智能化网络安全防攻击检测中数据抽取和分析

王思语
北京先进数通信息技术股份公司　北京　101300

摘　要：在网络高速发展的时代，每个人都和互联网脱离不了关联，而互联网安全也越来越成为人们关注的热点。随着信息化时代的到来，网络给人们的生活带来了无限的便利和快捷，但同时也给人们的生活带来了诸多的安全隐患，比如网上个人身份信息泄露等等。可以说，在某种程度上，网络其实是一把双刃剑，在给人们带来一定的便利的同时也会带来一些潜在的威胁。而我们每个人都身处于互联网时代中，网络安全越来越成为众多网络用户最关心的一件事情。本文主要就防止网络安全受到攻击的检测为主，从中抽取数据进行分析。主要内容就以下几个方面开始展开：首先，阐述网络安全相关的概念；其次，阐明了网络安全现阶段面临的问题；最后介绍了应对这些问题的解决办法。

关键词：网络安全；防攻击；智能化

Data extraction and analysis in intelligent network security anti attack detection

Siyu Wang
Beijing advanced digital communication information technology Co., Ltd. Beijing 101300

Abstract: in the era of rapid development of the network, everyone can not be separated from the Internet, and Internet security has increasingly become a hot spot. With the advent of the information age, the network has brought infinite convenience and rapidity to people's lives, but it has also brought many security risks to people's lives, such as the disclosure of online personal identity information and so on. It can be said that, to some extent, the network is actually a double-edged sword, which will bring some potential threats while bringing some convenience to people. Each of us is in the Internet age, and network security has increasingly become the most concerned thing of many network users. This paper mainly focuses on the detection to prevent network security from being attacked, and extracts data from it for analysis. The main content mainly starts from the following aspects: first, it expounds the concepts related to network security; Secondly, it clarifies the problems faced by network security at this stage; Finally, it introduces the solutions to these problems.

Keywords: network security; Anti attack; Intellectualization

一、网络安全的相关概念

（一）网络安全的含义

防止计算机网络系统中的一些软件、数据以及硬件不受到外部的恶意攻击或者其他各种因素的破坏。主要包括以下几个方面：用户未授权的网络数据在未经用户同意的情况下，没有被随意改变；信息传递者将信息传递给信息接收者的过程中，信息是完整的，而且该信息不会被泄露或者被破坏；用户在传递信息的过程中不会被恶意软件所截取其信息内容或者读取其信息的内容等等[1]。

（二）影响网络安全的因素

网络安全最主要的影响因素主要有以下几个：

1.网络系统的设计问题。在某种程度上可以说，网络设计的好坏是直接导致网络是否安全的最主要因素。如果设计师在设计网络系统的时候没有全面的考虑到所有的因素，那么网络系统中就会出现漏洞从而导致用户的数据泄露等等各种严重的问题。

作者简介：王思语，汉，河南，本科，ETL工程师，研究方向：ETL工程相关工作。

2.网络没有安全和严密的策略。关于网络的安全策略是实施用户的网络安全计划之前所需要做的一个非常充分的准备的阶段，或者说，这种策略是对网络安全防护设置的一种具体的行动。但是在很多情况下，用户的计算机网络的防火墙中设置的选项中，往往都扩大了用户的访问权限，这就很容易导致很多网络上的不法分子对用户的网络系统进行一些恶意的篡改和破坏。

3.局域网络的安全问题。局域网络是常常用来联系计算机和资源共享的一种渠道。局域网络有一个最大的特性就是开放性，但它的这种特性也很容易导致用户的信息被泄露。如果在局域网中再次设置上访问的控制配置，这在一定的程度上是可以提高用户计算机网络的安全性的，但是这种设置非常复杂，而且它还有一个缺点，就是会给别人提供一些可乘之机，对用户的计算机造成一定的损害。

（三）网络安全的发展趋势

网络安全的发展趋势主要体现在三个方面。首先是入侵检验的技术的发展，其次是防火墙技术的发展，最后是防病毒技术趋势的发展。

1.何为入侵检测技术呢？入侵检测技术就是对网络上的各种信息进行收集和整理，然后再对这些收集到的信息进行数据分析，最后对网络用户的系统进行检测。如果用户的主机系统受到网络上的不良攻击，或者用户在使用网络的过程中有违反计算机网络系统安全的违规行为，这种入侵检测技术就可以检测到。这也是对网络进行一个智能化的检测，这种智能化的检测是我们未来提高入侵检测技术的一个重要的突破口。

