 DOI: https://doi.org/10.26549/bdai.v5i1.15963

Machine-learning Based Hospital Network Ransomware Research on Attack Recognition and Defense Strategy

Le Ren

The Fourth People's Hospital of Zigong, Sichuan Province, Zigong, Sichuan, 643000, China

Abstract

With the increasingly severe threat of ransomware attacks, exploring effective defense strategies has become an urgent need. This study focuses on the use of machine learning technology to improve the identification and defense ability of ransomware attacks in hospital networks, analyzes the characteristics of ransomware attacks and their impact on hospital operations, and discusses the application principles and potential advantages of machine learning in network security. This paper also explores the design principles and implementation considerations of machine learning-based network security strategies, aiming to provide theoretical and strategic guidance for hospital network security. Through this study, it is expected to provide a new perspective for the field of hospital network security, and contribute to the defense of network threats and the protection of patient information security.

Keywords

hospital network security; ransomware attack; machine learning; network defense strategy; data protection

基于机器学习的医院网络勒索软件攻击识别与防御策略研究

任乐

四川省自贡市第四人民医院，中国·四川 自贡 643000

摘　要

随着医院网络安全面临日益严峻的勒索软件攻击威胁，探索有效的防御策略成为迫切需求。本研究聚焦于利用机器学习技术提升医院网络对勒索软件攻击的识别和防御能力，分析了勒索软件攻击的特征和对医院运营的影响，讨论了机器学习在网络安全中的应用原理及其潜在优势。论文还探讨了基于机器学习的网络安全策略的设计原则和实施考虑，旨在为医院网络安全提供理论和策略上的指导。通过此研究，期望为医院网络安全领域提供新的视角，为防御网络威胁、保护患者信息安全贡献力量。

关键词

医院网络安全；勒索软件攻击；机器学习；网络防御策略；数据保护

1 引言

随着时间推移，数据安全的重要性日益凸显。为确保数据的安全，中华人民共和国于 2021 年 6 月 10 日正式颁布了《数据安全法》，该法旨在加强对个人数据和敏感信息的保护，规范数据的处理和使用，以维护国家和个人的信息安全。在医疗行业日益走向数字化的今天，医院网络安全显得尤为重要 [1]。医院作为存储大量敏感个人和医疗信息的关键机构，其网络安全直接关系到患者信息的保护和医疗服务的连续性。随着技术的发展，医院网络面临着越来越多的新型威胁，其中勒索软件攻击的频发尤为引人关注。这类攻击不仅威胁到数据的安全和隐私，还可能导致医疗服务的中断，给患者的健康带来严重风险。

以诺顿医疗系统 2023 年遭受的勒索软件攻击为例，攻击者窃取了数百万患者和员工的个人信息，给医院的运营和声誉造成了严重损害。这一事件凸显了现有网络安全措施在应对复杂网络攻击面前的不足，揭示了医院网络安全体系亟须强化的现实。鉴于此，本研究旨在探讨利用机器学习技术提升医院网络对勒索软件攻击的识别和防御能力。机器学习的引入，为传统网络安全带来了新的可能性，特别是在攻击模式识别和预防策略制定方面 [2]。本研究将从勒索软件攻击的特征出发，探讨如何通过机器学习技术有效识别潜在的安全威胁，并设计相应的防御策略，以弥补现有研究的空白，为医院网络安全提供新的视角和解决方案。

2 医院网络安全现状

医院作为存储大量敏感医疗和个人信息的关键机构，其网络系统的安全性对维护患者隐私和医院运营的稳定至关重要。医院系统通常包括 his、lis、pacs 等数据处理系

【作者简介】任乐（1987–），男，中国四川自贡人，本科，工程师，从事信息管理、AI与人工智能研究。

统，这些系统的安全和稳定运行是医院提供连续医疗服务的基础。

勒索软件攻击是当前医院网络面临的主要安全威胁之一 [3]。这类攻击通常导致敏感数据被加密并要求赎金以恢复数据访问，严重时可导致医院运营中断和患者治疗受阻。以 2023 年诺顿医疗系统遭受的勒索软件攻击为例，该事件中攻击者访问并可能窃取了约 250 万患者和员工的个人与健康信息，造成了重大的信息泄露和运营中断。尽管医院已采取多项安全措施如防火墙和入侵检测系统，但这些传统安全机制往往难以应对日益复杂的网络威胁。因此，深入了解当前医院网络安全现状，并探索新的防御方法，对于保护医院免受网络攻击至关重要。这不仅关系到医院数据的安全，还直接影响医疗服务的质量和患者的安全。

