

# 僵尸网络检测与防御策略研究

蒋枘言

(南开大学 网络空间安全学院, 天津 300350)

**摘要** 本文探讨了僵尸网络在数字化时代对全球网络安全构成的严重威胁，强调了研究僵尸网络对于提升网络安全防护能力、促进技术发展和产业进步、构建国家网络安全体系及增强网络威慑力的重要性。文章综述了当前国内外在僵尸网络检测技术和防御策略方面的研究进展，包括人工智能、机器学习、深度学习等先进技术的应用，以及技术、管理和法律层面的综合防御措施。同时，通过具体案例分析了僵尸网络攻击的广泛性和严重性。最后，文章展望了未来僵尸网络的发展趋势，并提出了深化技术研究、构建综合防御体系、推动标准化建设和加强用户教育等应对策略。

**关键词** 僵尸网络；网络安全；检测技术；防御策略；人工智能；机器学习

## Research on Botnet Detection and Defense Strategies

Ruiyan Jiang

(College of Cyber Science, Nankai University, Tianjin 300350)

**Abstract** This article discusses the serious threat posed by botnets to global cybersecurity in the digital era, and emphasises the importance of research on botnets for enhancing cybersecurity protection capabilities, promoting technological development and industrial progress, building a national cybersecurity system, and strengthening cyber deterrence. The article overviews the current research progress in botnet detection technology and defence strategies at home and abroad, including the application of advanced technologies such as artificial intelligence, machine learning, deep learning, and comprehensive defence measures at the technical, managerial and legal levels. Meanwhile, the widespread and seriousness of botnet attacks are analysed through specific cases. Finally, the article looks forward to the future development trend of botnets and proposes coping strategies such as deepening technical research, building a comprehensive defence system, promoting standardisation and strengthening user education.

**Key words** Botnets; cyber security; detection techniques; defence strategies; artificial intelligence; machine learning

## 1 研究僵尸网络的背景

在数字化时代，互联网已成为现代社会的基础设施，支撑着经济、文化、政治和日常生活的各个方面。然而，随着网络技术的普及和应用，网络安全问题也日益凸显，尤其是僵尸网络(Botnet)的出现和演变，对全球网络安全构成了严重威胁。僵尸网络是由大量被恶意软件感染的计算机组成的网

络，这些计算机在不知情的情况下被远程控制，用于执行各种网络攻击，如分布式拒绝服务攻击(DDoS)、数据泄露、垃圾邮件传播等。由于其隐蔽性、自动化和大规模性，僵尸网络已成为网络犯罪分子的首选工具，给个人用户、企业乃至国家安全带来了前所未有的挑战。

## 2 研究僵尸网络的意义

研究僵尸网络对于网络安全领域至关重要，它不仅涉及到提升网络防御技术，还包括了对网络攻击行为的深入理解和预防。随着数字技术与传统行业的融合，安全科技成为护航数字中国持续发展的重要引擎。僵尸网络的研究有助于我们更好地理解网络攻击的模式和手段，从而开发出更先进的安全产品和解决方案，提高安全产品供给质量，缩小与国际先进水平的差距。此外，僵尸网络的研究还促进了安全产业的发展，预计到 2028 年，我国数字安全产业规模有望突破万亿元，增速位列全球第一，这表明安全科技的市场需求巨大，技术创新和研发能力的提升对于整个产业的发展至关重要。

在国家层面，僵尸网络的研究有助于构建和完善国家安全综合防御体系，强化国家关键信息基础设施的安全防护能力。同时，随着新一代信息技术的快速演进，僵尸网络的研究也推动了网络安全防护思路的变革，如零信任架构的提出和应用，它通过构建基于身份角色的逻辑边界，实现网络架构的新变革。这种变革对于适应新型业务场景的安全需求，提升未知威胁的防御能力具有重要意义。

