Jo Brown

CYSE 201s

11/16/2024

https://academic.oup.com/cybersecurity/article/10/1/tyad023/7504935?searchresult=1

Review on Advanced Persistent Threat Detection

Article Review 2

The article I have selected for this review focuses on the topic of Advanced Persistent Threats. Before an in-depth review of the article, definitions must be made; Advanced Persistent Threats (APTs) are threats within an organization's cybernetwork that utilize the latest technologies and cyberwarfare strategies to deeply infiltrate said networks and become entrenched. Cybercrimes perpetrated with the use of APTs are some of the most difficult to manage due to their nature as persistent thorns in the side of companies, and require careful planning and expertise to manage properly.

APTs by their very nature as cybercrimes utilize social engineering to make themselves an inroad into whatever system the perpetrator wishes to infiltrate, ranging from phishing attacks to email scams to scrape passwords. While these strategies may be the easiest to use, ATPs have become sophisticated enough to attack through Anti-virus software as well as firewalls intended to stop unauthorized access (Che Mat et al., 2024). The strategy behind ATP attacks is complex, with the article stating "An APT applies different attack tools to ensure that it can remain undetected within the target network for months and even years**..."** and "...The tools are consecutively used in different stages of the attack until they reach the target destination."(Che Mat et al., 2024). This ability to remain undetected poses serious risks to data integrity and cybersecurity within a firm, potentially allowing thousands of dollars worth of data to be stolen without any indication this is happening

In conclusion, Advanced Persistent Threats pose one of the greatest risks to cybersecurity due to their ability to largely remain undetected. The social repercussions of this fact is the potential to lead to the distrust of cybersecurity firms who may be unable to prevent APTs from taking hold.

Che Mat, N. I., Jamil, N., Yusoff, Y., & Mat Kiah, M. L. (2024). A systematic literature review on advanced persistent threat behaviors and its detection strategy. *Journal of Cybersecurity*, *10*(1). https://doi.org/10.1093/cybsec/tyad023