Network Deception Technologies and The Possible Integration with Artificial Intelligence

Simon Rafael Gaston
School of Sciences and Engineering
University of Asia and the Pacific
Pasig, Philippines
simonrafael.gaston@uap.asia

***Abstract*— Computer networks have employed a variety of techniques to secure themselves from attackers. A technique that is used is deception technologies, these are systems put in place to mislead a malicious actor and prevent them from accessing the important parts of a network. Such deception technologies include honeypots and moving target defense. Researchers are looking at improving deception technology by integrating artificial intelligence and machine learning in to facilitate the process.**

Keywords—Network security, honeypot, Moving Target Defense, Artificial Intelligence, Machine Learning, Generative Pre-Trained

I. INTRODUCTION

With the exponential growth of the internet and the ubiquity of electronic devices, there exists plenty of data that is utilized for business use or private individual use. As such the theft of data and breaches of network are becoming more a course of action for cyber criminals [1]. Computer networks are growing all the more susceptible and vulnerable to attacks by malicious actors; while modern software and systems have refined their methods to counterattack these attacks, so too have the malicious actors, they improve their modus operandi with more refined software [2].

A few of the techniques to mitigate the negative effects of such attacks is the implementation of improvements to Honeypots and Moving Target Defenses (MTD), some of which include the utilization of Artificial Intelligence (AI) and Machine Learning (ML) [3].

Honeypots in the modern computer network setting have evolved from their yesteryear form whereby they were not as interactive and not as encompassing as they are now. Honeypot technologies are now more sophisticated and more difficult to distinguish from the networks they try to imitate, much of its improvements can be attributed to the integration of AI and ML into their systems [4].

This paper intends to look into the various forms of such deception technologies, how networks can benefit from certain improvements in their implementation, and possible integration with AI.
This paper seeks to answer the following:

1. How did deceptive technologies come to exist?
2. What are the different techniques in deceptive technologies?
3. What do current researches recommend as the best techniques in deceptive technology?

II. RELATED LITERATURE

A. A. AI and ML

AI and ML are powerful tools that can observe various forms of datasets and render sophisticated analysis. In addition it can lead to the development of models of higher complexity [5]. The utilization of Reinforcement Learning (RL) in reducing the damage caused by zeroday attacks is a potential solution that can be integrated into the network security of IoT devices [6].

ML can be used as a suitable solution for detecting malware in networks. When defense teams partner ML with better system awareness of their networks, they will be able to better detect and respond to intrusions that occur in their network. ML can modify aspects of a network in an automated manner without the need for human intervention, thus being more efficient at implementing network security [3].

B. B. Honeypots and AI & ML

The key need to integrate AI smoothly with a Security Information and Event Manager (SIEM) technologies is indicated to be a potential solution to make defending networks more efficient. Such a solution would be able to funnel dynamic log types from honeypots into a SIEM which would otherwise be difficult without the integration of AI [4].

ChatGPT, through the use of Generative Pre-trained Transformer models, can be a tool for the expedited and easy creation of honeypots through the input of commands. In addition AI can then develop honeypots that are dynamic and draw the attention of potential attackers to the network [7].

The utilization of Machine Learning can expedite the creation of honeypots for Internet of Things (IoT) devices which reduces the resource strain on network security administrators for creating effective honeypots [8]. Such is of great assistance when considering that honeypots have various parts that can be interacted and automated with such as the degree with which they can be interacted with and if they are located on a server or a client [9].

C. C. Moving Target Defense

MTD is a defense mechanism which continuously modifies the various aspects of a device in a network to reduce the attack surface that a malicious actor would exploit as a vulnerability in their attack [10]. In addition the implementation of MTD to confuse and mislead malicious actors is also usually done with the integration of honeypots [11].

The advantages of using Machine Learning based Malware Detection are highlighted over more traditional detection methods, how it can be incorporated into a Network's defense and the importance of having a dynamically generated MTD system [11]. The results of this paper determine the ideal number of honeypots and MTDs to optimize the defensive capabilities of a network before diminishing returns occurs [11]. The creation of an effective MTD requires the combination of various techniques to create an optimization framework model that remains effective in the defense of a network with respect to budget constraints of an organization [12].

DOLOS is a novel architecture in the realm of network security. Its approach to restructuring the way MTD operates. The authors show that the integration of MTD is not only more effective than side-by-side deployment, but DOLOS is a reflection that it can be securely and seamlessly done so [13].