2.网络安全最主要的两大危险因素就是病毒以及黑客，那么我们提高防病毒的技术水平就能对遏制病毒和黑客的网络攻击具有很重要的意义。在一定程度上，在最大程度上来发展防病毒技术，可以通过查杀网络系统病毒来实现，以此同时，把防治病毒和黑客攻击两者进行有效的结合，也是这种技术未来发展的一个新趋势。最主要的是要从网络的入口处拦截网络病毒，因为在入口处拦截病毒是我们防止网络病毒入侵用户的网络系统的最主要的办法，也是最根本的办法。目前市面上有很多的计算机网络的生产商家也正在加大研究的力度，努力研发有效的防病毒软件以及防病毒的程序，把防病毒的这种软件和程序直接配置到用户的网络安全管理的方面[2]。

3.防火墙技术是很多网络用户最熟悉的一项计算机防护功能。而现在的。防火墙技术的防护水平以及各大商家研制出来的这种防火墙的产品都不是很成熟。在用户使用计算机网络的过程中，防火墙技术的缺陷使得其在使用过程中存在一定的安全隐患，这也使得很多网络用户对网络安全的需求得不到很大的满足。所以很多商家也在防火墙技术的发展领域不断的创新和提高它的防护功能，同时提高计算机网络处理信息的速度。要创新防火墙技术的发展，最重要的一点就是加大创新力度的投入，这样才能使得用户计算机网络上的防火墙技术具有更强的防护功能，使用户的计算机得到更加稳定的发展。随着计算机网络环境的快速改变，这项技术也在不断的发展，并且在发展中不断的进步，这也使得很多网络用户对其产生了越来越多的好感。最值得说的是这项防火墙技术如果被应用到用户的计算机网络加速方面，就能在很大程度上扩大对用户网络系统的服务功能以及安全保护功能。这也是对防火墙技术取得重大发展的一个重要的突破口，也是它创新的必经之路，现在很多的计算机网络都在着力于防火墙技术的研究，然后解决现在存在的一些网络上的安全问题。

二、网络安全的现状

（一）网络病毒的入侵

网络安全中最常见的问题就是网络上有病毒入侵。这种情况是网络安全中最常见的问题，一般会在用户使用计算机网络的时候出现。这种入侵的网络病毒其实就是一些不法人员通过特殊的代码或者特殊的指令而编写的，一种主要用于攻击网络用户的计算机网络系统的病毒。它对于用户网络安全的威胁非常大，有时候甚至能够让用户的网络进入死机，让用户的计算机系统进入无限死循环，从而最终减弱用户使用计算机的工作效率。随着科技而新月异的发展，社会不断的进步，这种网络病毒也在不断地进行创新，不断的进行改进，从之前单一的形式变为现在多样化的入侵形式，比如一封匿名邮件，一张匿名的卡片，或者是一个匿名的网址等等，这就极大地增加了网络用户对其防御的难度，使得我们对网络安全的进一步保护更加难以开展。随着一些不法分子对病毒进行不断的更新与升级，这些计算机网络病毒对用户计算机网络的破坏能力也在越来越显著。他们不仅破坏了用户的主机系统，而且还可以窃取用户在某些平台上所授权的一些身份信息，其中包括身份证信息、银行卡信息等等[3]。

（二）黑客的入侵

黑客攻击也是现代网络计算机最常见的一种攻击方式，某些不法分子以盗取目标用户网络计算机中的个人

身份信息或者隐私信息为目的，利用一些专业的科技侵袭软件进入到网络用户的主机系统中，其中有很多表现形式，主要有：将网络用户的隐私文件或者信息进行盗取或者篡改；有的甚至直接将用户的加密文件盗走，从而导致用户的网络计算机系统受到侵袭。这些不法分子把一些黑客的攻击程序进行编辑，根据自身需要编辑成不同的黑客程序，成功编辑好之后，把编辑的程序直接发布在各个用户的网络系统中，从而进行大量的传播，而这些网络用户一旦访问有访问记录或者是点击过他们编辑好的程序，那么这些用户的电脑网络系统就会立即瘫痪，甚至死机。而且甚至可能造成一些重要文件的丢失。这些网络黑客随着信息技术的发展也越来越多，而且他们也逐渐成为危害计算机网络环境的一个最大的因素。由黑客引起的一些计算机网络袭击造成的很多问题都没有解决，现在的很多不法人员对一些常见的黑客技术，甚至是一些创新性的黑客技术都非常的了解，他们非常的熟悉如何入侵网络用户的电脑，而且他们也可以设计出很多侵略网络用户电脑的路径，使得网络用户即使非常努力地防范自身系统的安全，也没办法保障自己电脑系统的安全。即使现在国家和相关部门一直在严厉打击这种黑客行为，但是还是并不能非常有效地杜绝这种行为。

