ASSIGNMENT 4:

Literature Review

Gaston Carvallo - 048530133, Cedric De Pano - 110569159, Loyd Rafols - 022827158

REA605: Research Methodologies

February 8, 2021

Abstract

Machine learning is an up-and-coming technology which brings many advantages to a security operation center through automatically processing data into meaningful intelligence. A properly trained machine learning model can identify threats, limit the amount of manual work and processing done by a human administrator, and increase the security of a network against realized threats. Existing approaches for detecting malware through machine learning predominantly focuses on changes in behaviour of a system, before and after infection, along with detecting malicious traffic over web traffic. Network-level detection and analysis brings a valuable perspective to malware detection, augmenting the system-level features present in antimalware software, as this would provide an early warning of malware activities taking place on a network which gives administrators the information required to remediate the threats before significant damage is caused. In this literature review we look at different articles related to the topic of detecting malware through network traffic analysis using a machine learning model. we describe the state of the art around the topic, as well as identifying limitations and future work done by experts in the field. To do so, several peer-reviewed papers from each subtopic were evaluated for their contribution to the field, and their limitations and future work were listed as potential gaps that could be filled with the research done on this paper.

Contents

Introduction

Many organizations deploy an IDS[1] in order to protect themselves from malicious attacks. These devices seek to analyze data captured by its sensors and raise alarm to human analysts that make the final determination. Depending on the algorithm the IDS uses to determine if an attack is occurring, they can be categorized in on of 3 types:[2]

a) Rule or signature based:

The IDS looks for specific data patterns that have previously linked to attacks. while fast and efficient they cannot detect novel attacks and are susceptible to adversaries attempts to obfuscate the attack by intentionally changing its pattern.

b) Statistic or anomaly based:

Statistics-based algorithms attempt to detect anomalies in user or network behavior by creating a model of normal behavior and using statistical analysis to determine if the observations are significantly different.[3]

c) Machine learning (ML):

Consist in training a classifier, an algorithm that is trained to classify data in categories. most commonly attack/legitimate.

In order to properly implement a machine learning model, we first have to look at the general state of study for machine learning, network traffic analysis and malware behaviors,

[1] Intrusion Detection System - A software or hardware appliance that detects malicious traffic that passes through it.
[2] Gümüşbaş, Dilara, et al. "A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems." IEEE Systems Journal, doi: 10.1109/JSYST.2020.2992966.
[3] Gümüşbaş, Dilara, et al. "A comprehensive survey of databases”

culminating in the understanding of how to detect malicious traffic generated by malware using a machine learning model.

Literature Review

The research topic revolves around the concept of detecting malware through the network traffic it generates using machine learning classifiers and methods. To break down the topic, it has been organized into three distinct criteria: machine learning, network traffic analysis, and detecting malicious behaviour patterns.

Machine Learning

Das and Morris presented a list of machine learning (ML) methods and datasets used in cybersecurity, they highlighted the need to fully understand the data that will be used to train the selector - not only to be able to select the features to be incorporated in the model but to transform the raw data into a format that can be used by the ML algorithms.[4] They also identified some of the datasets available to researchers, the DARPA 1998/99 datasets, the KDD cup 1999[5] and the Mississippi State University SCADA[6] dataset, which they used to analyze the effectiveness of some of the most common ML methods - specifically, Naïve Bayes, Random Forest, J48, and the OneR method[7]. To test the effectiveness of the ML methods the receiver operating characteristics curve was plotted. This is done by plotting the true positive rate vs the false positive rate.[8]

---

[4]Rishabh Das and Thomas. H. Morris, "Machine Learning and Cyber Security," *2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE)*, Kolkata, 2017, pp. 1-7, doi: 10.1109/ICCECE.2017.8526232.

[5] The KDD Cup is an annual data mining and knowledge discovery competition.

[6] Supervisory Control and Data Acquisition

[7] Das and Morris, “Machine Learning and Cyber Security,” 4.

[8] Das and Morris, “Machine Learning and Cyber Security,” 4.

There are several surveys on machine learning on the literature, Gumisbas and other focus on deep learning methods and identify the most common attack types,[9] Gaonkar and others focus on techniques for botnet detections,[10] Aslan and Samet perform a comprehensive review on malware detection, they identified and evaluated 8 different categories of approaches.[11]

Network Traffic Analysis

The concept of analyzing a network's traffic for malicious traffic is central to our research topic. This mainly revolves around capturing a network's traffic, extracting the most relevant data for our purposes, then analyzing the extracted data[12] through a machine learning classifier model to extrapolate meaningful information. Jakob Premrn explores creating a device capable of detecting C2[13] channels using a machine learning model.[14] Premrn also believes that this machine learning model can be improved with a certain implementation of cyber threat intelligence - that is, threat intelligence does not need to be pre-classified like data in the machine learning model does.[15] This paper provides a good baseline point for detecting different specific malware variants as separate datasets. Jaimin Modi used the certificate-based fields of network connections capture (certificates, signers, and dates) as the features in the machine learning classifier model, in order to detect ransomware in encrypted traffic.[16] The primary

---

[9] Gümüşbaş, Dilara, et al. "A comprehensive survey of databases"
[10] Gaonkar, Shivani, et al. "A survey on botnet detection techniques."*2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, Vellore, India, 2020, pp. 1-6, doi: 10.1109/ic-ETITE47903.2020.Id-70.
[11] Aslan, Omar and Refik Samet, "A Comprehensive Review on Malware Detection Approaches," IEEE Access, vol. 8, pp. 6249-6271, 2020, doi: 10.1109/ACCESS.2019.2963724.
[12] Also called features.
[13] Also known as Command & Control - a method of controlling multiple infected hosts through a centralized server.
[14] Jakob Premrn, "*Analysis of command and control connections using machine learning algorithms*." University of Ljubljana, Faculty of Electrical Engineering, 2020, 5.
[15] Premrn, "*Analysis command and control machine learning*," 90
[16] Jaimin Modi. "Detecting Ransomware in Encrypted Network Traffic Using Machine Learning", University of Victoria, 2019, 5.

future work identified by Modi is to be more specific in its detection of malware, specifically the family of which a ransomware belongs to.[17] In Modi's dissertation, it is believed that there was insufficient coverage in detecting ransomware C2 channels through the usage of generating random subdomains using a DGA.[18] In these two papers, there is a gap in regards to the different permutations of the features used to analyze malicious traffic - particularly with DNS requests and replies through DGAs, amongst other features - in the used machine learning model.

