Advanced Persistent Threats: Addressed and Open Research Questions

Shakhzod Yuldoshkhujaev*, Hyungjoon Koo**

Department of Computer Science and Engineering,
Sungkyunkwan University (Graduate Student*, Professor**)

Abstract

Advanced Persistent Threats (APTs) refer to sophisticated, long-term cyberattacks often carried out by state-sponsored actors targeting critical sectors and remaining undetected for extended periods. These attacks pose significant threats to national security and economic stability through espionage and sabotage. This paper surveys the current landscape of APT research, focusing on developments in detection methods, adversarial strategies, and cyber threat intelligence (CTI). Despite these advancements, unresolved challenges persist in areas such as APT tracking, zero-day vulnerability exploitation, and defense mechanisms for cloud and IoT systems. By highlighting both resolved and open research questions, this study aims to support ongoing efforts to enhance APT defense strategies and shape future research directions.

I. Introduction

Advanced Persistent Threats (APTs) are concealed and sophisticated cyberattacks that usually target critical infrastructure. These assaults can remain undetected in networks for long periods [6].

Given the severity of the dangers, the research community has made significant advances in understanding, identifying, and mitigating APTs. However, while substantial progress has been achieved in detection systems [7], adversarial tactics [2], cyber threat intelligence (CTI) [3], mitigation strategies [4], and dataset creation [5], there are still major research gaps. These gaps highlight the need for more research on APT evolution, mitigation measures, and sophisticated security systems. This work aims to give a broad review of the present status of APT research, categorizing the findings into two groups: research issues that have been effectively addressed [2, 3, 4, 5, 7] and those that require more investigation. This study attempts to highlight major advances in the area and open research questions to further be addressed.

This work was supported by the Basic Science Research Program through NRF grant funded by the Ministry of Education of the Government of South Korea (No. 2024R1F1A1074373), and Institute of Information & Communications Technology Planning & Evaluation (IITP) grants funded by the Korean government (MSIT) (No. 2024-0-01199; Graduate School of Convergence Security (Sungkyunkwan University), No.RS-2024-00398745; Proofs and Responses against Evidence Tampering in the New Digital Environment).

II. Advanced Persistent Treats

(Characteristics) APTs are a sophisticated form of cyberattack characterized by their long-term persistence, strategic objectives, and high level of organization. Typically

conducted by state-sponsored actors or well-resourced groups, APTs differ from common cyberattacks in their focus on maintaining undetected access to target systems for extended periods, often lasting months or even years [1]. Their primary objectives include espionage, sabotage, and the disruption of critical infrastructure, particularly targeting high-value sectors such as government, and financial institutions. To gain entry, APT actors employ a range of tactics, including the exploitation of zero-day vulnerabilities, software flaws unknown to the vendor, custom malware deployment, and social engineering. The consequences of these attacks are far-reaching, potentially compromising national security and essential infrastructure. This work aims to analyze the current research landscape on APTs, with a focus on both addressed and open research questions in the literature.

(Stages) APT attacks typically follow several distinct stages. The first stage is *reconnaissance,* during which attackers gather intelligence about the target, including details about the organization's infrastructure, software, or employee behavior. The second stage, *establishing a foothold*, involves the exploitation of vulnerabilities or the use of social engineering techniques to gain initial access to the network. Once inside, attackers engage in *lateral movement*, navigating the internal network to access more valuable resources. This phase often includes privilege escalation and the use of legitimate credentials, rendering detection particularly challenging. The *exfiltration* stage follows, during which the attackers achieve their primary objective, such as stealing data or disrupting operations. Finally, the *post-exfiltration* stage entails maintaining a presence within the network, either to continue exploiting the system or to erase traces of the attack to avoid detection [6].

III. Existing Works

Prior studies on APTs have made significant contributions to a wide range of research areas, although gaps remain in fully understanding and addressing these threats. Extensive research has been conducted in key domains, which we classify into four categories: *APT detection mechanisms* [7], *adversarial tactics* [2], CTI [3], *mitigation strategies* [4], and *dataset creation* [5], with many studies offering valuable insights into the complex nature of APTs.

(Detections) HOLMES [7] leverages the correlation of suspicious information flows within networks to identify potential APT activity. The authors focus on the challenges of detecting APTs due to their stealthy and prolonged presence in systems. HOLMES aims to address these challenges by monitoring and correlating various data points across the network, identifying malicious patterns that may indicate an ongoing APT attack. Through extensive evaluation, HOLMES demonstrates effectiveness in providing timely and accurate APT detection.

(Tactics) Addressing the complex nature of adversarial strategies, Bahrami et al. [2] introduced a cyber kill chain-based taxonomy that systematically categorizes the tactics, techniques, and procedures (TTPs) employed by APT groups. This study emphasizes how APT actors continuously adapt their techniques at each stage of the attack lifecycle to remain undetected, highlighting the evolving nature of their operations in response to defensive advancements.

(CTI) aCTIon [3] introduces an automated

framework that enhances the collection and analysis of real-time threat data from publicly available sources. This work focuses on streamlining the interpretation of CTI related to APT activities, enabling fast detection and more effective responses to emerging threats by leveraging automated tools to process threat indicators.

(Mitigations) Shen et al. [4] explored the effectiveness of Endpoint Detection and Response (EDR) systems using the MITRE Engenuity ATT&CK Enterprise Evaluation. Their study evaluates how well these tools perform in detecting and mitigating APT adversarial tactics in real-world environments, revealing both the strengths and limitations of EDR systems when faced with sophisticated, multi-stage APT attacks.

