APT Threat Intel Project - Information Guide

Description

APT (Advanced Persistent Threat) is a complex persistent attack that attempts to break into computing devices. The term was coined after Mandiant released the first report in 2013. APT attacks are carried out by advanced malware groups. Each of these “attacks” use multiple malwares and go through multiple steps in their attacks (MITRE ATT&CK tactics). These attacks have been documented and grouped together to form APT databases (Mandiant Advanced Persistent Threats). Since APT groups target high importance organisations (governments, big/multiple companies), the methods used are often novel. Oftentimes, zero day attacks are employed. However, many of the APT groups reuse malwares for the respective attack stages. Hence, it's not impossible to detect the attacks, which otherwise don't fit into the models used by most antivirus solutions. Following this idea, there's space for improvement in preventive solutions that would detect such advanced attacks.

Objective

To build a solution that is capable of detecting APT attacks on a host machine before damage has been done. This solution should work on a proactive basis instead of reactive. Hence, the long term goal is to implement a model that can predict the next action of a software or tool, installed on a device, given its current state. This “behaviour”-based approach would make sure the malwares are caught in the initial-most of an attack stage. In contrast, current antivirus solutions mainly detect based on policy matches. Our product should be able to actively “hunt” for the malwares on the host machine and thereby protect it.

Plan of Action

The project is being headed by the Dean, School of Computing (Dr Shankar Shriram). After discussions with him, along with Dr Sujeet Jagtap (who shall be supervising the project), we currently have formulated the following phases:-

Phase 1

Collect the signatures of all the APT groups we can gather (there are over 150). Collect the signatures of the individual malwares used in each attack. Build a repository of all the signatures.

Phase 2

Use the repository of signatures to build a model for an Intrusion Detection System that can detect any attacks, if they use the existing malwares. Hence, they could detect any attacks from the past APT groups. This phase would also involve analysing more about the behaviour of the malwares. Further details to be added.

Phase 3

Train and build an AI model that can predict attacks based on the patterns of the malwares instead of signatures alone. This module would be responsible for building a threat Intel solution that works on the behaviour of the malwares, instead of previously framed policies. Once an attack is detected, the model should be able to integrate the knowledge acquired it into its knowledge base. Further details to be added.

Deadlines and Reviews

Since this project involves fundings from external sources, strict deadlines are being imposed on the work. We shall also have frequent reviews to guage the progress.

The tentative details are as follows:-

Phase	Deadline	Reviews
1 (Building repository)	3rd Aug, 2024	To be decided
2 (Building model for IDS)	To be decided	To be decided
3 (Further works)	To be decided	To be decided

Requirements

This project is open for interested persons. We want to only underline the following:-

- Willingness to learn: The field of the project is new for everyone involved. We would love if you have prior experience. Regardless, willingness to learn is sufficient.
- Starter resources: We have a few starter resources you can go through to get a headstart regarding the project. Please contact Abdul Haq for the same.
- Deadlines: Deadlines and reviews are the only “restrictions” we have regarding the project. We are working with a time constraint and deadlines and reviews would be strictly enforced. Further details to be discussed.

Miscellaneous

- We have access to the Cybersecurity Lab in TIFAC Core. Whenever the lab is free, it can be utilised for this project. There are plans for a more “permanent” workspace soon.
- We will figure out a storage solution soon for the repository (Phase 1).
- Some links:
    - What's VT Hunting? (virustotal.com)
    - MalwareBazaar | API (abuse.ch)
    - Index of /malware-bazaar (abuse.ch)
    - API Scripts and client libraries (virustotal.com)
    - ClamAVNet
    - MalwareBazaar | About (abuse.ch) (See the Technology section)
    - APT Groups and Operations - Google Sheets