长的时间。钓鱼攻击者利用虚假的社交媒体资料、电子邮件等与受害者建立联系，在几天、几周、甚至几个月的时间里，骗取受害者的信任，然后获取受害者本人及其家人朋友的信息数据，因为人们只会将数据交给自己信任的人。这些数据可以是个人或朋友的联系方式、聊天记录、住址、出生日期等个人数据，也可以是公司的地址、邮箱及密码，甚至可以是信用卡信息、网上银行支付密码等财务数据。在网络攻击者手中，所有这些信息都可以被用来进行诈骗、勒索或让受害者难堪，比如身份盗窃，或者用偷来的数据购买物品，甚至勒索受害者支付赎金购买这些信息。无论攻击者用这些信息干什么，都将对受害者带来无可挽回的损失。

2 网络风险的危害及其危害方式

2.1 网络风险的危害

2.1.1 信息泄露

网络风险的危害是众所周知的，人人都可能中招，却又无可奈何，因此在购进电脑后第一件事就是安装杀毒软件，因为病毒就是网络风险最大也是最主要的风险来源。人们之所以害怕病毒是因为它可能给我们带来的潜在损失，比如计算机的瘫痪，又如黑客攻击一旦发生，被攻击的电脑将失去正常的速度、功能乃至无法使用，影响正常工作。更严重的，个人的生活隐私信息遭到窃取，则可能造成个人事业方面无可挽回的影响，又或者会造成公司产品、财务、人员等信息泄露，此种信息泄露危害更大，严重时可能会导致公司破产，无法经营下去。无论是哪一种信息泄露，都是非常严重的事情，然而当前从网络风险的角度来说，信息泄露的危险无处不在，哪怕是家用电脑没有开启的摄像头，也能够成为黑客用以窃取私人信息的手段，电脑科技应用的同时，也会成为人们日常生活及工作中的潜在危险，不得不防。

2.1.2 财务损失

网络风险带给我们的第二个损失就是财务损失，电商时代网络购物成为主流，包括各种费用的缴纳如水电费、物业费等，都可以通过网络完成，而黑客则可能通过技术手段如植入病毒、木马等窃取个人账户密码，进而窃取账户资金。它给我们带来的损失可大可小，然而无论是什么样的损失，都是我们所不愿意遭遇的，因此我们在计算机使用的过程中，需要将网络风险如病毒等视为头号天敌，每日都要杀毒和清理系统。此外，当个人在进行网络支付的同时，可能使用了密码储存或者免密支付的操作，这些储存在网络系统当中的信息同样有遭到泄漏和造成财务损失的风险[2]。一旦自己的家用电脑被远程操控的木马所控制，入侵者将如入无人之境，这同样是值得我们重点防控的。

2.2 网络风险的危害方式

2.2.1 攻击计算机漏洞

电脑的系统漏洞，是黑客攻击的一个非常重要的途径。我们日常使用的各种电脑终端，通常都有各种安全隐患，来自不完备的系统性能以及设备固有的先天性能缺失等等[3]。通常的电脑使用者，如果缺乏专业的电脑技术，往往无法填补这些漏洞。此外，电脑用户后期的使用不当，如补丁安装的不及时等等，都会给黑客攻击提供突破口[4]。一系列公开化的工具，扫描器也是黑客发现计算机漏洞的重要手段。其扫描的具体原理如下：

1. 全 TCP 连接。

2.SYN 扫描（半打开式扫描）。

发送 SYN，远端端口开放，则回应 SYN=1，ACK=1，本地发送 RST 给远端，拒绝连接。

发送 SYN，远端端口未开放，回应 RST。

3.FIN 扫描（秘密扫描）。

本地发送 FIN=1，远端端口开放，丢弃此包，不回应。

本地发送 FIN=1，远端端口未开放，返回一个 RST 包。

2.2.2 利用木马入侵电脑

木马的植入，是黑客进行计算机系统攻击的第二大方式。专门的木马程序，可以针对特定的电脑终端种类进行运作。电脑的使用必须要联网，而网络功能的完善，为用户提供了各种各样的服务功能如阅读、购物、视频观看等等[5]。这个过程中端口是开放的，那么黑客就有了可乘之机。他们可以进行网络系统路由器路由表的查阅，从而获取目标主机所在网络的拓扑结构及其内部细节的 SNMP 协议，进而通过该程序获取达目标主机所要经过的网络数和路由器数的 traceroute 程序，从而实现对终端电脑的入侵，造成电脑各种使用功能的故障。

2.2.3 利用管理工具攻击系统

企业或者其他集团机构的办公区域通常使用局域网的形式进行联网，各局域网由管理者进行管理，为

了方便，许多网络管理者会进行网络监测器的安装，其初衷是为了方便管理，并提高局域网内的计算机安全系数[6]。然而黑客也可能利用该管理工具，进行局域网系统主机的控制，从而造成不可预料的后果。黑客一旦掌握了网络检测器信息，就能够控制主机，进而实现对局域网内其他机器的控制，从而控制整个局域网的网络信息出入，并截获大量的商业信息、重要机密等等。当前社会计算机的使用日驱普遍，用户逐日增多，然而并不是每个人对系统的安全性都有完备的知识[7]，很多用户安全意识缺失，各种对安全防护的手段的忽视都给黑客提供了可乘之机。

