基于ATT&CK框架的铁路网络数据勒索攻击威胁模型研究

胡　骋　王　健*
北京交通大学　北京　100044

摘　要：随着信息技术在轨道交通领域的深度融合，铁路系统面临日益严峻的网络安全挑战，其中以“双重勒索”为代表的新型勒索软件攻击成为潜在的主要威胁之一。为应对此类威胁，本文首先分析了近年间主流勒索软件家族的攻击方式，然后评估并对比了多种主流威胁建模方法优缺点，提出了一种基于ATT&CK框架的铁路票务系统的勒索攻击全链条威胁模型。最后通过与STRIDE和攻击树建模框架的对比分析，验证了基于ATT&CK框架构建的威胁模型在威胁表达粒度与落地可评估能力等方面的综合优势。

关键词：勒索病毒；威胁建模；网络杀伤链模型；ATT&CK模型

引言

随着数字化时代来临，各个领域的组织和用户对信息系统和数据资源的依赖程度日益加深，数据已成为核心资产。以铁路系统为例，铁路作为国家重要的基础设施，其数据资源已形成一个庞大体系，渗透到运输生产的每一个环节。这些数据相互关联，不仅能提升运输效率和优化服务质量，更直接关系到国家交通网络的安全与稳定，成为铁路系统数字化转型的核心命脉。

正是因为这些数据极其重要，网络攻击者有了发动网络攻击的动机。其中，以勒索病毒攻击为代表的一系列网络攻击已成为全球范围内最具破坏力的网络攻击方式之一。勒索病毒本质上是一种恶意软件，通过加密算法，对受害者网络存储中的数据进行加密，阻止用户对自身数据进行访问，进而追要解密赎金。

铁路系统，尤其是客票系统的数据保护，已成为网络安全中的重要领域。随着客票系统对公众开放的服务和设备的增加，攻击者越来越多地将这些系统视为潜在的目标。

基金项目：2024年国铁集团科技研发项目“勒索病毒攻击场景下的铁路网络数据安全保护关键技术研究”（项目编号：N2024W007）

作者简介：
胡骋（2004.01--），男，汉族，江西吉安人，本科生，研究方向为网络空间安全。
王健（1975.09--），男，汉族，山东烟台人，博士，副教授，研究方向为网络安全。

为了解决这一问题，本文借助ATT&CK等威胁建模工具，对铁路系统进行了勒索病毒威胁模型构建，一定程度上为铁路系统安全团队精准地预测攻击路径、评估现有防御体系的薄弱环节，协助部署覆盖攻击链各阶段的、更具针对性的纵深防御策略。本文共包含四个章节，其中第1章介绍了勒索病毒的演进与当前威胁态势。第2章分析了当前勒索病毒威胁模型框架构建方法的优缺点，并选定ATT&CK框架作为威胁模型构建框架。第3章详细介绍了基于ATT&CK模型的勒索病毒威胁模型构建过程。第4章对提出的威胁模型进行效果展示与对比分析。第5章总结了全文内容，分析了本文研究中的局限性及未来研究重点。

一、勒索病毒威胁模型框架构建方法分析

面对日益复杂和具有破坏性的勒索病毒，仅依赖事件驱动的被动防御已无法满足要求。用户更希望转向一种主动的、结构化的方法来预测并抵御攻击。威胁建模能够有效实现这一想法。本部分分析几种主流的威胁建模方法，并探讨其在防御勒索病毒中的价值。

早期安全分析主要依赖专家经验，缺少标准化工具，随着系统复杂度上升，其局限性愈发明显。20世纪90年代末微软提出的STRIDE与攻击树方法，首次将威胁建模从抽象讨论推进到结构化的工程化实践；随后DREAD模型尝试用评分机制量化威胁优先级，但因其主观性强、复现性差，难以在实际场景落地，这也促使大家寻求更实际的方法。PASTA与OCTAVE在此背景下发展起来，它们分别从应用系统和组织管理视角切入，将业务目标

