On the use of Cyber Threat Intelligence (CTI) in Support of Developing the Commander's Understanding of the Adversary

Cameron Noakes

February 2022

1 Sentence Overview

The collection of adversary related data is mapped to the techniques and tactics described in the ATT&CK framework matrix. In order to derive evidence to support adversary characterisation and to help in cyber threat intelligence (CTI) the model needs to determine the best possible multi-domain courses of action.

This literature describes the methodology, approach, outcomes and next steps for the conducted experiments and the subsequent mapping of adversarial data to ATT&CK tactics and techniques within the matrix.

2 Introduction

The active collection of information and data from the tactics and techniques via cyber threat intelligence feeds can also aid in understanding adversary characteristics which can be used to support various theories of adversary identification and mindset/methodologies.

The Allied Command Transformation (ACT) and the Communication and Information Agency (NCI) conducted experimentation focused on the employment of deception techniques such as honeypots to collect adversarial data from a practical use case in real world scenarios to be able to collect the most relevant and accurate data possible due to the attacker not knowing they are in a fake computer honeypot. The collected adversarial data was then subsequently analysed, with reference of the ATT&CK framework, to highlight known patterns

of adversary activity.

The ACT and NCI agencies conducted honeypot exercises to collect adversarial data, the researchers of this literature use the data collected by these agencies in their efforts to map to tactics and techniques in the ATT&CK framework to this data, identifying and highlighting its importance and relevance to expand and summarise upon.

This referenced and conducted objective with the honeypot was achieved via the execution of three test use cases:

1) validate that honey pots are able to provide "rich enough" information for analysis

2) Check that the data from the first test case can be mapped to the tactics and techniques of the ATT&CK framework

3) validate that operational context based on the threat actors identified in test case 2 can be collected using the Malware Information Sharing Platform (MISP).

3 Testbed Preparation

A mock test environment was prepared, the test environment was intentionally simple to allow more of a focus on the data collection aspects. A DMZ, CORE, User LAN and Administrative segment were created. The environment consisted of several Virtual Machines (VMs) to emulate user workstations, servers, honeypots and alike all situated within the user Local Area Network (LAN).

4 Validation and Deception Technologies

A common deception technology is to deceive the attacker into thinking they are on a real workstation whether that be as a normal user of admin/root, these methods are developed into a practical use case of honeypots, these can offer enough data about the adversary and their mindset, methodology and motives to map findings to the ATT&CK framework's tactics and techniques.

The deployed trap honeypots were highly interactive, meaning full installations of the OS footprint used on operational systems were installed and deployed to provide a more throughout fake computer, allowing the attacker interacting with the honeypot full ability to explore the system and perform a large variety of functions in an adversary attackers toolkit.

The experiment with honeypots was able to correctly identify which adversary information collected related to specific tactics and techniques in the ATT&CK framework and the illustrative image is shown being somewhat readable [figure 5].

MISP and open source intelligence (OSINT) can help provide interesting information that, when coupled with metadata, can provide a better understanding of the adversary.

5 Conclusion

The researchers leveraged 3 Test Cases (TCs) for cyber threat intelligence in very unique ways to facilitate support for adversary characterisation through various real world use cases and experiments to make unbiased datasets and information ready for the analysis and subsequent mapping to the ATT&CK tactics and techniques in the ATT&CK framework matrix.

This paper is about taking CTI data and analysis from two agencies to then map it to ATTCK tactics and techniques, there is no machine learning as there is no automation process.

6 What problem does this solve?

CTI requires mitigation strategies and various other information sets and to accomplish this requires certain mapping of frameworks to applications in order to form an overall solution to help with CTI.

7 How do they solve it?

The researchers proposed and developed a system solution that takes unbiased real world, practical datasets and information and accurately maps them to the ATT&CK frameworks tactics, techniques for various reasons such as better mitigation strategies but mainly to conclude on adversarial behaviour mindsets and methodologies.

8 How do they assess it?

The assess the current solution the researchers developed through a testbed. Testing was performed from within their own experimental techniques listed as: a DMZ, CORE, User LAN.