Chapter 10
Advanced Cybersecurity Detection Techniques

Vinay Kumar Kasula
https://orcid.org/0009-0001-1131-3059
University of the Cumberlands, USA

Mounica Yenugula
https://orcid.org/0009-0002-3259-4563
University of the Cumberlands, USA

Bhargavi Konda
https://orcid.org/0009-0001-4704-1526
University of the Cumberlands, USA

ABSTRACT

This chapter delves into the evolving landscape of Advanced Persistent Threats (APT) from both an attack and detection perspective. It begins by reviewing the definition and characteristics of APTs, providing an overview of the various attack models developed over time. Building upon this foundation, the chapter introduces a comprehensive APT lifecycle model, which is divided into four distinct stages: information gathering, intrusion implementation, internal network attacks, and data exfiltration. For each of these stages, the chapter surveys research from the past five years, highlighting the latest advancements in both attack strategies and detection techniques. Finally, the chapter examines the dynamic interplay between attack and defense technologies, pointing out the challenges faced by both attackers and defenders. It concludes by discussing the rapid advancements in APT tactics and defenses, offering insights into the future directions for research and development in the field of cybersecurity and APT detection.

DOI: 10.4018/979-8-3373-3186-7.ch010

Copyright © 2026, IGI Global Scientific Publishing. Copying or distributing in print or electronic forms without written permission of IGI Global Scientific Publishing is prohibited. Use of this chapter to train generative artificial intelligence (AI) technologies is expressly prohibited. The publisher reserves all rights to license its use for generative AI training and machine learning model development.

1. INTRODUCTION

The pervasive digitization of societal infrastructure—spanning industrial automation, healthcare, finance, and personal computing—has intensified the attack surface for cyber threats. In parallel, the growing sophistication of threat actors, often equipped with nation-state-level capabilities, demands structured frameworks to systematically understand, detect, and mitigate cyber attacks. The MITRE ATT&CK Framework, a curated knowledge base of adversary tactics and techniques based on real-world observations, has become a de facto standard for threat modeling. While several studies have applied the MITRE ATT&CK Framework in cybersecurity analysis, the existing literature remains fragmented—often focusing on isolated domains (e.g., malware detection, network intrusion, IoT threats) or limited to either attack or defense strategies. Moreover, there is a lack of integrative lifecycle-based models that unify both adversarial techniques and corresponding detection methods within a coherent analytical structure.

This chapter addresses these gaps by proposing a comprehensive, lifecycle-oriented model of cybersecurity grounded in the MITRE ATT&CK Framework. It provides a dual-perspective analysis that systematically correlates attack vectors with detection methodologies, offering a structured synthesis of recent academic research and real-world threat cases. The novelty of this work lies in:

- Developing a cyber attack-detection lifecycle model that maps adversarial techniques to corresponding detection phases, using MITRE ATT&CK as a foundational taxonomy.
- Conducting a cross-domain synthesis that bridges traditional attack surfaces (e.g., web, malware) with emerging areas such as AI-based attacks, IoT vulnerabilities, and GNN-enabled defense systems.
- Integrating case-based evidence (e.g., Stuxnet, iOS 0-click attacks) with state-of-the-art detection techniques to demonstrate the real-world applicability and evolving nature of cyber threats.
- Highlighting research trends and gaps through bibliometric analysis of leading security venues (IEEE S&P, USENIX, NDSS, ACM CCS), with a focus on studies from the last five years.

The proposed lifecycle model segments the cyber attack process into preparation, execution, and persistence phases, each mapped to corresponding ATT&CK tactics and techniques. Parallel to this, detection methods are categorized based on their temporal applicability and technological basis (e.g., anomaly detection, GNNs, threat intelligence correlation). This structure facilitates comparative analysis, enabling the assessment of coverage gaps and overlaps across detection approaches.

38 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/advanced-cybersecurity-detection-techniques/390773

Related Content

ICT4D and its Potential Role in the Detection, Surveillance, and Prevention of Novel Zoonotic Disease Outbreaks for Global, National, and Local Pandemic Prevention

Shalin Hai-Jew (2014). *Human Rights and the Impact of ICT in the Public Sphere: Participation, Democracy, and Political Autonomy (pp. 94-143).*

www.irma-international.org/chapter/ict4d-its-potential-role-detection/112168

Impact of Islamic and Conventional Corporate Governance Mechanisms on Financial Performance of Islamic Banks: Evidence from Malaysia

Jamel Eddine Mkadmiand Khamoussi Halioui (2016). *Ethical and Social Perspectives on Global Business Interaction in Emerging Markets (pp. 186-203).*

www.irma-international.org/chapter/impact-of-islamic-and-conventional-corporate-governance-mechanisms-on-financial-performance-of-islamic-banks/146096

Social Workers and Agencies: How to Avoid Sexual Misconduct Issues on Social Media

Becky Anthonyand Jayleen Galarza (2017). *Sexual Misconduct in the Education and Human Services Sector (pp. 140-155).*

www.irma-international.org/chapter/social-workers-and-agencies/160491

Teacher Insight on RTI Implementation at the Middle and High School Levels: A Comparative Case Study

Pam L. Epler (2017). *Medical Education and Ethics: Concepts, Methodologies, Tools, and Applications (pp. 747-764).*

www.irma-international.org/chapter/teacher-insight-on-rti-implementation-at-the-middle-and-high-school-levels/167316

Regulation of Online Platforms in European and Global Jurisdictions

Irena Lovreni Držaniand Suzana Žili Fišer (2026). *Navigating Modern Digital Communication Ethics and Law (pp. 251-290).*

www.irma-international.org/chapter/regulation-of-online-platforms-in-european-and-global-jurisdictions/387245