Detecting Malicious Behavioural Patterns

Zhu and others introduce a network behavior-based method for detection of malicious reverse connections.[19] After concluding on a typical network communication pattern, network behavior features are extracted from TCP[20] sessions to be used as the detection model input. Algorithms were then applied on network traffic data collected, distinguishing malicious traffic from legitimate sessions such as cloud applications and P2P.[21] The proposed method has proven to also work for encrypted malware traffic, specifically remote access trojans. Ability of handling imbalanced data sets were evaluated based on detection accuracies of the tested algorithms. Ghafir and others also presented an approach for detecting of botnet C2 traffic that is capable of real time detection.[22] In their proposed system called BotDet, which is divided in two stages. They developed four modules for detection of different approaches used in malicious C2

[17] Modi, *"Detecting Ransomware Encrypted Traffic*", 68
[18] Domain Generation Algorithm - a C2 channel used by malware to establish connections between an infected host and a controller server by way of a randomly generated subdomain name.
[19] Zhu, H et al. "A Network Behavior Analysis Method to Detect Reverse Remote Access Trojan." *2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS)*, Beijing, China, 2018, pp. 1007-1010, doi: 10.1109/ICSESS.2018.8663903.
[20] Transport Control Protocol - used for transporting data over a network, the internet.
[21] Peer-to-Peer - direct connections from one host to another, without relying on a centralized host.
[22] Ghafir, I., et al "BotDet: A System for Real Time Botnet Command and Control Traffic Detection." *IEEE Access* 6 (2018): 38947–38958. doi: 10.1109/ACCESS.2018.2846740.2.

communications. Additionally, to reduce the rate of false positives, they also designed a framework for correlation which balances false positives and true positive rates.

Conclusions

In conclusion, this article explored the fields of machine learning, network traffic analysis and malicious behavioural patterns for their current state of the art, and potential limitations, future work and gaps in knowledge that can be applied to the research topic. Within the realm of machine learning, the most important takeaway when work starts on this project is to understand which data will be a meaningful contribution to the features used when training the machine learning model.[23] Network traffic analysis revolves around the idea of detecting traffic generated by malware using web traffic and other typically unencrypted means, but the work done by Premrn and Modi indicates future work to be done within the realm of encrypted traffic or through DNS[24] traffic. In terms of behavioural patterns, the work done by Zhou and others provides an important insight into the current state of malicious behavioural patterns, where malicious traffic can be successfully segregated from benign, normal traffic.[25] Finally, Ghafir and others provide a model capable of detecting C2 traffic in real time, which serves as a good basis for future work done within the research topic.[26]

[23] Das and Morris, "Machine Learning and Cyber Security," 2017
[24] Domain Name System - a protocol used to resolve IP addresses into human-readable domain names.
[25] Zhu, H et al. “Detect Reverse Remote Access Trojan.”, 1007-1010.
[26] Ghafir, I., et al “BotDet: Real Time Botnet Detection.”, 38947-38958.

Bibliography

Aslan, Omar and Refik Samet, "A Comprehensive Review on Malware Detection Approaches," *IEEE Access*, vol. 8, pp. 6249-6271, 2020, doi: 10.1109/ACCESS.2019.2963724.

Das, Rishabh and Thomas. H. Morris, "Machine Learning and Cyber Security," *2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE)*, Kolkata, 2017, pp. 1-7, doi: 10.1109/ICCECE.2017.8526232.

Gaonkar, Shivani, Nandini Fal Dessai, Jenny Costa, Ashlesha Borkar, Shailendra Aswale, and Pratiksha Shetgaonkar. "A survey on botnet detection techniques."*2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, Vellore, India, 2020, pp. 1-6, doi: 10.1109/ic-ETITE47903.2020.Id-70.

Ghafir, I., V. Prenosil, M. Hammoudeh, T. Baker, S. Jabbar, S. Khalid, and S. Jaf. "BotDet: A System for Real Time Botnet Command and Control Traffic Detection."IEEE Access6 (2018): 38947–38958. doi: 10.1109/ACCESS.2018.2846740.2.

Gümüşbaş, Dilara, Tulay Yıldırım, Angelo Genovese, and Fabio Scotti. "A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems." *IEEE Systems Journal*, doi: 10.1109/JSYST.2020.2992966.

Modi, Jaimin. "*Detecting Ransomware in Encrypted Network Traffic Using Machine Learning*", Master's thesis, University of Victoria, 2019.

Premrn, Jakob. "*Analysis of command and control connections using machine learning algorithms*." Master's thesis, University of Ljubljana, Faculty of Electrical Engineering, 2020.

Zhu, H., Z. Wu, J. Tian, Z. Tian, H. Qiao, X. Li, and S. Chen. "A Network Behavior Analysis Method to Detect Reverse Remote Access Trojan." *2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS)*, Beijing, China, 2018, pp. 1007-1010, doi: 10.1109/ICSESS.2018.8663903.