Peer Response by: Aldo Madrid

Thank you for your post Zihaad, I t was a great opportunity to get introduced to the concept of Advance Persistence Threats (APT).

Cyberattacks can be categorized into two groups: targeted and untargeted attacks (Khalid, Zainal, Aizaini, Ghaleb, 2021). Normally the objective of untargeted attacks is infecting as much computers and networks as they can without having a particular target. In the other hand the targeted attacks require more planning and a more efficient strategy to infiltrate a specific target. These last types of attacks normally are founded by governments or organisations with vast economical resources.

The APT are considered as a targeted attacks because they stay in the systems of a targeted organisation for an extended period recollecting and analysing data to later perform a more efficient attack. Formally there are 6 identified stages of the life cycle of an APT (Khalid, Zainal, Aizaini, Ghaleb, 2021): reconnaissance, weaponize, deliver, exploitation, installation and command and control. Attackers go through these stages infiltrating deeper in every stage until finally they possess full communication with the networks and systems of the organisation and proceed to perform its malicious operations.

To protect from APT’s organizations use intrusion detection systems. They can be signature or anomaly based. The signature-based systems require a previously existent database with information of past attacks, to compare attackers’ signature with the ones in database. This technique is less effective than anomaly based because it does not grant protection to newer attacks. The second type of intrusion detection systems compare normal data sets with malicious data sets that usually are generated with machine learning methods.

As a curious fact the majority of APT are made with zero-day attacks, because they usually are attacks with no previous knowledge about them which make them harder to detect. The term zero-day was used by developers because when a vulnerability exploited by these attacks was detected, developers had zero days to fix it (Riofrío, Astudillo, Tello, Merchan, 2021).

Khalid, A., Zainal, A., Aizaini, M., Ghaleb, F. (2021) Advanced Persistent Threat Detection: A Survey. Available from: https://ieeexplore.ieee.org/document/9392626

Riofrío, X., Astudillo, F., Tello, L., Merchan, J. (2021) Zero-day attack: Deployment and evolution. Pp 38-53. Available from: https://lajc.epn.edu.ec/Volumenes/LAJC\_vol8no1.pdf