III. DECEPTIVE TECHNOLOGIES

A. *What Are Deceptive Technologies*

Deceptive technologies were originally designed to be relatively basic techniques to combat attacks on networks. The early implementation of honeypots for instance, were very basic systems with low levels of interaction that could only simulate certain portions of a network. Initially, sufficient for the early days of computing, honeypots have evolved to become more capable in today's more network integrated world. Honeypots can now be interacted with on very granular levels while being able to present itself as an operating system in its entirety, thus increasing the probability that an attacker will interact with the honeypot [4].

Moving Target Defense (MTD) is a more dynamic approach to implementing deceptive technologies in a network. MTD relies on the alteration of various aspects of a network to force the attacker to spend more resources and time to hit their intended target. With the utilization of Machine Learning, more modern MTD can modify and obfuscate network identifiers and addresses much more efficiently and regularly [3].

B. *Artificial Intelligence and Machine Learning*

Machine Learning (ML) is a capable tool that can be used for the analytics of data sets [5]. The data can then be used to train models which can be used in the improvement of techniques in network security.

Artificial Intelligence (AI) and ML may not inherently be a deceptive technology, however it has the potential to be adopted for deceptive security use cases. Currently, researchers are looking into finding ways to integrate ML to better understand attacker behavior and AI to come up with more appropriate solutions. Such an example is using AI as the engine to drive end user facing chatbots to create and manage honeypots more optimally than the traditional honeypot interface [7].

C. *Honeypots*

Honeypots have been used in protecting networks through luring and trapping a malicious actors by presenting themselves as though they were the intended target of the malicious actor. Such a technique has been used to deceive malicious actors into thinking that they are attacking a real system, when in reality they have been engaging with a honeypot [14]. Defensive network teams can then either contain the attacker in the honeypot to prevent it from accessing other segments of the network or better understand the attacker's techniques through further study and observation [15].

The Internet of Things (IoT) has become more integral to the operations of various industries given its potential value to organizations through automation and data generation. IoT devices however, vary significantly on their intended use, vendors, and firmware; as such if a malicious actor wanted to attack an IoT network, it would need to check various factors on a target client to determine how best to attack it in its pre-check attack phase. A honeypot therefore needs to be interactive enough to appear as though it were the device it was trying to mimic, otherwise the attacker will notice the lack of interaction coming from the device and would avoid the honeypot. IoT networks are highly dependent on interactive honeypots in order to effectively deceive and counter IoT malicious actor. The utilization of ML concepts to better understand how to interact with malicious actors optimally and independent of human intervention is proving to be a viable solution for IoT network security [8]. The optimization of honeypots on an IoT network is even more important given the limitations of IoT devices in their hardware [16].

Modern methods of deceptive technologies include the utilization of ML whereby Generative Pre Trained Models (GPT) is fed with data from honeypots in order to create more efficient honeypots which can then be integrated into a network's defense system. ML can also be integrated with a network's Security Information and Event Management (SIEM) to provide analysis on more dynamic log topics such as content that is generated by human beings. Such new data can be a useful tool for network security teams to run analytics on in order to better understand what is legitimate traffic and what can be potentially flagged as malicious activity [4].

D. *Moving Target Defense*

MTDs are techniques in deception technology by making the job of a malicious actor much more difficult through the constant amount of uncertainty that they project onto an attacker. Certain use cases include the mutation of network addresses and other identifiable details about a device on a network. This forces an attacker to expend more time and resources in their attempt to attack a network. MTDs have proven to be very effective when defending against Advanced Persistent Threats (APT). Those in charge of network security must consider the value that MTDs have to offer in hardening the security of a network and determine if the increase in security is worth the tradeoff in network performance [11].

The value that MTDs can provide through their ability to constantly obfuscate and reconfiguring important aspects of a network must be balanced with the costs to the network's efficiency. The implementation of MTDs can result in the delay in the delivery of network packets and even result to packets being lost entirely. The optimization of one's network is dependent upon the design of a network and the potential attack scenarios that are the most likely to occur, network security teams should adjust their MTDs accordingly [12].

Currently, studies are being made on the potential to develop new architecture for integrating MTDs in systems instead of being deployed alongside them through a new architecture called DOLOS. The integration of DOLOS into systems would impede the efforts of malicious attackers as it would be more difficult for attackers to bypass an MTD that was integrated into a system instead of being implemented in isolated deployments alongside them [13].