此外，僵尸网络的研究还与网络威慑力的构建息息相关。在网络空间中，威慑力的构建需要让潜在的攻击者知道动手后将面临严重的后果。通过研究僵尸网络，我们可以更好地理解网络攻击的心理和行为模式，从而更有效地构建网络威慑力，保护国家网络安全，保障国家在网络空间和物理空间的核心利益。

综上所述，僵尸网络的研究不仅对提升网络安全防护能力、促进技术发展和产业进步具有重要意义，还对构建国家网络安全体系、增强网络威慑力以及推动电子化、信息化的健康发展起到了关键作用。

## 3 当前国内外的研究进展

### 2.1 僵尸网络的检测技术

当前僵尸网络检测技术的发展主要集中在以下几个方面：

**人工智能技术的应用：**近年来，人工智能(AI)技术的进步极大地推动了僵尸网络检测技术的发展。特别是，生成对抗网络(GANs)被用于网络流

量中的异常检测，通过结合主成分分析(PCA)进行特征选择和降维，然后利用GANs学习正常网络流量的底层分布并生成合成样本进行异常检测。这种方法通过结合特征选择和生成建模的优势，有效地识别异常活动与正常网络行为。

**机器学习在网络异常检测中的作用：**机器学习(ML)技术在提高数字基础设施安全性方面发挥着重要作用，特别是在网络异常检测和安全防御方面。研究评估了包括深度学习(DL)、集成方法以及监督学习和无监督学习在内的关键ML技术在识别异常和降低风险方面的有效性。ML技术通过实时监控和适应性反应，强调了ML系统在综合安全框架中的集成。

**深度学习在网络入侵检测系统中的应用：**深度学习技术在网络入侵检测系统(NIDS)中显示出了其识别复杂和动态风险的能力。特别是，循环神经网络(RNNs)和长短期记忆(LSTM)网络因其在网络流量中的时间依赖性而在该领域得到了广泛的应用。

**结合网络和主机流量特征的检测系统：**通过结合网络和主机流量特征，可以显著提高NIDS的流量处理能力。研究强调了特征选择技术在提高入侵检测能力方面的重要性，并为物联网(IoT)应用创建了新的统计流量特征，以进一步改善网络流量安全。

**大型预测模型在入侵检测中的应用：**BERT系列和GPT系列等大型预测模型利用变换器和注意力机制的力量，在理解和处理序列数据方面展现出了显著的能力。这些模型在网络安全领域，特别是在入侵检测技术中，显示出了巨大的潜力。

**面向IoT环境的特定技术：**最新的研究强调了物联网(IoT)特定技术的需求，并开发了详细的系统入侵检测和预防方法，特别是在IoT环境中。

综上所述，当前僵尸网络检测技术正朝着集成更先进的AI和ML技术、深度学习、以及针对特定环境(如IoT)的定制化解决方案方向发展。这些技术的发展不仅提高了检测的准确性和效率，还增强了系统的适应性和鲁棒性，以应对不断演变的网络安全威胁。

### 2.2 僵尸网络的防御策略

#### 2.2.1 技术层面的防御策略

**安装和更新安全软件：**安装并定期更新杀毒软件、防火墙和反间谍软件，这些软件可以及时发现和清除病毒、木马等恶意软件，阻止恶意流量进入

计算机, 防止计算机被感染和控制。

**及时升级系统和应用程序:** 系统和应用程序的漏洞是黑客攻击的入口之一。因此, 应及时升级系统和应用程序, 修补这些漏洞, 提高系统的安全性。

**使用智能 IP 过滤:** 通过智能的预过滤来防止僵尸网络产生的恶意通信到达防火墙。企业可以设置一个专门的网关来持续监视和主动过滤被僵尸网络控制的 IP 地址。当网关收到这些已知的恶意地址的通信时, 会自动高速过滤掉这些地址, 使其无法达到企业网络。

