Offensive Security: Towards Proactive Threat Hunting via Adversary Emulation

Cameron Noakes

February 2022

1 Sentence Overview

The proposed solution is based on a novel approach of adversary emulation by mapping each phase and model inside the threat hunting approach. The results from the experiments conducted are for the proposed solution approach using cyber threat hunting via adversary emulation on hunting advanced persistent level threats. This work is built upon the 'Atomic Red Team' mechanism to create various test cases for the ATT&CK framework matrix tactics and techniques.

The threat detection ability of the proposed solution approach uses minimum resources, allowing the approach to be used in various limiting environments. The proposed solution approach can be used to develop the security infrastructure environment for organizations and to help uncover advanced attack mechanisms and test for attack detection.

2 Introduction

The researchers said how threat hunting often uses data from different sources, some examples are endpoints, Indicators of Compromise, Firewalls and Intrusion Detection and Prevention Systems (IDS, IPS), providing relevant datasets and examples of where the researchers got their data from for the proposed solution approach and any analysis conducted.

Many organizations, as mentioned by the researchers, conduct offensive security exercises such as penetration testing and adversary simulation for many various reasons such as testing security, training and development, securing systems or recon. e. In an evolving threat environment, where attackers are

motivated to employ sophisticated attacks it is crucial to identify and understand these sectors and what they gave to offer.

The researchers identified a useful approach by using event logs, event logs generated at endpoints can, over time, retain huge information. Such logs require significant processing and analysis which increases the usage of resources, since the researchers are developing an approach/model using minimal resources it resolves to the conclusion that using endpoint event logs would not be the most efficient which gives the reasoning behind using other methods. False positive alerts are also said to be within the event logs, providing in a less efficient and robust model.

In the paper, the researchers propose a threat hunting model approach as a proposed solution via adversary emulation with minimal resource utilization to allow organizations to perform two different related tasks simultaneously.

The proposed solution was developed and then assessed via an evaluation approach to identify the skilfulness of the proposed approach. This was done by testing the approach with various advanced persistent threats (APTs) in an emulation/ simulation environment with fully patched up to date systems.

The developed and given approach for the proposed solution uses an induced form of another model (seen in the first referenced appendix resource in the paper) with an addition of an adversary emulation model. The research provides an efficient method for evaluating internal infrastructure security such as computer and network security using threat hunting through offensive security techniques.

3 Threat Hunting and Offensive Security Approach

The researchers developed the proposed approach by integrating a proactive approach for hunting cyber threats within an adversary emulation process and model the threats on the basis of techniques used in offensive security.

Some of the example metrics taken to be assessed for relevance are below:

threat severity

progression

relevance for threat modeling

The authors of the literature and the proposed solution exclaimed how they have used PE files, OLE files and PS1 for the experiments for the proposed approach. The proposed offensive security model consists of eight steps which are sequential (in order).

The given steps are seen below which are provided in the literature by the researchers:

purpose

scope

equip

planning

weaponizing

plan review and validation

execute

reporting

Mathematics and algorithmic equations are used within this literature to calculate things such as 'Scope set S, Equip set E, Weaponization set and Execute set EX', with various other mathematical algorithm equations to provide other variable results as well, provided with definitions of all these resulting variables under all the equations.

Mathematics was used in the form of algorithms in the above scenario in the literature, under these algorithms using math were coding algorithms to propose Sending and Generating Phishing Mails. Where the given coding algorithms will check the payload type, and if it is a malicious document then it will try to inject malicious code inside of the PDF document or macros in a Word document (docx).

4 Experiment

The researchers exclaim that their experiments are lab based but aim to closely represent real world scenarios. This is evident from the use of attack emulations and simulations with these being mapped from datasets previously mentioned.

Example attacks are given with the mitigation strategies in the literature explained by the researchers to provide examples of the types of attacks used in the simulations/emulations of internal; infrastructure environments to develop and test their proposed solution approach.

5 Conclusion

A novel hybrid model approach for launching offensive security exercises to understand attack patterns better using threat hunting is proposed.

The proposed approach has increased efficiency for identifying and also countering cyber threats whilst using real world scenarios for advanced cyber threats and presents an algorithm to generate attack vectors for phishing.

6 What problem does this solve?

Limitation for defense teams to understand attack patterns to their full extent, with making countermeasures and efficiency of finding new cyber threat attacks easier.

7 How do they solve it?

By proposing a solution model approach using adversarial emulations and mathematical algorithms and equations with datasets to launch offensive security exercises.

8 How do they assess it?

In order for the researchers to validate their proposed solution of an approach model, they built a simulated environment to launch real world APT attack scenarios on various patched systems.