黑客利用管理工具进行的系统攻击还表现为篡改网页、僵尸网络两方面。僵尸网络又被称为 Botnet。Bot 为 Robot 的缩写，它可以自动执行被定义的功能，也可通过预定义的指令对其进行控制，已经实现了一定的人工智能化，通过溢出漏洞攻击、蠕虫病毒、共享网络、猜测密码以及 P2P 软甲等等进入用户计算机。一旦进入，便能够联系上处于局域网内的一台或者多台控制主机，形成一个控制网络。黑客则是通过这个控制网络发送控制指令，使这些计算机甚至控制服务器，都成为“Botnet”的一部分。此情形一旦爆发，受害者的应对措施往往无法做到及时和全面，导致计算机病毒肆意传播和黑客指令无法得到及时的扼制。它们对许多公司企业的业务网站造成了极大的破坏性影响，破坏方式主要表现在三个方面：一是利用一些特殊的软件，在短时间内向用户团网络服务器发出大量超出系统负荷的信息，造成其服务器超负荷、网络堵塞以及系统崩溃的状况。二是对系统进行非法访问，获取大量的用户信息，使得广大用户的利益受到了严重的威胁。三是对用户系统进行非法访问，窃取其公司的商业信息，不仅造成了程序与数据的丢失，亦使系统表现出异常动作，如生成不可见的表格文件或者特定文件，显示出一些无意义的画面、问候语等。

2.2.4 钓鱼邮件

钓鱼邮件指网络攻击者利用伪装的电子邮件，引诱收件人打开藏有木马程序的附件，或引导收件人点击邮件中的网页链接、扫描二维码加入某个微信群等方式获取、诱骗收件人或其公司的信息。网络攻击者利用获取的这些信息通过敲诈、售卖等方式获取非法利益，全球每年都会因钓鱼邮件造成大量经济损失。虽然钓鱼邮件已经成为我们日常工作生活中网络攻击的防范重点，但是钓鱼邮件的种类繁多，格式各样，令人防不胜防。典型的钓鱼邮件有：仿冒邮件、链接钓鱼邮件、附件钓鱼邮件、商务诈骗邮件、二维码钓鱼邮件等等。这些钓鱼邮件都有显著的特征，那就是非常逼真，从而使我们难以防范，再加上盲目的信任邮件服务器的防范措施，导致我们对收到的“正常”邮件不再加以辨别，从而常常让网络攻击者的奸计得逞，造成信息泄露或经济损失。

3 网络风险的防范技术分析

3.1 加强网络风险防范意识

俗话说最大的风险就是不知道存在风险。当前互联网技术的发展日新月异，新功能、新应用层出不穷，网络风险也在不断加大和不断翻新，从常见钓鱼邮件、木马攻击，到少见的安全漏洞、DOS 攻击等等都在不断变化，造成了个人及企业的大量损失。因此我们要加强网络风险的防范意识，增强学习、培训，尤其是非专业人员的培训，让他们认识到网络风险的多种多样，从而时刻保持警惕之心，这样才能更好地防范网络风险。

3.2 日常体检、杀毒

要制止网络风险，我们当前最常用的防范措施就是每天体检、杀毒。杀毒软件已经是每台电脑的标配，只有不断更新杀毒软件版本，并进行日常的电脑扫描，才能够将潜藏于电脑操作系统当中的木马、病毒及时清除。这样就能制止病毒在电脑系统内的进一步散播和攻击行为，同时，具有一定计算机技术功底的人，还可以用专门的系统设计如 NET 技术的功能模块化管理等，使用专有的数据库，能够避开病毒与木马传播的一般路径。例如为了保护气象行政许可专门设计的系统，基于 .NET 技术，采用功能模块化的管理，将功能模块的权限授予使用者，权限使用 Session 验证，系统将数据逻辑都写在程序代码中，数据库采用 SQL Server 2005，从而大大增强了防范网络攻击的力度。

3.3 检查端口，及时制止黑客攻击

日常体检需要作为必要工序，计算机用户还必须经常进行计算机端口的检查，查看有没有闲置的端口或者程序[8]。如果有程序在运行而自己并没有使用，就说明是外来的黑客程序入侵了。此时，我们可以马上杀毒，或者第一时间断网，切断黑客对电脑的控制路径。然后彻底清理计算机系统，清除所有的黑客程序及病毒，再恢复网络连接。在网络处于接通状态的时候，也要注意减少端口的开放，从而减少病毒进入的路径[9]，为了在防止黑客入侵的同时不影响我们正常上网，只