**配置防火墙:** 防火墙可以过滤网络流量, 阻止恶意流量进入计算机。应配置适当的防火墙保护, 限制或消除不必要的广泛访问权限, 有助于阻止僵尸网络在网络中传播。

**数据过滤:** 可以应用出口内容过滤工具, 强制组织的网络流量通过过滤器, 以防止信息流出组织网络。数据丢失预防 (DLP) 解决方案还可用于监视未经授权的访问和破坏, 防止它们泄漏信息。

**使用负载均衡策略:** 基于真实网络测试的负载均衡策略通过分散通信量, 有助于平衡通信的高峰和低谷, 对于减轻 DDoS 攻击企图的影响是一个重要方法。

## 2.2.2 管理层面的防御策略

**禁用不必要的服务:** 管理员应该仅启用必要的服务, 关闭不需要的服务, 以减少系统的漏洞和攻击面。

**强化密码安全:** 使用强密码, 包括字母、数字和特殊字符的组合。定期更改密码, 避免在多个账户间使用相同的密码。

**提高用户安全意识:** 教育用户警惕垃圾邮件、不点击可疑链接、从安全来源下载软件等。用户是防御僵尸网络的第一道防线, 提高用户的安全意识至关重要。

**定期备份重要数据:** 将备份文件存储在离线或安全的地方。在遭受僵尸网络攻击时, 能够迅速恢复系统, 减少损失。

**持续监控网络:** 密切监控网络, 掌握网络连接用户在组织内的操作活动。当僵尸网络或其他恶意软件入侵开始时, 更深入地监测网络交互行为, 可以更快速地检测到异常活动。

**制定应急预案:** 应急预案应包括流程、责任分工、人员培训、备份等内容。在发生 DDoS 攻击或其他网络安全事件时, 及时启动应急预案, 采取相应的措施。

## 2.2.3 法律与合作层面的防御策略

**加强国际合作:** 僵尸网络往往跨越国界, 因此加强国际合作是打击僵尸网络的重要手段。各国可以共享情报、协调行动, 共同应对僵尸网络的威胁。

**依法打击:** 对于发现的僵尸网络攻击行为, 应依法进行打击。通过法律手段追究攻击者的责任, 维护网络空间的安全和秩序。

## 2.3 僵尸网络的攻击案例研究

**Mirai 僵尸网络攻击:** 2016 年 9 月, Mirai 僵尸网络以 620Gbps 的速度攻击了安全记者 Brian Krebs 的网站。2016 年 9 月, Mirai 僵尸网络攻击法国 Web 主机 OVH, 攻击流量达到约 1Tbps。2016 年 10 月, Mirai 对 DNS 提供商 Dyn 发起大规模 DDoS 攻击, 导致欧洲和美国的互联网服务中断, 影响了 Reddit、Twitter 和 Netflix 等主要网站。2016 年 11 月, Mirai 攻击利比里亚的 ISP 和移动服务提供商, 导致该国大部分通信渠道中断。

**BadBox 安卓僵尸网络:** 2023 年, BadBox 僵尸网络感染超过 19.2 万台设备, 包括 Yandex 4K QLED 智能电视和海信智能手机, 被用于广告欺诈活动, 甚至被出租给网络犯罪分子作为发动网络攻击的工具。

**911 S5 僵尸网络:** 由 Wang 运营的 911 S5 僵尸网络渗透到全球近 200 个国家的计算机系统中, 掌控了超过 1900 万个唯一 IP 地址, 其中在美国就有超过 61 万个。

**Reaper (ToTroop) 僵尸网络:** 2017 年发现的 Reaper 僵尸网络比 Mirai 更先进, 因为它利用了物联网设备中已知的漏洞, 而不仅仅是依赖默认凭据, 能够控制数百万台物联网设备。

**Pink 僵尸网络:** 2019 年 12 月, CNCERT 披露了一个超大规模的物联网僵尸网络 Pink, 被黑客入侵并控制的设备数量超过百万, 其中 96%以上的受害者分布在中国境内。

这些案例展示了僵尸网络攻击的广泛性和严重性, 它们不仅能够造成大规模的网络中断, 还可能被用于各种网络犯罪活动, 如 DDoS 攻击、垃圾邮件发送、个人信息泄露和资源滥用等。

