论网络空间安全与攻防技术

程占斌
中国电信股份有限公司东莞分公司，广东 东莞 523000
DOI: 10.61369/TACS.2026090001

摘　　要： 网络空间安全正遭遇高级持续性威胁、勒索软件、供应链攻击与零日漏洞等风险，攻击手段不断升级，危害持续扩大。应对威胁可运用入侵防御、态势感知、情报共享、零信任架构及自动化响应等技术。结合典型案例分析，可从完善基础设施、共享威胁情报、推进技术创新、培育专业人才、优化应急机制入手，搭建主动、智能、协同的网络安全防御体系。

关 键 词： 网络空间安全；网络攻防；APT 攻击

On Cyberspace Security and Attack-Defense Technologies

Cheng Zhanbin
Dongguan Branch of China Telecom Corporation Limited, Dongguan, Guangdong 523000

Abstract: Cyberspace security is currently confronted with risks such as advanced persistent threats, ransomware, supply chain attacks, and zero-day vulnerabilities. The attack methods are constantly upgrading, and the harm is continuously expanding. Threats can be addressed by applying technologies such as intrusion prevention, situation awareness, intelligence sharing, zero-trust architecture, and automated response. Based on the analysis of typical cases, a proactive, intelligent and collaborative cybersecurity defense system can be established by starting from improving infrastructure, sharing threat intelligence, promoting technological innovation, cultivating professional talents and optimizing emergency response mechanisms.

Keywords: cyberspace security; network attack and defense; APT attack

引言

数字化发展步伐不断加快，网络安全问题愈发突出。高级持续性威胁、勒索软件等攻击方式持续演变，对各类机构与关键信息基础设施造成极大风险。传统边界防护方式已无法适配当下复杂的网络环境，亟须打造主动、智能、协同的防御体系。本文结合攻击技术、防御思路与实际案例梳理经验，制定对应防护方案，能够有效提升整体网络安全防护水平。

一、网络安全威胁分析

（一）高级持续性威胁（APT）

APT 是现阶段网络环境中破坏力极强的攻击类型。这类攻击主要具备四大特点。

其一为持续性，攻击活动往往会维持数月乃至数年，攻击者长期潜伏，逐步渗透目标网络。

其二为针对性，攻击对象指向性明确，多选取政府、军工、科研机构及大型企业等高价值主体。

其三为隐蔽性，攻击者会借助代码混淆、加密传输、挪用正规工具等方式，躲避安全检测。

其四为技术先进性，攻击常结合零日漏洞、专属恶意程序等高端技术开展破坏活动。

完整的 APT 攻击可分为多个递进阶段，主要涵盖情报收集、初始入侵、建立立足点、权限提升、横向移动、数据窃取与痕迹清除等环节。攻击者大多通过钓鱼邮件、水坑攻击、供应链攻击等常见方式突破目标网络，完成初始入侵。入侵成功后，攻击者会利用系统漏洞、窃取账户凭证等方式提升操作权限，再通过内网横向移动持续渗透，不断扩大对网络设备和业务系统的控制范围。在完成内网渗透后，攻击者会窃取目标核心数据，或对关键信息系统进行破坏，最后清理攻击痕迹，规避安全设备检测与溯源排查。

当下 APT 攻击事件屡见不鲜。部分境外 APT 组织将目标瞄准能源、电力、交通等关键信息基础设施，相关攻击行为带来了极大的网络安全隐患。在金融领域的相关事件里，攻击者长期潜伏达 18 个月以上，大量核心敏感数据遭到窃取。从各类实际事件不难看出，APT 攻击已然演变为国家之间网络博弈的主要手段之一。

（二）勒索软件攻击

勒索软件近年来传播速度迅猛，已成为破坏力极强的网络攻

 Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

击手段。这类攻击主要通过加密数据、封锁系统等手段，胁迫受害方支付赎金。据相关统计，2024 年全球勒索软件攻击突破 4500 起，由此产生的经济损失逾 300 亿美元。

勒索软件的攻击技术仍在持续升级。其传播渠道不再单一，除了传统邮件附件，如今还可借助系统漏洞、远程服务、供应链等途径扩散。攻击者的目标选择也愈发精准，通常会提前探查网络环境，针对高价值主体发起定向打击。攻击形式演变为双重勒索，在加密用户数据的同时窃取信息，以曝光数据作为要挟。与此同时，勒索软件即服务模式开始流行，大幅降低了攻击实施门槛，不法分子可直接租用工具开展攻击。

勒索软件攻击对企业和机构造成严重影响。某医院遭受勒索软件攻击，系统瘫痪导致手术取消、患者诊疗中断；某制造企业遭受攻击，生产线停摆造成巨额损失。这些案例凸显了勒索软件防御的紧迫性。