IV. CONCLUSION

Deceptive technologies have been a consistent technique in defending networks against attacks since the early days of networking. Their utilization has proven to be effective but the advancement of computing and networking technologies necessitates more innovative techniques to implement such solutions to better defend networks [11].

The increasing amount of data that organizations store in cyberspace has incentivized cybercrime and malicious actors to try and gain unauthorized access to a network [2]. As such, various forms of deceptive technologies have come into use to further strengthen the defense of a network [4].

Honeypots and MTDs have been techniques in deceptive technologies that have been in use since. As attackers become more sophisticated with their methods so have network defenses. Not only have honeypots and MTDs been refined to be more indiscernible and efficient from the systems that they try to mimic, their potential value to network security can greatly be increased through the utilization of GPT models and AI [11].

Novel techniques and the integration of advancements from other fields in computer science, such as generative AI, have been studied to understand their potential in the strengthening of a network's security. The integration of AI and ML into Honeypots and ML can serve as extensions to deceptive technologies thus adding AI and ML as a possible new form of deceptive technology. As such, further research is being done to find ways to integrate AI and ML into network security to optimize network defense and resource allocation [7].

Researchers also recommend that honeypots need to be developed to become more dynamic, which can be facilitated with AI to not only become more efficient in being deployed across networks [7] but also to develop insightful analysis to better understand attackers [4].

V. REFERENCES

[1] N. Meghanathan, S. Reddy Allam, and L. A. Moore, "Tools and Techniques for Network Forensics."

[2] L. Elluri, V. Mandalapu, P. Vyas, and N. Roy, "Advances in Cybercrime Prediction: A Survey of Machine, Deep, Transfer, and Adaptive Learning Techniques," Apr. 2023., in press.

[3] A. Rashid and J. Such, "Effectiveness of Moving Target Defenses for Adversarial Attacks in ML-based Malware Detection," Feb. 2023. , in press.

[4] F. Setianto, E. Tsani, F. Sadiq, G. Domalis, D. Tsakalidis, and P. Kostakos, "GPT-2C," Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 2021., in press.

[5] A. Desai, "Machine Learning for Economics Research: When what and how?," *SSRN Electronic Journal*, Apr. 2023., in press.

[6] A. H. Celdran, P. M. Sanchez Sanchez, J. von der Assen, T. Schenk, G. Bovet, G. M. Perez, and B. Stiller, "RL and Fingerprinting to Select Moving Target Defense Mechanisms for Zero-day Attacks in IoT," Dec. 2022., in press.

[7] F. McKee and D. Noever, "Chatbots in a Honeypot World," Jan. 2023., in press.

[8] V. S. Mfogo, A. Zemkoho, L. Njilla, M. Nkenlifack, and C. Kamhoua, "AIIPot: Adaptive Intelligent-Interaction Honeypot for IoT Devices," Mar. 2023., in press.

[9] M. Nawrocki, J. Kristoff, R. Hiesgen, C. Kanich, T. C. Schmidt, and M. Wahlisch, "SoK: A Data-driven View on Methods to Detect Reflective Amplification DDoS Attacks Using Honeypots," Feb. 2023., in press.

[10] J. von der Assen, A. Huertas Celdran, P. M. Sanchez Sanchez, J. Cedeno, G. Bovet, G. Martinez Perez, and B. Stiller, "A Lightweight Moving Target Defense Framework for Multi-purpose Malware Affecting IoT Devices," Oct. 2022., in press.

[11] D. Reti, D. Fraunholz, K. Elzer, D. Schneider, and H. D. Schotten, "Evaluating deception and moving target defense with network attack simulation," *Proceedings of the 9th ACM Workshop on Moving Target Defense*, 2022.

[12] D. Ergenc, F. Schneider, P. Kling, and M. Fischer, "Moving Target Defense for Service-oriented Mission-critical Networks," Mar. 2023., in press.

[13] G. Pagnotta, F. de Gaspari, D. Hitaj, M. Andreolini, M. Colajanni, and L. V. Mancini, "DOLOS: A Novel Architecture for Moving Target Defense," Mar. 2023., in press

[14] L. Huang and Q. Zhu, "Adaptive honeypot engagement through reinforcement learning of semi-markov decision processes," *Lecture Notes in Computer Science*, pp. 196–216, 2019.

[15] B. Cates, A. Kulkarni, and S. Sreedharan, "Planning for Attacker Entrapment in Adversarial Settings," Apr. 2023.

[16] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2351–2383, 2021.