IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, March 2025
Impact Factor: 7.67

Honey Tokens using API – A Survey

Ms. Dhanashree Wadnere, Rahul N. Shelar, Siddhant R. Lokare
Department of Computer Science & Engg.
Sandip University, Nashik, India

Abstract: The tutorial "Creating a Honeypot Token" on GitGuardians' blog provides step-by-step instructions for setting up honeypot tokens to improve security. Honeypot tokens serve as bait for recognition of unauthorized access and potential threats. By implementing Honeypot tokens, organizations can identify attack patterns, respond effectively to threats, and improve general security centers. This aggressive approach helps protect sensitive information and understand the behavior of malicious actors.

Keywords: Honeypot, GitGardian, Honey Tokens

I. INTRODUCTION

In today's rapidly developing digital landscape, cybersecurity remains a critical issue for organizations of all sizes. As c yber threats become more severe and ubiquitous, traditional security measures are no longer sufficient to protect sensiti ve information and critical systems. To stay ahead of malicious players and protect valuable assets, you need a proactiv e and innovative approach. Such an approach is an implementation of Honeypot Tokens, a technology designed to reco gnize unauthorized access and malicious activity by creating attractive Potters for potential attackers. A Honeypot token is a false registration information or token that appears to be valuable to an attacker but does not meet the actual purpos e. If these tokens are accessed or used, they trigger warnings to allow businesses to identify and respond to potential sec urity violations.

This tutorial begins with an implementation of the requirements, including a basic understanding of programming and s ecurity concepts, as well as access to gitguardian for managing and monitoring honeypots to biscuits. This tutorial cove rs the step-by-

step process of generating tokens, configuring GitGuardian for monitoring, providing tokens in the codebase, and conti nuous monitoring of alerts.

The important steps covered in the tutorial include:

1. Creating Tokens: Create appearance tokens that mimic legitimate login or sensitive information and are attractive tar gets for attackers.
2. Configuring gitguardian: Sets Gitguardian for repository monitoring and detection of exposure or honeypot token usa ge.
3. Token Provided: Strategically insert honeypot tokens into your codebase. B. Configuration files or surrounding varia bles to maximize visibility of potential attackers.
4. Monitoring and Response: We considered that Gitguardian warning monitoring and access were not certified, identifi ed potential threats and took appropriate security measures.

The tutorial shows the benefits of honeypot tokens, including the ability to recognize unparalleled access in controlling attack patterns, the overall security of an organization. Implementing Honeypot tokens allows businesses to actively ide ntify weaknesses and respond effectively to threats that enhance their defense against cyberattacks.

II. CHARACTERSTICS

1. Deception and Attractive

Purpose: Honeypot Tokens are designed to look valuable and legal to potential attackers. It mimics actual login or sensi tive information and creates attractive goals for attempts that are not permitted to access.

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, March 2025
Impact Factor: 7.67

2. Monitoring and Alarms
Function: After provisioning, honeypot tokens are continuously monitored by security tools such as Gitguardian. If the t oken is accessed or used, it triggers a notification to prevent the company from recognizing and investigating authorized activities.

3. Strategic Placement
Provided by: Honeypot tokens are strategically placed in codebases, configuration files, or environment variables. This strategic placement increases the likelihood that malicious actors tokens will be discovered and accessed.

4. Aggressive Security Measurement
rolle: The honeypot token acts as a proactive security measure. They help businesses identify potential weaknesses, und erstand attack patterns, and respond to threats before escalating.

5. Not working
nature: The honeypot token is not working. This means that it does not provide real access to sensitive systems or data. Instead, they are designed for recognition and surveillance purposes only.

6. Incentive Data Collection
Advantages: By recording unauthorized access attempts, honeypots provide valuable insight into the behaviors and tech niques used by attackers. This information can be used to improve general security strategies and defenses.

7. Easy Integration
Implementation: Honeypot tokens can be easily integrated into your existing safety infrastructure. Tools such as Gitgua rdian simplify the process of producing, delivering and monitoring these tokens, allowing organizations to access acqui sitions of this security practice.
These properties make honeypot tokens an effective device for improving cybersecurity and improving early warning o f potential threats. By implementing it, companies can strengthen their immune systems and better understand the threat landscape.