与合规需求纳入威胁分析，使建模不再局限于技术层面，而真正融入企业整体风险管理体系。与此同时，美国MITRE推出的ATT&CK框架则推动威胁建模走向实战化：它基于海量真实攻击行为构建知识库，以完整的战术链条刻画攻击者行动模式，具备更高的准确性与应用价值。

鉴于现代勒索软件从入侵到加密的周期大幅缩短，在攻击者完成数据窃取和加密之前，能否有效检测到其动向决定了最终破坏程度。ATT&CK能细致刻画勒索攻击全过程，对完整生命周期进行覆盖，并能准确映射勒索软件核心特征。因此，本研究最终选用ATT&CK框架进行威胁建模。

二、基于ATT&CK模型的勒索病毒威胁模型构建

铁路作为国家交通命脉，系统中承载着大量各级组织与用户的信息。以客票系统为例，其数据规模庞大，数据多级分布存储，并发高，还涉及隐私数据脱敏、防泄漏与防篡改需求，因此成为勒索组织眼中的“高价值目标”。本文以客票系统为例，基于ATT&CK框架构建了10阶段的攻击链模型，完整描绘了勒索病毒攻击客票系统全过程。以下是具体的10阶段攻击方式：

（一）初始访问

初始访问旨在突破外部防线并建立立足点，客票系统因攻击面广，常见路径包括：

①利用面向公众的应用（T1190）：此手段利用票务Web站点、App API等公开服务漏洞（如RCE、SQL注入）获取未授权执行权限。

②网络钓鱼（T1566）：此手段向具备权限的运维或者客服人员投递恶意邮件，通过诱导点击在办公终端建立控制通道。

（二）执行

在取得访问后，攻击方需执行恶意代码推进攻击。

①命令和脚本解释器（T1059）：利用系统原生命令行工具（PowerShell、Bash）执行侦察。

（三）持久化

持久化用于维持长期隐蔽访问，即便重启或凭证变化仍可控制系统。

①服务器软件组件（T1505）：此技术在Web服务器中植入Webshell，以正常HTTP/S流量维持后门。

②创建账户（T1136）：创建伪装为系统服务的隐藏高权账户，形成冗余访问通道。

（四）权限提升

此阶段的核心目标是将当前获取的低级别用户权限提升至系统级管理员权限，以解除后续操作的权限限制。

①利用漏洞进行提权（T1068）：攻击方利用系统内核或已装软件存在的本地提权漏洞获取完全控制权限。

（五）防御规避

攻击方通过多种技术绕过杀毒、审计等防护措施。

①混淆文件或信息（T1027）：攻击方利用加壳、加密或编码等手段，对其恶意载荷的静态特征进行处理，以对抗基于签名的检测引擎。

②主机上的指标移除（T1070）：为破坏安全审计的完整性与可追溯性，攻击方会系统性地清除或修改能够暴露其行踪的日志文件，从而增加事后取证的难度。

（六）发现

在获得稳固的立足点和高级权限后，获得稳固立足点后，攻击方对内部环境开展侦察。

①系统、网络与账户发现（T1082，T1016，T1087）：攻击方利用systeminfo、netstat、net user/domain等原生命令收集拓扑结构、高权账户与服务信息。