## 4 总结与未来发展趋势

僵尸网络作为网络安全领域的重大威胁, 已经引起了广泛的研究兴趣。僵尸网络是指一组被黑客控制的网络设备, 这些设备在黑客的指挥下协同行

动, 进行各种恶意行为, 如数据窃取、网络攻击、广告推广等。僵尸网络的形成和存在与网络设备的漏洞利用、社交工程的攻击以及用户的不良上网习惯等因素有关。

僵尸网络具有规模庞大、难以发现、难以清除和危害严重等特点。黑客可以通过传播恶意代码、利用漏洞等方式快速控制大量网络设备, 形成庞大的僵尸网络。被控制的网络设备通常不会出现明显异常, 使得僵尸网络难以被普通用户察觉。同时, 黑客可以通过远程控制对僵尸网络进行操作, 而清除僵尸网络需要找到并解救被控制的设备, 难度较大。僵尸网络可以造成各种严重的网络安全问题, 如数据泄露、网站被攻击、服务瘫痪等。

针对僵尸网络的防御对策可以从技术、管理、法律等多个方面展开。技术上, 可以通过升级软件和打补丁的方式及时修复漏洞, 提高设备的安全性; 管理上, 加强网络访问控制和安全审计, 定期对网络安全进行评估和演练; 法律上, 完善相关法律法规, 加大对僵尸网络犯罪的打击力度。在实践方面, 很多企业和组织已经采取了各种措施来防范和清除僵尸网络, 如通过安全扫描和入侵检测系统 (IDS) 来监测和控制网络流量, 及时发现并阻止僵尸网络的恶意行为; 加强网络安全教育和培训, 提高用户的安全意识和技能。

随着互联网的不断发展, 僵尸网络威胁将持续存在并可能进一步加剧。未来僵尸网络的发展将呈现以下趋势: (1)技术对抗性增强: 黑客将不断研发新的攻击手段和技术, 以提高僵尸网络的隐蔽性和对抗性。例如, 利用加密技术、P2P 网络等技术手段来增强僵尸网络的抗检测能力。(2)与其他高级威胁结合: 僵尸网络将与其他高级威胁攻击如 APT (高级持续性威胁)、勒索软件等相互配合, 形成复杂的攻击链。这种结合将使得攻击更加难以防范和应对。(3)物联网设备的加入: 随着物联网设备的普及, 僵尸网络将可能利用物联网设备的漏洞进行攻击。物联网设备的多样性和复杂性将给僵尸网络的防御带来更大的挑战。(4)僵尸网络团伙活动: 新兴僵尸网络团伙将通过网络犯罪活动来获取经济利益或政治目的。这些团伙将可能通过社交媒体宣传、黑客论坛等方式扩大影响力, 并展现出不同的发展轨迹和攻击策略。

为了应对未来僵尸网络的威胁, 需要持续研究和创新防御技术和管理方法。以下是一些建议: (1)深化技术研究: 需要进一步深入研究和探索更加高

效、准确的僵尸网络检测和防御技术, 提高整体安全性。例如, 利用人工智能、机器学习等技术手段来提高检测和防御的自动化程度和准确率。(2)构建综合防御体系: 需要研究各种技术的协同防御策略, 构建综合的防御体系, 提高整体防御效果。例如, 结合入侵检测、防火墙、安全审计等技术手段来形成多层次的防御体系。(3)推动标准化建设: 需要推动行业间的合作与交流, 制定统一的标准和规范, 促进技术的协调发展。这将有助于形成更加有效的协同防御机制, 提高整体防御能力。(4)加强用户教育和培训: 用户是防御僵尸网络的第一道防线。需要加强网络安全教育和培训, 提高用户的安全意识和技能。通过普及网络安全知识、提高用户的防范意识来减少僵尸网络的威胁。