（三）安全防护漏洞不足

随着网络的发展，当今社会上很多用户在使用电脑网络时严重缺乏网络安全知识，就拿我们平时设置的登录密码来举例，很多网络用户设置账户登录密码设置的非常的简单，或者是非常的简短，再或者在很多不同的网络平台都使用相同的简单的密码。这样就很容易让一些不法分子钻了空子，然后盗取用户的登录信息，从而造成网络用户的账户财产被盗取。另外，还有一些用户很容易被一些不正规的网站链接所吸引，这些网站往往要求用户必须输入其个人信息，还有一些手机验证码的信息，而这些信息正是不法分子盗取用户信息和财产所需要的一些信息，最终导致网络用户造成巨大的损失[4]。

三、网络安全防攻击的办法分析

（一）网络病毒入侵的防治

随着科技的发展日新月异，网络病毒的防治越来越重要。现在如果仅仅只是采用简单的方法来对网络病毒入侵进行防治，已经远远不能够满足现在网络用户的需求，所以要想彻底的阻止网络病毒的入侵必须使用与自身计算机网络系统相匹配的全方位杀毒软件。但是现在市场上并没有哪种杀毒软件是无所不能的，因此，当网络用户遇到网络系统自带的杀毒软件无法消除病毒时，用户也可以到某些网站上去下载一些防治病毒的杀毒软件。但是最重要的一点是，网络用户尽管安装了这些杀毒软件，但是还必须保证每周或者每两周对该杀毒软件进行一次更新，因为这些网络病毒是有时效性的，只有经常更新这些杀毒软件，才能最有效地防治网络病毒的入侵[5]。另外我们还需要每周或者每半个月对我们的电脑硬盘进行一次全方位的杀毒和扫描，这样可以有利于网络用户发现隐藏在我们的网络系统中的病毒。最后，当网络用户的计算机网络不小心受到了网络病毒入侵时，应该马上把计算机网络中现有的杀毒软件升级到最新的版本，然后对整个网络电脑的硬盘进行全方位的扫描，这样的目的主要是可以清除所有可以查杀的网络病毒。

（二）建立有效的防火墙技术

网络最可靠、最基本以及最有效的网络安全措施之一就是建立有效的防火墙技术。近年来，随着科技的不断发展以及新兴网络的不断兴起，防火墙技术越来越成为计算机网络安全的一项重大的防护措施，也是保障网络用户安全的一项重要的屏障。有效的防火墙技术主要是通过计算机网络的软硬件相结合，然后在用户电脑的外部网络和内部网络之间构建起一个对用户网络系统的保护膜。用户在计算机网络上所有发送和接收的信息，都要通过这样的一层保护膜进行连接。只有经过此检查批准之后才会授权，授权允许之后才能成功地发送或者接收。但是，值得重视的一点是，这种防火墙技术并没有对某些合理合法的数据包中存在的病毒进行阻断和识别，从而达到阻止病毒进入用户的电脑网络的目的。

（三）规避“网络钓鱼”邮件

众所周知，“网络钓鱼”是以其他知名机构或者是某些知名银行的名义来发送一些欺骗性的垃圾邮件，目的是引导网络用户给出例如手机验证码等等的一些个人隐私信息。黑客主要是利用这些电子邮件以及一些伪造的网络网站来进行一系列的诈骗活动，某些不清楚网络平台规范的一些用户，往往会在这些平台上泄露自己的私人身份证号和银行卡保密信息，从而造成自身财产的巨大损失。通常情况下，很多黑客经常会把自己伪装成某些零售商、某些知名银行以及某些知名的公司，目的是骗取网络用户的一些私人信息，对于这样的情况，我们的网络用户应该不断的学习网络安全规范，提高网络使用的警惕性[6]。登录某些官方网站的地址时，也要认真核对网站地址、网址，避免错误地输入了网站的网址，

