A Strategic Framework for Mitigating Advanced Persistent Threats: A Hidden Markov Model Approach

Rudra Prasad Baksi and Shambhu J. Upadhyaya

Abstract

Deception has been proposed in the literature as an effective defense mechanism to address Advanced Persistent Threats (APT). However, administering deception in a cost-effective manner requires a good understanding of the attack landscape. In this paper, we develop a Hidden Markov Model based framework where the indicators of compromise (IoC) are used as the observables. This framework would help in selecting an appropriate *deception script* and triggering the proper defensive strategy when faced with APTs or other malware. The effectiveness of the model and the associated framework are illustrated by considering ransomware as the offending APT in a networked system.

Summary

Problem Addressed:

- Traditional signature based detection techniques are not effective against APTs
- New techniques that could gather attacker's intent and attack mode are desired
- Ultimate goal is to detect APTs of the type of ransomware

Solution Technique:

- Deception is used as a defense strategy
- A Hidden Markov Model (HMM) based detection model was designed, as APTs are known to be quiet invaders
- Indicators of Compromise (IoC) are used as observable features to design the detection model

Key Result:

- A HMM based ransomware detection model
- A cost effective model to fend-off attacks from APT groups

Deception

The idea is to deceive the attacker into believing in it's success while triggering a cost effective counter measure to repel attacks from APT groups by deploying the costliest defensive strategy against the most aggressive attack.

The Model

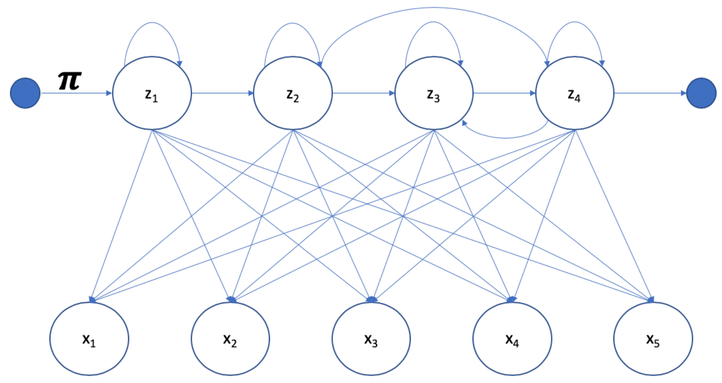

Figure 1. HMM based ransomware type APT detection model

Hidden Sates:

- z_1: Malware
- z_2: Ransomware
- z_3: Ransomware + APT
- z_4: Ransomware + APT with Contingency Plan of Attack

Observable Sates:

- x_1: Reconnaissance
- x_2: Interaction with honeypots or real-databases of high value
- x_3: Backdoor implants and/or back-channel traffic
- x_4: Existence of "Campaign Abort" strategy
- x_5: Existence of other contingency plan of attack

Transition Probability:

$$T(ij) = p(z_{k+1} = j | z_k = i)$$

Emission Probability:

$$\varepsilon_i(x) = p(X_k = x | z_k = i)$$

Initial Probability:

$$\pi(i) = p(z_1 = i)$$

Transition Matrix

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & 0 & 0 \\ 0 & \alpha_{22} & \alpha_{23} & \alpha_{24} \\ 0 & 0 & \alpha_{33} & \alpha_{34} \\ 0 & 0 & \alpha_{43} & \alpha_{44} \end{bmatrix}$$

Emission Matrix

$$B = \begin{bmatrix} \beta_{11} & \beta_{12} & \beta_{13} & \beta_{14} & \beta_{15} \\ \beta_{21} & \beta_{22} & \beta_{23} & \beta_{24} & \beta_{25} \\ \beta_{31} & \beta_{32} & \beta_{33} & \beta_{34} & \beta_{35} \\ \beta_{41} & \beta_{42} & \beta_{43} & \beta_{44} & \beta_{45} \end{bmatrix}$$

Analysis

Once the experiments are carried out, we will have numerical values for the transition, emission and initial probabilities for the system. Then we plug-in the values from the matrices in the probability equations to detect the status of the malware.

Application

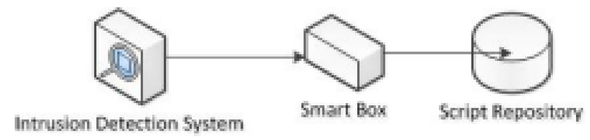

Figure 2. Smart Box

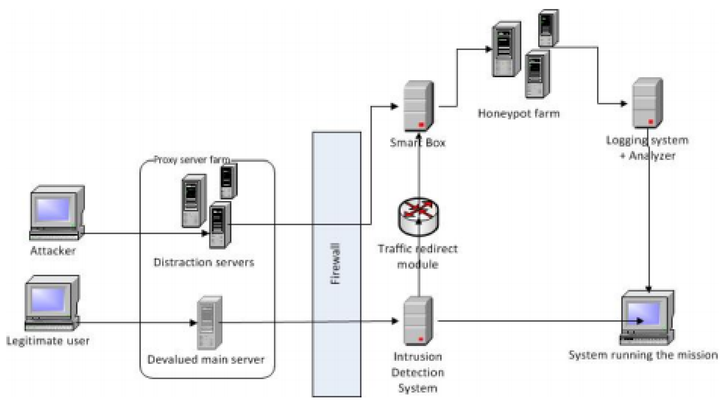

Figure 3. Deception Framework for mission survivability

Conclusion

The paper designs a Hidden Markov Model (HMM) based ransomware type APT detection model. This would help the defender to make informed decision regarding a cost-effective countermeasure against the attacks mounted by APT groups. The cost-effective defensive strategy is put forward so as to not degrade the quality of service (QoS). Deception helps the defender to surreptitiously trigger a countermeasure which denies the attacker the opportunity to become more aggressive.

Acknowledgment

This research is supported in part by National Science Foundation Grant No. DGE-1754085.

References

1. Baksi, R.P., Upadhyaya, S.J.: Kidemonas: The silent guardian. arXiv preprintarXiv:1712.00841 (2017).
2. Baksi, R.P., Upadhyaya, S.J.: A comprehensive model for elucidating advanced persistent threats (apt). In: Proceedings of the International Conference on Secu-rity and Management (SAM). pp. 245–251. The Steering Committee of The WorldCongress in Computer Science, Computer (2018).
3. Mehresh, R., Upadhyaya, S.: A deception framework for survivability against nextgeneration cyber attacks. In: Proceedings of the International Conference on Security and Management (SAM). p. 1. The Steering Committee of The World Congressin Computer Science, Computer (2012).
4. Mehresh, R.: Schemes for surviving advanced persistent threats. Faculty of theGraduate School of the University at Buffalo, State University of New York (2013).
5. Hutchins, E.M., Cloppert, M.J., Amin, R.M.: Intelligence-driven computer networkdefense informed by analysis of adversary campaigns and intrusion kill chains.Leading Issues in Information Warfare & Security Research1(1), 80 (2011).
6. LogRhythm: The apt lifecycle and its log trail. Tech. Rep. (July 2013).

University at Buffalo The State University of New York

Dept. of Computer Science and Engineering
University at Buffalo, SUNY
rudrapra@buffalo.edu