窃密攻击检测与溯源技术在网络信息安全中的应用

韩建鹏[1]　李恒云[1]　王顺民[2]
(1.中孚信息股份有限公司 济南 250101;
2.山东国耀量子雷达科技有限公司 济南 250101)

摘　要　文中深入研究了窃密攻击检测与溯源技术在网络信息安全中的应用。首先,通过对窃密攻击行为的细致分析,提出了一种基于行为特征的检测方法,其能快速、准确地识别潜在的窃密威胁。其次,探讨了溯源技术在追踪窃密攻击源头中的作用,通过构建多层次的溯源模型,实现了对攻击者的有效溯源和追踪。在实验验证方面,应用实际攻击样本进行模拟,结果表明该方法在检测和溯源上均有着较好的效果,为网络信息安全领域提供了一种创新的解决方案,有望推动窃密攻击防范技术的进步。

关键词:窃密攻击;检测技术;溯源技术;网络信息安全;行为特征
中图分类号　TN915.08

Application of Stealing Attack Detection and Traceability Technology in Network Information Security

HAN Jianpeng[1], LI Hengyun[1] and WANG Shunmin[2]
(1.Zhongfu Information Inc., Jinan 250101, China;
2.Shandong Guoyao Quantum Lidar Technology Company Co., Ltd., Jinan 250101, China)

Abstract　This paper dives deep into research on the application of exfiltration attack detection and traceability technology in network information security. First, through detailed analysis of exfiltration attack behavior, a detection method based on behavioral features is proposed, which can quickly and accurately identify the threat of stolen secrets. Secondly, the role of traceability technology in tracking the source of exfiltration attacks is discussed, and the implementation of valid traceability and tracing of attackers is achieved by building a multi-level traceability model. In terms of experimental verification, the actual attack samples are used for simulation. The results show that the method has achieved remarkable results in detection and traceability, providing an innovative solution for the network information security domain, and is expected to promote the progress of exfiltration attack prevention technology.

Keywords　Stealing attacks, Detection technology, Traceability technology, Network information security, Behavior characteristics

0　引言

随着互联网技术的快速发展,网络已经成为人们生活中不可或缺的一部分。然而,其也带来了较为严重的网络安全问题,其中窃密攻击作为一种隐蔽且具有破坏性的威胁,对个人隐私、企业机密及国家安全产生了严重的影响。随着信息技术的不断进步,窃密攻击手段也愈发多样化,变得难以防范,这使得传统的安全防范手段逐渐显得力不从心。在人们对网络信息安全愈发重视的背景下,对窃密攻击进行及时、准确的检测变得至关重要。传统的基于签名的检测方法难以应对日益复杂的窃密攻击形式,因而需要使用更为先进和智能的技术手段。同时,一旦窃密行为发生,对攻击源头的溯源追踪成为网络安全领域中的一大难题。有效的溯源技术可以追溯攻击者的身份和动机,为进一步的安全防范提供重要参考。本文旨在深入探讨窃密攻击检测与溯源技术在网络信息安全中的应用,以应对不断演进的网络威胁。通过对窃密攻击行为的详细分析,本文提出了一种基于行为特征的检测方法,以及时发现和防范潜在的威胁。

1　窃密攻击检测技术

1.1　窃密攻击行为分析

窃密攻击行为分析是理解攻击者行为模式的关键。攻击者常常会通过各种隐蔽手段获取目标系统的内部信息,如窃取用户凭证、监控敏感数据的传输等[1]。为更深刻地

作者简介:韩建鹏(1983—),本科,工程师,研究方向为信息安全;李恒云(1984—),本科,工程师,研究方向为信息安全;王顺民(1986—),硕士,工程师,研究方向为电子信息。

理解窃密攻击行为，首先需要深入分析攻击者的潜在目标和常用手段。对攻击行为的研究不仅涉及对网络通信的分析，还需要考虑攻击者可能采用的隐蔽手段，如隐匿通信、侧信道攻击等。

在分析窃密攻击行为的过程中，可采用行为建模的方法，将攻击者的活动建模为一系列离散的事件。这些事件可以包括登录尝试、数据访问请求、异常数据传输等。通过建立行为模型，能有效捕捉攻击者在网络中的痕迹，识别潜在的窃密行为。