（三）供应链攻击

供应链攻击是近年来兴起的一种危害较大的攻击形式。攻击者往往先入侵上游环节，比如软件供应商、硬件制造商或服务提供商。他们利用这些合法渠道，将恶意代码植入正常产品中，从而对下游用户发起大规模攻击。供应链攻击具有以下特点：（1）攻击面广：一次供应链攻击可影响成千上万甚至数百万用户；（2）隐蔽性强：恶意代码隐藏在合法产品中，难以被传统安全检测手段发现；（3）持久性高：恶意代码可能潜伏数月甚至数年；（4）危害性大：攻击者可获得用户系统的高级权限 [1]。

典型供应链攻击案例：某网络管理软件被植入后门，导致全球超过18000个机构受影响，包括多家政府机构和世界500强企业；某代码编辑器插件被植入恶意代码，影响大量开发者和软件项目。这些案例表明供应链安全已成为网络安全的重要环节。

（四）零日漏洞攻击

零日漏洞，指暂未对外公布，也暂无官方修复补丁的系统安全缺陷。利用该类漏洞发起攻击，往往能在漏洞曝光与补丁上线前实现高成功率入侵。2024 年全球对外披露的零日漏洞数量超 1200 个，相较往年出现明显增幅。

零日漏洞攻击大多瞄准操作系统、浏览器、办公软件、移动端应用等主流常用程序。借助这类漏洞，攻击者能够规避常规安全防护，实现远程控权、提升权限、盗取数据等恶意操作。零日漏洞在地下交易市场身价不菲，部分单个漏洞售价可达数十万美元，也由此催生出专门的漏洞交易产业链。

二、网络防御技术

（一）入侵检测与防御系统

入侵检测系统与入侵防御系统是网络安全防护体系中的核心基础设备，二者协同配合，构建起基础的网络安全防御屏障。其中，入侵检测系统主要负责监测网络流量、采集系统日志数据，通过分析比对数据信息，识别网络中的异常操作与各类攻击行为，并第一时间发出安全预警。入侵防御系统则具备主动防御能力，能够在精准识别攻击行为后，自动拦截攻击链路，有效规避网络安全风险。

入侵检测技术包含特征检测、异常检测与混合检测三类。特征检测比对攻击特征库，准确率高，无法识别未知攻击。异常检测依据正常行为基线判别异常，可发现未知攻击，但误报率偏高。混合检测结合二者，优化整体检测效果 [2]。

如今入侵检测系统融合机器学习与深度学习算法，显著提升了智能检测能力。机器学习可自主归纳各类攻击行为特征，有效应对不断出现的新型网络威胁。深度学习则擅长解析大规模数据，精准捕捉隐蔽且复杂的攻击行为。市面上部分智能入侵检测产品，检测准确率可突破 98%，误报问题也得到大幅改善，降幅达 60%。

（二）安全态势感知

安全态势感知是对网络安全状态进行实时监测、分析、预警的技术体系。态势感知系统通过采集网络流量、系统日志、安全告警等多源数据，进行关联分析和态势研判，实现对网络安全态势的全局掌控。

态势感知系统的核心功能包括多个方面。数据采集主要收集网络设备、安全设备、服务器和终端等各类数据。数据处理则对采集到的信息进行清洗、标准化和关联分析。在此基础上，利用数据挖掘与机器学习技术开展态势分析。可视化展示以图形化方式呈现安全态势，便于安全人员理解和决策。预警响应功能能够及时通报安全威胁，并联动响应系统进行处置。

某省级网络安全态势感知平台，接入全省关键信息基础设施的安全数据，实现了对全省网络安全态势的实时监测和预警。平台运行以来，累计发现并处置安全威胁超过10万起，有效提升了网络安全防护能力。

（三）威胁情报

威胁情报涵盖网络安全相关的各类风险信息，主要包含攻击主体、攻击方式、恶意程序以及系统漏洞等内容。借助这类情报，相关机构能够清晰掌握潜在网络风险，进而落实对应的安全防护手段。

威胁情报包含多个类别。战略情报偏向宏观层面，研判威胁整体态势与发展趋势，为决策工作提供支撑。战术情报分析攻击者的动机、能力与攻击手段，面向安全管理人员。技术情报整理恶意代码特征、攻击标识等细节，供一线技术人员参考。运营情报为实时威胁数据，相关指标可直接接入安全设备与系统。

威胁情报平台（TIP）是管控与运用威胁情报的核心载体，支持情报采集、分析、共享及落地应用。开展情报共享，能让各类机构快速掌握最新风险动态，提前做好安全防护。目前国内不仅搭建了国家级情报共享机制，各行业也陆续上线专属平台，逐步构建起网络协同防御体系 [3]。

（四）零信任架构

零信任是当下主流的新型网络安全理念，核心准则为 “永不信任，始终验证”。传统架构依靠边界防护，默认内网环境安全；零信任则打破边界思维，正视内外部各类威胁，要求对每一次访问都完成身份核验与权限判定。其主要原则分为五点：一是对用户、设备及应用开展严格身份验证；二是遵循最小权限规则分配

Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

访问权限；三是借助网络微隔离，划分安全区域以遏制风险横向扩散；四是实时监控访问行为，动态调整权限；五是完整记录、审计全部访问行为。落地零信任常运用身份访问管理、软件定义边界、微隔离、安全访问服务边缘等技术。有大型企业完成架构升级后，安全事件减少七成，数据泄露隐患得到有效控制。

（五）安全编排自动化响应（SOAR）

安全编排自动化响应（SOAR）是一体化安全平台，集成编排、自动化、响应多项功能。它整合安全工具与数据资源，可自动处理安全事件，大幅提升安全运营效率。

SOAR 拥有多项核心能力。安全编排可汇聚各类安全工具，梳理统一工作流程。自动化执行按照预设规则开展操作，减少人工操作。事件管理覆盖安全事件全流程，实时跟进处置进度。报告分析能够汇总运营数据，评估安全状态与响应质量。金融机构应用该平台后，事件响应效率显著提升，平均耗时降至 30 分钟，自动化处置率 85%，团队工作效率提升三倍有余。

三、典型安全事件案例分析

案例一：某能源企业 APT 攻击事件。攻击者利用钓鱼邮件入侵企业网络，借助系统漏洞提升操作权限。其在内网持续横向移动六个月，最终盗走企业核心技术文件。结合事件复盘来看，该企业安全防护能力不足，员工安全意识欠缺，且缺少完善的威胁监测手段。对此企业开展多项整改工作，部署高级威胁检测系统，强化终端安全管理，落实网络微隔离，并定期组织安全培训。

案例二：某医疗机构勒索软件攻击事件。攻击者借助远程桌面服务漏洞侵入内网，投放勒索软件加密核心系统。此次攻击造成院内医疗服务暂停，中断时长共计三天。复盘事件可知，该机构长期未及时更新系统补丁，远程访问管控存在漏洞，数据备份工作也存在明显缺陷。后续机构落实多项整改：定期更新系统补丁，收紧远程访问权限，搭建离线数据备份体系，同时编制专项应急处置预案。

案例三：某软件供应链攻击事件。攻击者攻破软件开发工具供应链，在更新包内植入后门，波及全球数万用户。此次事件暴露出开发环节安全管控缺位，供应链风险评估工作也存在漏洞。后续相关方完善防护手段，规范开发安全流程，开展软件成分检测，搭建风险评估体系，并启用软件签名验证。

四、网络安全防护建议

（一）完善网络安全基础防护设施，搭建纵深防御架构

配备防火墙、入侵防御、终端检测等安全系统，并上线态势感知平台。针对 APT 攻击部署专项威胁检测工具，依托数据备份与恢复机制抵御勒索软件威胁，同时强化管控力度，防范软件供应链类攻击[4]。

（二）接入行业与国家级威胁情报共享体系，及时掌握各类安全威胁动态

企业内部做好情报分析工作，把情报运用到安全监测和风险防控中，实现从被动处置到主动预警的转变。建立跨部门协作机制，常态化交流分析结果，优化情报使用流程，保障信息顺畅传递。健全情报流转全流程，可加快威胁处置速度，提升防护能力，减少安全事故造成的影响

（三）聚焦网络安全领域的新技术发展

关注人工智能、量子计算、区块链的落地应用。发力智能检测、自动化运维与隐私计算等相关技术，逐步提升安全防护的智能化能力。

（四）打造专业网络安全人才队伍

当前人才缺口，已成为安全能力发展的一大阻碍。一方面完善学科建设，侧重培养实战型人才；另一方面搭建系统化培训体系，既强化在岗人员专业技能，也面向全体人员开展安全教育，普及安全防范知识[5]。

（五）完善应急响应机制

制定网络安全应急预案，明确应急响应流程和职责分工。建立应急响应队伍，定期开展应急演练。与专业安全机构建立合作关系，确保发生安全事件时能够及时获得专业支持。

五、结束语

网络空间安全形势日益严峻，APT 攻击、勒索软件、供应链攻击及零日漏洞等新型威胁持续演进，传统边界防御模式已难以应对。构建基于入侵检测、态势感知、威胁情报、零信任架构及安全编排自动化响应的主动防御体系成为必然选择。通过完善安全基础设施、强化情报共享、推进技术创新、培养专业人才并健全应急响应机制，可实现从被动防御向主动免疫的转变。唯有持续提升安全防护能力，方能有效应对日益复杂的网络攻击挑战。

参考文献

[1] 张耕源 . 论网络空间安全与攻防技术 [J]. 信息系统工程 ,2023(12):137-140.

[2] 罗坤瑾 , 许嘉馨 . 网络空间安全共同体构建的源起、逻辑与路径 [J]. 现代传播 ,2024,46(2):119-128.

[3] 徐艳艳 . 大数据背景下网络空间安全防御的研究应用 [J]. 中国宽带 ,2025,21(10):55-57.

[4] 梅亦 . 基于实战的网络安全攻防演练探索 [J]. 数字通信世界 ,2025(8):169-171.

[5] 冯登国 , 连一峰 . 网络空间安全面临的挑战与对策 [J]. 中国科学院院刊 ,2021,36(10):1239-1245.

 Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License