(Datasets) Stojanović et al. [5] reviewed the existing APT datasets and the modeling of attacks for use in automated detection methods. They emphasize the limited availability of public datasets, the challenges in obtaining realistic attack data, and the need to balance data privacy with the development of comprehensive datasets that capture the complexity of APT activities. This work highlights the crucial role of high-quality datasets in advancing research on automated detection techniques.

IV. Remaining Research

While APT research has made significant advances, several critical gaps requiring further investigation remain.

(Longitudinal Analysis) One of the key areas requiring further exploration is the longitudinal analysis of APT campaigns. Although there has been significant research into individual APT incidents, few studies have systematically tracked APT groups and their behavior over extended periods. A deeper understanding of how APTs evolve, adapt to defenses, and maintain persistence within targeted networks could yield important insights for developing more effective, long-term defensive strategies.

(Zero-day Exploitation) Another open question was described by Alshamrani et al. [6], which involves zero-day vulnerability exploitation. While this strategy is a common entry point for APT actors, the process by which these vulnerabilities are discovered, weaponized, and traded in underground markets is still not fully understood. More research is required to investigate the lifecycle of zero-day vulnerabilities in the context of APT campaigns, focusing on how they are integrated into attack strategies and how early detection or proactive mitigation can be improved. Addressing this challenge will help bridge the gap between vulnerability management and effective APT defense.

(Harnessing New Environments) The increasing reliance on cloud environments and Internet of Things (IoT) systems presents new challenges for APT detection. Current research [1, 7] has predominantly focused on traditional network environments, but as organizations migrate to cloud-based infrastructures and deploy IoT devices, APT actors are likely to exploit vulnerabilities unique to these systems. Further research is needed to develop detection and defense mechanisms specifically tailored to cloud and IoT environments, where the decentralized nature and shared security responsibilities complicate traditional security approaches.

(Lateral Movement Detection) Moreover, as Alshamrani et al. [6] further described, lateral movement detection remains a

persistent challenge in the fight against APTs. Although much progress has been made in detecting initial breaches and command-and-control (C&C) communications, identifying lateral movement within a compromised network, particularly when attackers use stealthy techniques, continues to be difficult. A majority of APT actors mimic legitimate user behavior, making it hard to distinguish between normal and malicious activities. Further research is necessary to improve lateral movement detection without generating excessive false positives.

Addressing all these open research questions is crucial for advancing APT defense strategies and keeping pace with the evolving threat landscape.

V. Conclusion

This paper surveys the current state of research on APTs, outlining both addressed and open research questions in the field. While significant progress has been made in key areas such as detection techniques, adversarial tactics, cyber threat intelligence, mitigation strategies, and dataset creation, several critical challenges remain unresolved. These include the need for more extensive longitudinal studies of APT campaigns, an improved understanding of zero-day vulnerability exploitation, and the development of robust detection mechanisms for cloud and IoT environments. Furthermore, challenges in detecting lateral movement within networks and ensuring privacy-preserving threat intelligence sharing remain pivotal areas for future research.

By identifying these open research questions, this paper underscores the need for continued innovation in APT defense strategies to keep pace with the evolving tactics of adversarial actors.

[References]

[1] Amit Sharma, Brij B. Gupta, Awadhesh Kumar Singh, and V.K. Saraswat. Advanced Persistent Threats (APT): Evolution, Anatomy, Attribution and Countermeasures. Journal of Ambient Intelligence and Humanized Computing 14, 7, 2023, 9355 - 9381.

[2] Pooneh Nikkhah Bahrami, Ali Dehghantanha, Tooska Dargahi, Reza M. Parizi, Kim-Kwang Raymond Choo, and Hamid H.S. Javadi. Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures. Journal of Information Processing Systems 15, 4, 2019, 865 - 889.

[3] Giuseppe Siracusano, Davide Sanvito, Roberto González, Manikantan Srinivasan, Sivakaman Kamatchi, Wataru Takahashi, Masaru Kawakita, Takahiro Kakumaru, and Roberto Bifulco. Time for aCTIon: Automated Analysis of Cyber Threat Intelligence in the Wild. arXiv:2307.10214, 2023. https://doi.org/10.48550/arXiv.2307.10214.

[4] Xiangmin Shen, Zhenyuan Li, Graham Burleigh, Lingzhi Wang, and Yan Chen. Decoding the MITRE Engenuity ATT&CK Enterprise Evaluation: An Analysis of EDR Performance in Real-World Environments. In Proceedings of the 19th ACM Asia Conference on Computer and Communications Security (ASIA CCS '24), 2024, 96 - 111. https://doi.org/10.1145/3634737.3645012.

[5] Branka Stojanović, Katharina Hofer-Schmitz, and Ulrike Kleb. APT Datasets and Attack Modeling for Automated Detection Methods: A Review. Computers & Security 92, 2020, 101734. https://doi.org/10.1016/j.cose.2020.101734.

[6] Adel Alshamrani, Sowmya Myneni, Ankur Chowdhary, and Dijiang Huang. A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. IEEE Communications Surveys & Tutorials 21, 2, 2019, 1851 - 1877. https://doi.org/10.1109/COMST.2019.2891891.

[7] Sadegh M. Milajerdi, Rigel Gjomemo, Birhanu Eshete, R. Sekar, and V.N. Venkatakrishnan. HOLMES: Real-Time APT Detection through Correlation of Suspicious Information Flows. In 2019 IEEE Symposium on Security and Privacy (SP), 2019, 1137 - 1152. https://doi.org/10.1109/SP.2019.00026.