Early Detection of Cyber Attacks Using Decoy Systems – Analysis of Deception-Based Cyber Security Strategies

Mădălina Spiridon, Lenuța Alboaie, Dragoș Gavriluț

Abstract

Deception technology is a modern security solution that provides specific actions against malicious activities and is a relevant component for a complete approach to cyber security. The methodology behind this solution involves the creation and deployment of decoy assets, easy to configure and highly attractive, encouraging attackers to engage with them. The dynamic aspect of continuously producing and updating these decoy assets has been a major discovery point in this field.

Keywords: deception, security, innovation, engage, dynamic.

1 Introduction

Ransomware and info stealers continue to affect a growing number of victims, demanding significant ransom payments to restore compromised data and pledging not to release sensitive data on the dark web [1]. Although these threats are not a new concern, attackers have adapted their techniques to circumvent current security solutions [2]. In response to these persistent malware threats, it has become essential to develop a proactive and efficient strategy capable of detecting and responding to attacks almost in real-time. The scope of deception technology is the protection against ransomware attacks and info stealers, being an useful technique to have in place once a suspected event

©2024 by Mădălina Spiridon, Lenuța Alboaie, Dragoș Gavriluț

has happened. Additionally, these technologies slow down an attack by increasing the computation time for file encryption.

2 Deceptive Technologies

Deceptive technologies, such as those patented for detecting unauthorized access, often involve traps that mimic real network resources and deploy decoy drivers to attract attackers [3]. Notable examples include FortiDeceptor's AI-driven honeypots for isolating attacks [4], Fidelis's deception mechanisms to expose attacker tactics [5], and Acalvio's ShadowPlex system, which deploys various decoys across digital assets [6].

Decoy technologies serve as an advanced defense layer against cyber threats like ransomware and data theft. Decoy system use deceptive artifacts, which are fake assets mimicking real ones, to lure attackers, and any interaction with these monitored decoys signals potential malicious activity. The decoy module integrates with broader security ecosystems, enhancing protection by working alongside existing security solutions such as SIEM[1] and endpoint protection platforms.

3 New Insights in Decoy Systems

In this paper, we are proposing a module that incorporates methods to collect indicators of compromise, ensuring that when malicious activity is detected, the content of the compromised file is preserved. This allows it to be safely detonated later in a completely isolated environment, where it can be analyzed in depth to discover the adversary's tactics and to better understand the attack kill-chain. To highlight the capabilities of the decoy module, a series of tests were performed using ransomware and info stealer samples with different scenarios such as: commands and key-exchanges from a C2 server, code injection mechanisms, which use memory stores or which involved integration with

[1] Security Information and Event Management

Telegram bots for publishing and selling stolen data. Additionally, tests were conducted using ransomware specialized in identity theft aimed at stealing banking information and browser data. During tests involving

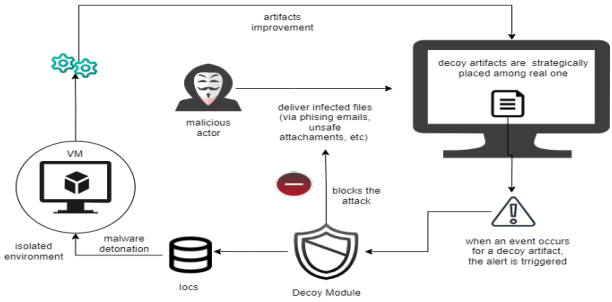


Figure 1. Architecture

ransomware and info stealer samples, the module demonstrated its effectiveness both in terms of detection speed, with an average detection time (the duration it takes for the system to identify a potential threat or suspicious activity) of 2-3 seconds, and the time it took to block the attack, ensuring that no real files were affected, only decoy artifacts. During the tests, no false positives have been observed.

	non decoy files	**encr non decoy files**	**decoy files**	**encr decoy files**
#1	13	0	9	2
#2	13	3	18	9

Table 1. Testing Results

The decoy module aligns with market protection standards and adheres to the techniques and tactics prescribed by the MITRE [7] organization while also incorporating innovative components.

4 Conclusions

In this period when attackers are gaining more and more ground and are developing using advanced techniques, the implementation and use of an integrated solution with deceptive technologies is an additional protection measure. The decoy technology will have a considerable impact in improving defense and is expected to gain popularity in the market due to its beneficial contributions in terms of early detection of cybercriminals. The role it plays in improving security can be major because it can easily detect the newest types of ransomware and maintain protection against sophisticated attacks.

References

[1] ReliaQuest Threat Research Team. *Ransomware and Cyber Extortion in Q2 2024.*

[2] T. McIntosh, T. Susnjak, et.al. *Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration.* 2024.

[3] Topspin Security. *System and a method for identifying the presence of malware and ransomware using mini-traps set at network endpoints.* 2016, pp. 6–8.

[4] J. Oltsik. *Active Defense and Deception Technology: The Time is Now!* 2023.

[5] Fidelis Security. *Fidelis Deception- Turn Adversaries into Targets.* 2023.

[6] Acalvio. *ShadowPlex Advanced Threat Defense.* 2024.

[7] https://www.mitre.org/news-insights/impact-story/mitre-engage-framework-and-community-cyber-deception.

Mădălina Spiridon[1], Lenuța Alboaie[2], Dragoș Gavriluț[3]

[1]Alexandru Ioan Cuza University: Iasi, RO, Bitdefender Labs
E-mail: mspiridon@bitdefender.com
ORCID: https://orcid.org/0009-0006-1799-5800

[2]Alexandru Ioan Cuza University: Iasi, RO
E–mail: lalboaie@gmail.com
ORCID: https://orcid.org/0000-0003-0969-8102

[3]Alexandru Ioan Cuza University: Iasi, RO, Bitdefender Labs
E–mail: dgavrilut@bitdefender.com
ORCID: https://orcid.org/0009-0004-3339-9625