（下转第 117 页）

4 结论

1. 综合考虑工程概况，从计算方法、计算载荷、工程地质、计算模型及重要力学参数取值等方面，结合“港口地基工程计算系统”，经复核计算，堤身开槽施工不会影响防波堤稳定性。

2. 在四种施工工况中，防波堤临海侧的稳定性总是高于防波堤内侧。

3. 在四种施工工况中，堤身斜坡面表层开槽（工况一）对防波堤稳定性影响最大；堤顶电缆沟开槽（工况二）对防波堤稳定性影响最小。

参考文献：

[1] 韩意，张磊，吴伟东，等 . 改进型四脚空心方块海尔港防波堤的稳定性分析 [J]. 海洋湖沼通报 ,2020(05):32-39.
[2] 李彦卿，别社安 . 宽肩台防波堤稳定性数值模拟方法研究 [J]. 海洋通报 ,2020,39(06):10.
[3] 陈昊哲，陶然 . 斯里兰卡某深水防波堤结构设计与稳定性试验 [J]. 中国港湾建设 ,2021,41(06):41-45,79.
[4] 中交天津港湾工程研究院 . 水运工程地基设计规范 (JTS147-2017)[S]. 北京：人民交通出版社 ,2018.
[5] 仇锦先 . 新沭河堤防防渗处理开槽施工的几点体会 [J]. 水利水电科技进展 ,2002(04):46-48.
[6] 李二霞 . 滹沱河北大堤垂直铺塑开槽施工控制谈 [J]. 河北水利 ,2004(10):29-30.
[7] 孙兆地，李志华，宫晓琳 . 基于雄安新区高标准防洪工程建设模式探讨生态型堤防未来设计趋势——以雄安新区萍河左堤防洪治理工程为例 [J]. 中国水利 ,2021(20):86-89.
[8] 同 [4].
[9] 同 [1].
[10] 崔志芳，王学潮，尚锋，等 . 开封某堤段截渗墙施工异常与地质条件关系分析 [J]. 人民黄河 ,2001(09):16-17.
[11] 朱国康 . 海堤加固工程典型断面沉降的复核计算及应用 [J]. 黑龙江水利科技 ,2021,49(10):133-136.

（上接第 101 页）

开放 80 端口就行了，如果还需要上 pop 再开放 l09、1l0。不常用的或者几乎不用的全部关闭，不给黑客的攻击提供机会。

3.4 谨慎安装电脑软件

电脑的使用频率越高，被黑客光顾的概率也就越高。相对而言，有效应对黑客的手段是防患于未然，平时应加强警惕。对于网页推荐的或者是不熟悉的软件，在使用或者安装的时候都要慎之又慎。对于一系列没经过认证、来源不明、内容混乱的网页，尽量不要打开，以避免相关风险 [10]。同时，对于应用安装过程中系统提示的软件安装通知，我们也应当尽量只选自己需要的，避免被黑客所利用，从而大大降低被黑客攻击的风险。在已经遭遇黑客的情况下，应当第一时间关闭网络连接、专业重要信息，并更改计算机信息，截断黑客的电脑控制权，及时止损。

4 结论

网络环境虽然险恶，存在许多弊端，但是它给人们带来的便利也是实实在在的。当前网络技术仍然不成熟，各种漏洞层出不穷，而这就是黑客生存的土壤。虽然各种网络风险的存在，给我们的工作生活带来了很多困难，但它也倒逼着我们网络技术的发展。因此我们期待随着网络技术的发展，Internet 可以提升安全技术，从而保障网络运行环境的安全，使人们能够更安心地使用网络终端。

参考文献：

[1] 李燕 . 由支付宝看我国第三方支付平台 [J]. 广西质量监督导报 ,2008(02):26-27.
[2] 骆炎平 . 基于 SWOT 分析的网络银行经营研究 [J]. 现代商贸工业 ,2009,21(14):101-104.
[3] 张炜，许研 . 电子商务概论 [M]. 北京：经济科学出版社 ,2010.
[4] 陈鑫 .C2C 电子商务平台欺诈问题研究 [J]. 电子商务 ,2011(07):22-23.
[5] 张伟 . 浅谈电子商务安全问题 [J]. 吉林农业科技学院学报 ,2008,17(04):74-75.
[6] 陈鑫 . 网上交易安全问题研究 [J]. 电子商务 ,2011(09):43-44.
[7] 李阳，胡高格 . 构建安全的电子商务第三方支付平台——浅谈电子商务第三方支付平台的发展 [J]. 中国电子商务 ,2012(08):20-21.
[8] 王升保 . 信息安全等级保护体系研究及应用 [D]. 合肥工业大学 ,2009.
[9] 胡曼 . 基于 Linux 系统的在线安全认证中心的构建及研究 [D]. 山东大学 ,2009.
[10] 李振汕 . 黑客攻击与防范方法研究 [J]. 网络安全技术与应用 ,2008(01):16-18.