Application of Advanced Persistent Threat Actors‘ Techniques or Evaluating Defensive Countermeasures

Cameron Noakes

January 2022

1 Sentence Overview

This literature focuses its efforts on detailing the development of a methodology for adversarial tactics in addition to making determined requirements for information security system and evaluating defensive countermeasures. Using this proposition would provide a minimum basis of requirements and recommendations for measures to protect information and assets.

The literature research and proposed solution uses the Russian Threat Data Bank provided by Federal service of technical and export control (FSTEC TDB) as an example of information security threats classification in their work.

2 ATT&CK Implementation Methodology for Defensive Countermeasures Evaluation

The main idea behind the proposed solution from the researchers of the method is to determine the actor's techniques which can then accurately be mapped into information systems with structural and functional characteristics.

The researchers in this literature conducted preparatory measures in order to collect and concatenate knowledge about the actors' tactics and techniques into the process of designing an information protection system, where quantitative results were obtained which are identified later in the literature.

The literature research and proposed solution uses the Russian Threat Data Bank provided by Federal service of technical and export control (FSTEC TDB) as an example of information security threats classification in their work.

To develop adequate countermeasures for adversarial cyber attacks and threats and the methodology proposed, it is outlined that the first step is often to identify analytics in the information system according to the previously defined set of actors' techniques of actions which can be achieved through using the 'Cyber analytic repository' (CAR) database.

3 Conclusion

This literature was comprised of discussion around developing a threat actor methodology to better advance the integration of defensive countermeasures to better protect information systems and assets. Using specific databases like FSTEC TDB, the researchers were able to accurately map out specific areas of the methodology.

4 What problem does this solve?

There is currently no minimum basis of requirements and recommendations for measures to protect information and assets according to the researchers therefore proposing a methodology can help achieve this.

5 How do they solve it?

The researchers discussed relevant research and the development of a methodology that could be used by threat actors to help defend cyber attacks with high grade countermeasures.

6 How do they assess it?

There was no mention from the researchers for how they would assess this methodology and what success metrics they have taken to ensure it has real world industry value, no beta testing or evaluation approaches either.