（七）收集

此阶段的目标是识别并聚合攻击方感兴趣的高价值数据资产，为最终的数据窃取做准备。

①存档收集的数据（T1560）：攻击方将导出的数据库内容打包为加密压缩档，作为暂存数据。

（八）命令与控制

攻击方与已植入恶意软件间建立通信通道。

①入口工具传输（T1105）：通过C2通道将核心勒索程序传入目标关键服务器。

（九）数据窃取

将已收集的数据上传至攻击方控制的外部位置，是“双重勒索”的基础步骤。

①窃取数据到C2（T1041）：通过加密、分块、限速等方式经C2渠道传输数据，规避出口流量检测。

（十）影响

攻击方通过破坏可用性和完整性实现最终目的。

①抑制系统恢复（T1490）：删除卷影副本、破坏备份，阻断快速恢复。

②数据加密勒索（T1486）：对核心数据进行强加密并留勒索信，完成最终打击。

图1为上述构建的威胁模型矩阵，包含10阶段、17种攻击方式。

三、基于ATT&CK框架的效果展示与对比

在完成基于ATT&CK框架的勒索病毒攻击链建模后，

阶段	初始访问	执行阶段	持久化	权限提升	防御规避	发现阶段	收集阶段	命令与控制	数据窃取	影响
攻击1	T1190 攻击服务漏洞	T1059 命令和脚本解释器	T1505 服务器软件组件	T1068 利用特权账户	T1027 混淆文件或信息	T1082 系统信息发现	T1560 存档收集数据	T1105 获取工具	T1041 窃取数据	T1486 数据加密勒索
攻击2	T1566 网络钓鱼		T1136 创建账户		T1070 清除指标	T1016 系统网络连接发现				T1490 阻止系统恢复
攻击3						T1087 账户发现				T1491 篡改销毁数据

图1　基于ATT&CK框架的勒索病毒威胁模型

我们对其在铁路客票系统中的适配性进行了初步评估，并与STRIDE、攻击树等常见建模方法对比，结果表明ATT&CK模型在多个方面具有显著优势。

首先，ATT&CK模型覆盖全面，更能贴近现实攻击行为。与STRIDE聚焦于威胁类别逻辑不同，ATT&CK基于实际攻击技术构建全链路视图，从初始访问到最终破坏均有明确对应，使构建的模型既具理论价值又具高度实战性。在客票系统场景中，从钓鱼邮件入侵到执行数据加密的各阶段均能在ATT&CK技术库中找到精确映射，避免了传统模型的抽象化问题。

其次，ATT&CK更有利于量化评估与红蓝对抗演练。其技术手段可直接用于构建攻击模拟与红队测试，帮助安全团队在真实场景中验证现有防御措施的有效性。相比之下，攻击树模型虽然能系统表达攻击路径，但缺乏攻击者行为细节，不利于后续生成具体的响应策略。而ATT&CK中的每一个技术点均可关联具体工具与检测建议，大幅提升防御措施的可落地性。

结语

本文借助ATT&CK模型等威胁建模工具，对铁路系统进行了勒索病毒威胁模型构建，一定程度上为铁路系统安全团队能够更精准地预测攻击路径、评估现有防御体系的薄弱环节（如漏洞利用、凭证窃取等），并针对攻击链的各个阶段（如持久化、防御规避、数据窃取等）部署更具针对性的纵深防御策略提供相关帮助。这不仅是应对当前勒索病毒威胁的有效途径，更是构建面向未来的、具备韧性的网络安全防御体系的关键基石。随着攻击手法的不断演变，持续更新和应用此类威胁模型，将是保障国家关键基础设施安全稳定运行的长期战略要务。

参考文献

[1]郑啸宇，杨莹，汪龙.基于ATT&CK模型的勒索软件组织攻击方法研究[J].信息安全研究，2023，9（11）：1054-1060.

[2]董昱宏，宋广佳.勒索病毒技术发展研究综述[J].计算机应用与软件，2023，40（01）：331-343.

[3]卡巴斯基.2024勒索软件年度态势报告概述[EB/OL].（2025-3-6）[2025-7-28]. https：//www.secrss.com/articles/76336

[4]Masum M, Faruk M J H, Shahriar H, et al. Ransomware classification and detection with machine learning algorithms[C]//2022 IEEE 12th annual computing and communication workshop and conference (CCWC). IEEE, 2022: 0316-0322.

[5]Kok S, Abdullah A, Jhanjhi N, et al. Ransomware, threat and detection techniques: A review[J]. Int. J. Comput. Sci. Netw. Secur, 2019, 19(2): 136.

[6]张福，程度，鄢曲，等.基于ATT&CK框架的网络安全评估和检测技术研究[J].信息安全研究，2022，8（08）：751-759.