1.2 基于行为特征的检测方法

基于行为特征的检测方法可以通过深度挖掘用户和系统的操作行为，来捕捉窃密攻击在网络中的独特痕迹。在行为特征提取阶段，其定义了一系列与窃密攻击相关的特征，如用户登录频率、文件访问模式、数据传输量等。通过监测系统日志和网络流量，系统能实时提取这些特征，形成综合性较强的行为特征向量。随后，采用特征量化的手段，使用统计方法对行为特征进行数学处理，如计算均值、方差等，将原始数据转换为可供模型分析的数值型数据。这一步骤有助于提取出标准化特征，使模型能更好地理解和比较各种行为模式。

在行为特征量化的基础上，本文构建了行为特征分析与模型。采用机器学习算法，如支持向量机（SVM）或决策树，对已知攻击案例和正常行为进行训练。模型通过学习正常和异常行为的模式，建立了窃密攻击的行为模型。该模型不会局限于已知的攻击模式，还能识别新的、未见过的窃密行为，提高了系统的适应性和应对能力。最终，实时监测与报警环节是该方法的关键步骤。系统在运行时通过持续监测行为特征，使用预先训练好的模型进行实时检测。一旦检测到与窃密攻击行为相符的模式，系统会立即触发报警机制，通过邮件、短信等方式通知安全管理员，以便其采取相应的响应措施，如封锁攻击源、强化访问控制等。通过这一基于行为特征的检测方法，系统能在攻击者发起窃密行为的早期阶段进行有效的检测和响应，提高网络信息安全的整体水平。

2 窃密攻击溯源技术

2.1 溯源技术在网络安全中的作用

溯源技术在网络安全中扮演着关键角色，其作用是可以准确定位和快速追踪网络攻击源头。传统的网络安全防御主要依赖于防火墙和入侵检测系统，然而，当网络受到攻击时，了解攻击来源并快速采取应对措施尤为重要。溯源技术通过收集、分析网络流量和系统日志，能追踪攻击者的路径和方法，实现对攻击源头的准确定位。

溯源技术采用了多种手段，如 IP 地址追踪。通过分析网络流量中的 IP 地址信息，可以追溯攻击者的地理位置。IP 地址追踪是溯源技术中的常用手段之一[2]。通过 Traceroute 等工具获取的 IP 地址列表，可以计算出攻击路径的传播时间，如式(1)所示：

$$T=\frac{1}{n-1}\sum_{i=1}^{n-1}(t_{i+1}-t_i) \tag{1}$$

其中，n 为路由节点的数量，t_i 是第 i 个路由节点的响应时间。

还可以利用入侵检测系统的报警信息、流量日志等，通过对攻击行为的分析，识别攻击者的特征，为进一步的攻击溯源提供线索。溯源技术的作用不仅在于追踪攻击者，其还可以收集足够的证据，为后续的法律追诉提供支持。

2.2 构建多层次的溯源模型

构建多层次的溯源模型是保证网络安全的关键，其旨在通过对不同层次信息的综合分析，建立对攻击源头的全面、多维度的理解。这一过程不仅涉及网络层面的追踪，还包括应用层面和主机层面，以形成对攻击行为的全景式认知。

在网络层面的溯源中，为追踪攻击的传播路径，可以通过识别攻击经过的路由节点，建立网络拓扑结构。这一过程依赖于对网络流量、路由器日志等数据的分析。借助追踪路由（Traceroute）等技术，系统能确定攻击的传播路径，通过这种方式，快速定位攻击的传播轨迹，有助于形成整体的攻击图景[3]。

在应用层面的溯源中，应聚焦于分析攻击者与受害者之间的交互过程。监测应用层协议的交互，如 HTTP 请求和数据库查询，有助于识别攻击者的访问行为。通过构建攻击者与目标系统之间的关联模型，能深入理解攻击者与受害者之间的互动，从而更好地把握攻击者的意图和手段。

在主机层面的溯源中，需要深入研究攻击者在受害主机上的活动，包括对主机日志、系统调用等的细致分析，同时深入研究攻击者在主机上植入的恶意代码。构建主机层面的溯源模型，有助于追踪攻击者在主机上的行为轨迹，提供详实的信息支持，为进一步的溯源提供关键的线索。

通过整合这 3 个层次的溯源信息，本文建立了较为全面的攻击溯源模型。该模型不仅涵盖了攻击的传播路径，还深入挖掘了攻击者与受害者之间的互动和攻击者在主机上的活动。这样的全方位分析有助于形成对攻击源头的全景理解，为网络安全人员提供准确的信息支持，提高其对网络攻击的应对能力。