3 勒索软件攻击的特征、手段以及对医院的影响

勒索软件攻击方式，在医院网络安全领域中的显著增加，反映出其独特的攻击特性。这些攻击通常采用高级加密技术（如对称或非对称加密）来加密医院的关键数据文件，并要求支付赎金以解锁，直接威胁到医疗数据的可用性和机密性。攻击者在匿名性的保护下进行操作，通常使用加密货币进行赎金交易，以避免追踪 [4]。此外，某些勒索软件能够自我复制并迅速在网络中传播，增加了清除和控制的难度。攻击者有时会在网络中潜伏一段时间，收集信息并寻找最佳攻击时机。

这些攻击手段，主要包括但不限于以下几种：

钓鱼邮件：攻击者发送带有恶意附件或链接的电子邮件，诱使员工点击，从而植入勒索软件。利用系统漏洞：通过利用医院网络系统中已知的安全漏洞进行入侵。社会工程学技巧：利用员工的安全意识不足，通过虚假通信或诱导手段获取网络访问权限。远程桌面协议攻击：通过利用远程桌面协议的弱点，直接进入医院的内部网络。外部设备接入：如通过移动便携设备接入医院网络系统计算机，以该计算机为源头发起攻击。

医院遭受勒索软件攻击的后果是深远且多方面的。数据访问受阻，会导致医疗机构瘫痪，影响患者治疗。从经济角度来看，巨额赎金会给医疗机构带来巨大的财务压力。医院的声誉受损，这可能会导致患者信任度下降，从而对医院运营产生长期影响。在法律责任方面，患者数据泄露可能会使医院面临法律诉讼和罚款。

4 基于机器学习的攻击识别策略

传统的基于规则的防御系统已经不足以应对这些复杂且多变的威胁。在这种背景下，机器学习技术以其强大的数据处理能力和模式识别能力，可以为医院网络安全提供新的防御手段。

首先，预处理数据和提取特征是构建有效的机器学习模型的关键步骤。这有助于通过收集历史数据，来识别可用于区分攻击的显著特征。这些特征的选择直接影响模型的性能和准确性。此外，选择模型并对其进行训练，对于准确识别攻击至关重要。方法包括决策树、深度学习网络以及其他机器学习算法，这些算法根据特定要求和数据属性有自己的优势 [5]。在此过程中，使用包含已知攻击案例和正常操作数据集，标记历史数据集来训练模型，使其能够区分正常活动和异常行为，从而准确识别勒索软件攻击。

虽然机器学习模型的实施能够为医院带来一定的好处，也面临着一系列挑战。这个模型要求持续学习以便应对不断变化的网络威胁，这就需要定期更新和调整。相对于传统规则的安全系统，机器学习模型在识别精度和响应速度上有很大潜力。这些模型可以快速适应新的攻击方式，从而增强医院网络防御安全性。这也对模型实时性和误报率提出了更高的要求。

5 防御策略的设计与实施

在基于机器学习的攻击识别模型为医院网络安全提供了新的可能性后，接下来的重点是设计和实施有效的防御策略。这些策略应当不仅能够利用机器学习模型的预测能力，还应综合考虑医院网络的特点和实际需求。

5.1 防御策略的设计原则

为确保医疗机构网络的全面安全，防御策略需要覆盖物理层到应用层的各个方面 [6]。在物理层面，应包括设备的安全存放和防盗措施；在网络层面，应涵盖防火墙配置、入侵检测系统的部署；包括但不限于端对端的数据加密和安全的数据存储。考虑到医院日益增长移动设备和远程访问，这些方面的安全措施也不容忽视。网络环境和攻击手段的不断演变，要求防御策略具备高度的适应性和灵活性。医院应定期审查和更新其安全政策，确保能够对抗最新的威胁。这包括更新防病毒软件的签名库、调整入侵检测系统的规则以及及时修补已知的安全漏洞。

在设计防御策略时，应考虑到其对医院日常运营的潜在影响。策略应旨在最大限度地减少对医疗服务的干扰。例如，在执行系统更新或维护时，应选择医院的低峰时段，以最小化对患者护理的影响。另外，用户是医院网络安全的第一道防线。因此，需要定期对医院员工进行网络安全培训，提高工作人员对潜在网络威胁的意识。这些培训应包括：如何识别钓鱼邮件、安全地使用社交媒体以及如何处理敏感数据等内容。

5.2 实施的步骤

医院需要将机器学习模型与现有网络安全系统相集成。选择合适的网络特性机器学习模型。例如基于行为分析的模型，用于识别异常网络活动或未知的攻击手段。将这些模型与防火墙和入侵检测系统等安全基础设施相结合，以确保它们可以有效地协同工作以提高防御效率。

防御策略的有效性，在很大程度上取决于其在特定环境中的配置和调优。这需要医院的 IT 团队根据网络的具体特点和医院的业务需求，细致地调整策略参数。例如，针对不同类型的网络流量进行差异化处理，确保关键医疗设备的网络通信不受干扰，同时阻断或限制可疑流量。