造成自己的财产损失。

（四）定时修复网络系统漏洞

定时修复网络系统的漏洞是网络用户确保计算机网络安全的一项最重要的举措，因为电脑的每一个操作系统，或者说网络用户下载的每一个软件都不可能是没有漏洞或者是没有缺陷的，所以我们必须要定时的修复我们的网络系统，对它们进行网络修复。网络系统漏洞是一项网络用户主动防范网络病毒入侵的一项技术，它可以自动检测计算机网络上存在的漏洞或者说缺陷，让网络用户可以在网络受到攻击之前发现这些漏洞，从而弥补和修复这些漏洞[7]。

（五）避免浏览垃圾网站

避免浏览网垃圾网站主要有以下几个方面内容：第一，避免下载一些网站上来历不明的文件，因为这些文件中很有可能包含某些黑客设置的病毒或者一些携带病毒的代码；第二，在网站上下载软件，一定要选择官方的网址去下载软件，千万不要下载一些来历不明或者携带广告字样的和网站的软件，因为这些不正规的网站所提供的软件，很多都会包含病毒；第三，避免访问一些低级粗俗的网站，因为这些网站中的网页大多包含一些黑客设置的恶意代码，访问这些网站时，病毒会自动通过用户浏览的这些网页把病毒从而附着在用户的电脑网络之中，给用户的造成用户电脑的卡顿、死机，甚至是用户隐私的泄露；第四，使用公共聊天软件时，避免接收陌生文件，因为很多陌生文件中都可能会包含病毒，同时也要避免点击陌生人发来的一些不实的网页链接和网页信息。因为这些网页中大部分都包含一些病毒和代码；第五，最重要的是，避免打开一些来历不明的邮件或者是邮件的附件，因为很多邮件的附件中很有可能包含入侵用户计算机网络的病毒。

四、结语

随着科技和社会的不断发展，计算机网络也在不断的创新和发展，计算机网络的安全也越来越受到企业和网络用户的关注。网络安全是多样的，也是复杂的，而网络安全的发展也已经随着社会的发展，越来越变成了一种专门的防攻击技术服务。因此，我们必须根据不断更新的网络安全问题去及时总结和更新我们的防治网络安全、防攻击的一些方法和技术，这样才能够在不断发展的网络环境中持久地保证网络用户使用互联网的安全。最重要的一点是我们应该了解，在互联网时代，网络安全的防治是并不具备有完全的绝对性的，网络安全只能是一个相对的状态，我们只能够在不断的创新和不断的钻研中继续探索出防治网络安全的办法，同时不断创新网络安全的防治技术，以此来确保互联网网络长期的发展与繁荣。本文主要是阐述了智能化网络安全防攻击的一些现状以及一些相关的概念，最后阐述了应对网络安全攻击的解决办法，这对解决当下网络安全防攻击的一些事件具有一定的借鉴意义。

参考文献：

[1]杨宗跃.智能化网络安全防攻击检测中数据抽取和分析[J].计算机测量与控制，2021，29（5）：174-178.DOI：10.16526/j.cnki.11-4762/tp.2021.05.035.

[2]周云，刘月华.基于深度强化学习的智能网络安全防护研究[J].通信技术，2021，54（11）：2545-2550.DOI：10.3969/j.issn.1002-0802.2021.11.014.

[3]李继芳.县级融媒体中心机房的网络安全防护措施[J].数字通信世界，2021（12）：148-150.DOI：10.3969/J.ISSN.1672-7274.2021.12.053.

[4]张帆.“互联网+”背景下网络安全及防御技术探究[J].数字通信世界，2021（1）：135-136.DOI：10.3969/J.ISSN.1672-7274.2021.01.058.

[5]郑志荣.基于大数据的计算机网络安全防御系统建构[J].电脑编程技巧与维护，2021（4）：159-161.DOI：10.3969/j.issn.1006-4052.2021.04.060.

[6]廖宇翔.人工智能技术在网络安全防御中的应用[J].信息技术与信息化，2021（6）：182-184.DOI：10.3969/j.issn.1672-9528.2021.06.054.

[7]朱雪斌.基于智能计算的计算机网络安全防范措施解析[J].科技创新导报，2021，18（3）：98-100.DOI：10.16660/j.cnki.1674-098X.2010-5640-2160.