综上所述, 僵尸网络作为网络安全领域的重要威胁之一, 需要持续关注和投入。通过深化技术研究、构建综合防御体系、推动标准化建设和加强用户教育和培训等措施来应对未来僵尸网络的威胁, 将有助于提高网络安全的整体防范能力。

**致    谢** 感谢南开大学网络空间安全学院的王志老师开设《信息安全前沿技术》这门课, 请到了各个研究领域的不同老师来给我们作前沿技术的介绍, 让我们开拓了视野, 也让部分同学找到了自己感兴趣的研究方向。

## 参    考    文    献

- [1] 陈飞健. 基于时空残差网络的僵尸网络检测方法[J]. 计算机科学与应用, 2022, 12(4): 1054-1060.
- [2] 蒋鸿玲, 邵秀丽, 李耀芳. 基于MapReduce的僵尸网络在线检测算法[J]. 电子与信息学报, 2013, 35(7): 1732-1738.
- [3] Alieyan, K., Almomani, A., Manasrah, A., and Kadhum, M.M. (2017) A Survey of Botnet Detection Based on DNS. *Neural Computing and Applications*, 28, 1541-1558.
- [4] Oza, A., Ross, K., Low, R.M., and Stamp, M. (2014) HTTP Attack Detection Using N-Gram Analysis. *Computers & Security*, 45, 242-254.
- [5] Nielebock, S., Heumüller, R., Schott, K.M., and Ortmeier, F. (2021) Guided Pattern Mining for API Misuse Detection by Change-Based Code Analysis. *Automated Software Engineering*, 28, Article No. 15.

**Author1**, Ruiyan Jiang. Born in 2005, an undergraduate student in Nankai University.



## Background

Botnets, as a novel form of cyberattack, have posed severe threats to Internet security. By controlling a vast number of infected hosts, botnets achieve various malicious objectives such as information theft, distributed denial-of-service (DDoS) attacks, and spam distribution. As 5G technology, smart homes, and other mobile devices become increasingly prevalent, mobile networks have emerged as the backbone of telecommunications, leading to an escalation of cybersecurity threats.

The significance of researching botnets lies in its crucial role in maintaining network security. Firstly, it enhances the ability to recognize and defend against botnet attack behaviors, thereby mitigating losses incurred by cybercrime. Secondly, in-depth exploration of botnet working principles and propagation mechanisms provides theoretical support for the development of more effective cybersecurity technologies and strategies. This research is indispensable for building robust defenses against evolving cyber threats.

Current research progress on botnets encompasses various aspects. In terms of working principles, botnets typically undergo four stages: infection, connection, control, and snowball replication. Malware exploits system vulnerabilities to infiltrate computers, connects to command and control (C2) servers, awaits instructions for executing tasks, and continuously recruits more computers to expand the botnet.

Detection techniques for botnets are primarily divided into misuse detection and anomaly detection. Misuse detection relies on known signature databases, while anomaly detection is based on characteristic extraction from normal traffic behavior, albeit with a relatively high false positive rate. Recently, machine learning-based dynamic methods, particularly deep learning techniques, have gained widespread adoption due to their high accuracy in extracting spatio-temporal features.

Defense technologies for botnets involve monitoring, working mechanism analysis, signature analysis, detection, and proactive containment. Despite advancements, effectively addressing botnet threats remains a continuous and challenging endeavor due to their evolving nature and complexity.

In summary, botnet research is an interdisciplinary field encompassing network security, artificial intelligence, data mining, and more. Current research focuses on improving detection techniques and innovating defense strategies. The application of deep learning has brought new breakthroughs in botnet detection, yet it also faces challenges in feature extraction and model training. As botnet technology evolves, defense strategies must be continually updated to adapt to new threats. This background introduction sets the stage for further exploration and advancement in botnet research.