在将防御策略投入实际运营之前，进行模拟测试至关重要。这包括模拟各种网络攻击场景，评估防御策略的有效性以及策略对医院日常运营的可能影响。通过这种方式，可以在不影响实际运营的情况下，发现和修正潜在的问题。安全防御是一个持续的过程，即使在实施防御策略之后，也需要定期监控其性能，并根据新出现的威胁进行必要的调整和更新。这包括对新的漏洞和攻击方法保持警觉，定期更新安全协议和软件以及对整个网络进行定期的安全审计。

5.3 实施防御策略面临的挑战

在医院网络中实施先进的机器学习模型和其他安全措施，往往涉及众多技术的集成，这可能带来复杂性和兼容性问题。为有效应对这一挑战，医院可以建立专门的项目管理团队，负责协调各种技术的集成工作。此外，与经验丰富的供应商合作，利用他们的专业知识和经验，可以有效减少集成过程中的问题。

由于网络安全的威胁不断变化，防御策略需要不断更新以应对新挑战。因此，医院需要建立一个快速响应机制，以便及时了解新威胁，并迅速更新其防御策略。这些快速响应机制可以包括订阅安全情报服务、参加行业安全论坛以及建立内部安全研究团队。

6 评估与分析

在实施基于机器学习的防御策略后，评估和分析其效果对于确保医院网络安全至关重要。此过程涉及对策略的有效性、效率以及在真实环境中的应用性进行全面评估。

6.1 策略效果的评估

评估机器学习模型在识别勒索软件攻击方面的准确性，同时关注误报率的水平，因为过高的误报率可能导致不必要的干扰和资源浪费。分析系统在检测到攻击时的响应时间，这对于及时阻止或减轻攻击造成的损害至关重要。考虑网络环境和攻击手段的演变，评估模型的适应性和灵活性，确保其能够有效应对新出现的威胁。

6.2 分析与调整

通过收集和分析实施防御策略后的相关数据，包括攻击尝试、拦截情况和系统反应等，以获得关于策略效果的深入洞察。根据评估结果对模型和策略进行必要的调整和优化，以提高其总体效能和效率。分析特定的攻击案例，特别是那些成功被识别或遗漏的案例，从中学习并改进防御策略。

6.3 持续监测与改进

医院需要建立定期评估机制，以调控防御策略的效果，应对新的威胁与挑战。将来自医院管理层、IT 团队和其他利益相关者数据反馈收集起来，加以分析。确保目前的防御策略符合医院的整体安全需求。需要考虑到如今的技术手段和网络环境都在不断变化，研究的方向需随时调整，例如采用更先进的机器学习算法或更全面的数据分析技术。

7 结论与展望

本研究探讨了利用机器学习技术提高医院网络对勒索软件攻击的识别和防御能力。通过分析勒索软件攻击的特征、手段以及对医院的影响，论文阐明了医院网络面临的安全威胁，突出了机器学习在提高攻击识别准确性和响应速度方面的潜力。在设计防御策略时，本研究考虑了医院网络的特点，强调了全面性、适应性以及对医院运营影响最小化的重要性。同时，通过对策略实施后的评估和分析，论文提出了对技术和策略进行持续监测和改进的必要性。

随着医院网络环境的不断演变和技术的发展，未来的研究应继续关注机器学习技术在医院网络安全领域的应用。特别是在数据驱动的攻击预测、实时威胁响应和自适应防御策略方面，机器学习提供了巨大的潜力。未来的研究还应考虑集成更先进的机器学习算法，例如深度学习和强化学习，以进一步提高医院网络安全系统的智能化水平和效能。考虑到医院网络安全的复杂性和持续变化的网络威胁，跨学科的合作将变得越来越重要。这包括计算机科学、网络安全、医疗信息学和临床实践等领域的专家之间的合作，以确保提出的解决方案既技术上先进又符合医疗行业的实际需求。

因此，本研究为医院网络安全提供了新的视角和策略，旨在通过利用机器学习技术，为医院网络安全领域带来有效改进。未来的研究将继续探索这一领域的新方法，以更好地保护医院免受日益复杂的网络威胁。

参考文献

[1] 周润.信息化背景下医院网络安全管理措施研究[J].科技资讯,2020,18(18):26-27.

[2] 齐欢庆.大数据在医院网络安全防御中的应用与研究[J].网络安全技术与应用,2022(6):118-120.

[3] 高涌皓.探讨针对勒索病毒的医院安全防护体系设计[J].电子元器件与信息技术,2022,6(11):196-200.

[4] 孙倩倩.数字加密货币洗钱犯罪法律规制研究[D].南昌:江西财经大学,2021.

[5] 陆庭辉,饶茜霖,薛质.针对隐匿高危勒索病毒攻击的检测[J].通信技术,2022,55(11):1492-1498.

[6] 王涛,万笛.医院信息系统防御勒索病毒的策略与实践[J].中国数字医学,2022,17(8):106-109.