2.3 有效溯源和追踪攻击者

在实现有效溯源和追踪攻击者的过程中，需要整合多个层次的溯源信息，形成全面的攻击路径。这涉及溯源信息的关联和分析，可以通过关联规则挖掘、机器学习等技术实现。具体而言，通过关联分析网络层、应用层和主机层的溯源信息，可以还原攻击者的整体行为轨迹。借助网络流量分析技术，如深度包检测（DPI）等，可以对攻击流量进行更为细致的解析，进一步揭示攻击者的行为特征。

在多层次的溯源模型中，通常使用 Apriori 算法来挖掘

关联规则。其基本思想是挖掘出频繁项集，从而找到多个层次间的关联规则。关联规则的支持度(Support)和置信度(Confidence)的计算公式如式(2)、式(3)所示：

$$Support(X)=\frac{X}{T} \tag{2}$$

$$Confidence(X\Rightarrow Y)=\frac{Support(X\bigcup Y)}{Support(X)} \tag{3}$$

其中，X 和 Y 分别表示关联规则中的两个项集。

具体而言，设攻击者行为的多个方面为项集，通过Apriori算法可以找到这些项集之间的关联规则，从而构建出攻击者行为的多层次关联模型[4]。这为追踪攻击者提供了有力的依据，也为网络安全人员提供了更为直观的信息，有助于形成更全面、深刻的对抗策略。

在实际案例中，通过有效的溯源和追踪技术，能更快地定位攻击源头，从而采取及时、有效的应对措施。这不仅有助于提高网络信息安全的整体水平，也为网络安全领域的进一步研究和创新提供了新的思路和方法。

3 实验验证与结果

3.1 实验设计

实验目的是评估基于行为特征的窃密攻击检测方法和多层次溯源模型的性能。本文建立了一个包含正常访问行为和模拟窃密攻击行为的实验环境。窃密攻击类型包括SQL注入攻击、DDos攻击以及文件注入攻击。实验设计覆盖了这些攻击类型，并分别考虑了攻击的强度和持续时间。

3.2 模拟攻击样本的使用

在实验中，使用了具体、常见的模拟攻击样本。

(1)SQL注入攻击。通过向输入字段注入SQL代码，模拟攻击者试图访问、修改或删除数据库中的敏感信息的行为。

(2)DDoS攻击。通过模拟大量请求，使其超过系统处理能力，评估系统对拒绝服务攻击的检测和应对能力。

(3)文件注入攻击。攻击者试图将恶意文件注入系统，通过对文件访问模式的异常检测来识别此类攻击。

3.3 检测和溯源效果的验证

收集实验数据并用表格形式展示检测和溯源的效果，如表1所列。

表1 实验数据

实验编号	攻击类型	攻击强度	检测准确率/%	溯源成功率/%
1	SQL注入攻击	中	94	88
2	DDoS攻击	高	91	86
3	文件注入攻击	低	97	91

实验数据表明，基于行为特征的检测方法在各种攻击场景下均表现出较高的检测准确率。多层次的溯源模型成功追踪了攻击者的行为路径。值得注意的是，在高强度攻击场景下，该检测方法仍保持了较高的准确性，而溯源模型的成功率也达到了可接受的水平。这表明本文所提方法在实际应用中具有较强的鲁棒性和有效性，为网络信息安全提供了有力支持。

4 结语

基于行为特征的窃密攻击检测方法及多层次的溯源模型在网络信息安全领域展现了较大的潜力。实验证明，在多种攻击场景下，该方法表现出较高的准确性，可成功识别并应对SQL注入攻击、DDoS攻击等多种攻击类型。同时，多层次的溯源模型在对攻击行为的追踪中取得了令人满意的结果，成功还原了攻击者的路径和行为轨迹。这不仅为用户提供了有力的防御手段，也为未来的安全研究和技术创新提供了新的方向。总体而言，该方法不仅在实验室环境中展现了较强的可行性，在面对实际网络威胁时也具备实用性，为构建更为健壮的网络安全防线和提升信息安全水平提供了切实可行的方案。

参考文献

[1] 冯德尹，吴明念.可信计算技术在网络信息安全中的应用与研究[J].电脑知识与技术，2021，17(13)：53-54.

[2] 闫军.数据加密技术在计算机网络信息安全中的应用研究[J].信息记录材料，2023，24(9)：152-154.

[3] 蔡志珍.数据加密技术在计算机网络信息安全中的应用研究[J].信息记录材料，2021，22(11)：109-110.

[4] 孙慧青.数据加密技术在计算机网络信息安全中的应用研究[J].电脑知识与技术，2020，16(32)：61-62.