III. LITERATURE REVIEW

Honeypot tokens are relatively new, but more important instruments in cybersecurity. They are designed to act as bait, a ttract attackers and provide valuable information about how and what they do. The concept of honeypots has been inves tigated and developed in great detail over the years. The latest research focused on applications in a variety of fields.

1. The evolution of honeypots:
Early research on honeypots focuses on the basic function of a deck bird to attract attackers and monitor their activity. The study highlighted the importance of honeypots for cyber threat detection and analysis, providing insight into attack patterns and technology.

2. Honeypot Types:
There were a variety of honeypots, including honeypots with low interactions that simulate services and protocols, and honeypots with high interactions that allow the attacker to provide the real system for interaction. Recent advances have introduced tougher honeypots developed for IoT devices and health systems.

3. Honeypot-Token:
Honeypot-Token is a specific type of honeypot that mimics valuable login or sensitive information. They are strategically placed in the system to attract attackers and trigger warnings during access. Research shows that honeypot tokens are effective in identifying unauthorized attempts to access and identifying early warnings of potential threats.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, March 2025
Impact Factor: 7.67

4. Benefits and Challenges:
The main advantage of hoopot-
token is its ability to recognize and analyze attacks in real time and provide valuable data to improve security measures. However, the challenges include the need for continuous surveillance and the possibility that attackers can identify and avoid honeypots.

5. Future trends:
¢ Future research on honeypot tokens will likely focus on improving its effectiveness and reducing implementation cost s. Advances in machine learning and artificial intelligence can also play a role in improving the detection and response capabilities of honeypot tokens. By providing valuable insight into early detection of attacks and attacker behavior, they contribute to a more robust and proactive security strategy.

IV. RESEARCH GAP

Based on the current research environment, we will find the research gaps identified in the honeypot area. Dex is suscep tible to fake tokens and fraudulent traps.

1. Legal and Ethical Questions:
There is a lack of widespread guidelines regarding the legal and ethical implications of honeypot token use. In this area, further research is needed to set clear standards.

2. Integration with Advanced Technology:
There is continuous research into the integration of honeypot tokens with machine learning and AI, but there is still roo m for improving detection and response functions using these technologies.

3. Cost-effective regulations:
Improved honeypot configuration and threat accuracy to reduce maintenance costs develop threat detection. Finding ch eap solutions remains a challenge.

4. Transforming honeypot detection by attackers:
Research is needed on the development of methods to counter attackers that can identify and avoid honey.

V. CONCLUSION

Implementing Hoonypot tokens is a strategic and proactive approach to improving cybersecurity. By providing these de ception tokens, businesses can effectively recognize fraudulent attempts to access and collect valuable insights into atta cker behavior. Honeypot tokens act as an early warning system that allows for a timely response to potential threats and supports the identification of vulnerabilities within the safety infrastructure. They provide real data on attack patterns, c ontribute to more robust security centers, allowing businesses to stay ahead of new threats. Future advances in technolo gies such as machine learning and artificial intelligence are expected to further improve the effectiveness and integratio n of honeypot tokens. This makes it a crucial part of your modern cybersecurity strategy.

REFERENCES

1. https://blog.gitguardian.com/creating-a-honeypot-token-tutorial/
The main tutorial on which this is based on.
2. **Fortinet - Honey Tokens: What are they and How are they used?**
This article provides an overview of honey tokens, their differences from honeypots, and examples of their use. It explains how honey tokens can be used to track attackers and gather information about their methods.
3. **CrowdStrike - What are Honeytokens?**

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, March 2025
Impact Factor: 7.67

This resource explains the fundamentals of honeytokens, their role in cybersecurity, and best practices for implementing them. It also discusses the differences between honeytokens and honeypots.

4. **Honeypot.is API Reference**

This documentation provides information on how to use the Honeypot API to integrate honeypot checks into products. It covers authentication, supported chains and exchanges, and various API endpoints.