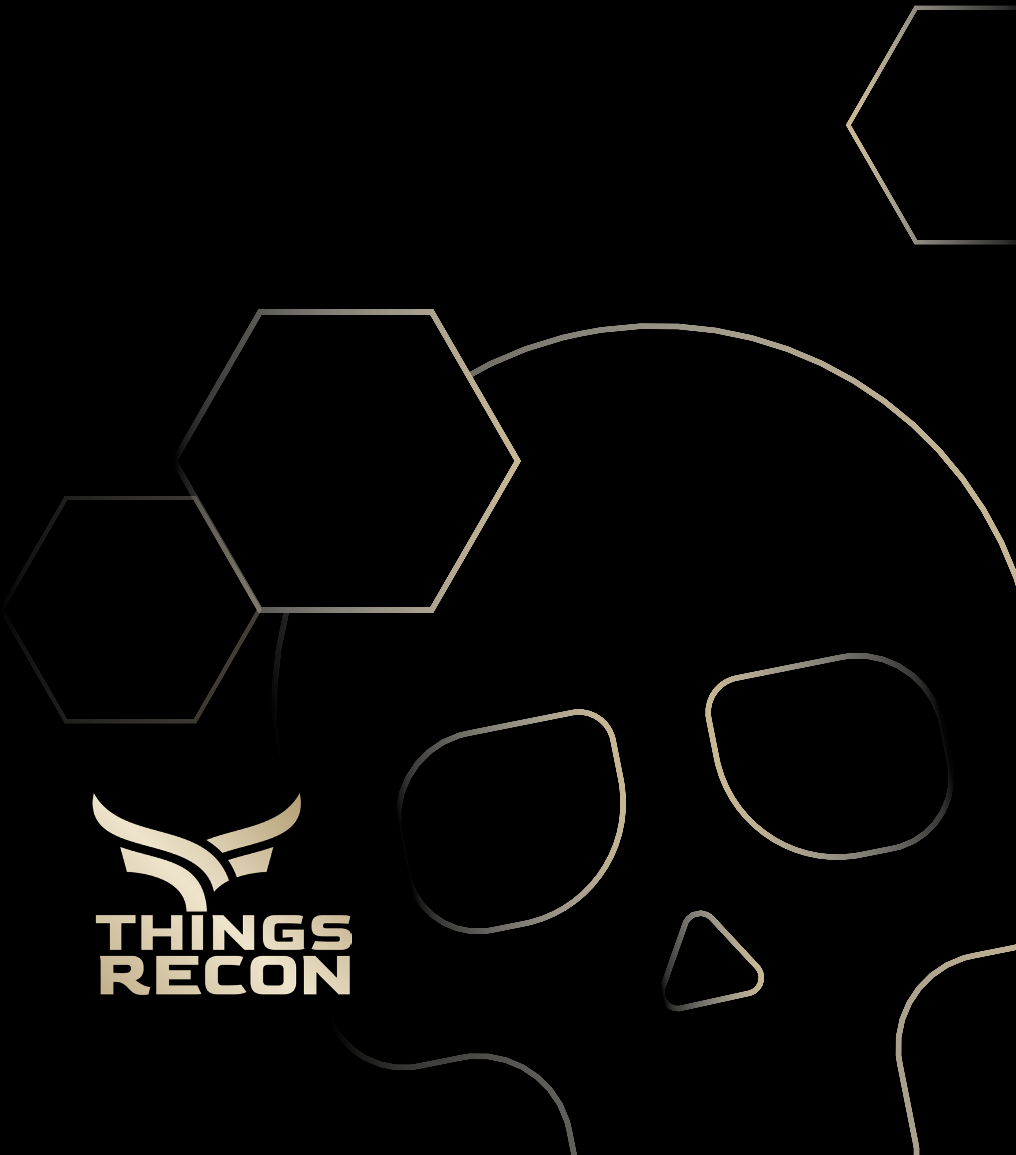
The Dark World of Shadow and Zombie APIs



THINGS
RECON

Introduction

As the Halloween season casts its shadow upon us, it's the perfect time to investigate the world of APIs (Application Programming Interfaces). These digital connectors serve as the building blocks of modern software and connect the digital world, powering everything from apps on our smartphones to complex cloud-based systems. However, not all APIs are what they seem. In this article, we explore the mysterious and often misunderstood world of Shadow and Zombie APIs, shedding light on these hidden entities that lurk in the digital shadows.

Defining Shadow and Zombie APIs

Before plunging deeper, it's essential to understand the distinction between Shadow and Zombie APIs :

- Shadow APIs : Shadow APIs, also known as Hidden APIs, are application interfaces that exist outside the knowledge and control of an organization's IT and security teams. These APIs are often undocumented and can pose a significant security risk, as they are not subject to regular security assessments or governance.

- Zombie APIs : Zombie APIs are APIs that are no longer in use or officially supported but still exist within a system's infrastructure. These undead APIs can be forgotten, overlooked, or simply left behind during software updates or migrations. Despite being inactive, Zombie APIs may contain vulnerabilities that attackers can exploit.

The Perils of Shadow APIs :

Shadow APIs can be a breeding ground for various security and compliance risks :

1. Unauthorized Data Access : They can provide a backdoor for unauthorized parties to access sensitive data, circumventing established security protocols.
2. Compliance Violations : Shadow APIs often escape the watchful eye of compliance regulations, potentially leading to non-compliance issues, data breaches, and legal consequences.
3. Data Leaks : As they lack proper security oversight, Shadow APIs can inadvertently expose sensitive information, leading to data leaks and breaches.
4. Hidden Attack Vectors : Attackers can exploit undocumented APIs to launch attacks that go unnoticed by security measures.

The Risks of Zombie APIs :

Even though Zombie APIs are inactive, they are not entirely harmless :

1. Security Vulnerabilities : Zombie APIs may contain vulnerabilities that were left unresolved before their retirement, which attackers can exploit.
2. Resource Drain : They can consume server resources even when unused, impacting system performance.
3. Confusion and Errors : Developers and administrators may inadvertently interact with Zombie APIs, leading to confusion and potential errors in system operations.

Techniques to discover Shadow and Zombie APIs

1. Passive Reconnaissance
   - Passive DNS monitoring
   - Passive HTTP Data Collection
2. API Fingerprinting
   - Analyse responses
   - Analyse error message
3. Web Application Scanning
4. Penetration Testing
5. Threat Intel Feeds
6. Leverage OSINT

Defending Against Shadow and Zombie APIs:

1. Inventory and Documentation : Establish a comprehensive inventory of all APIs, including Shadow and Zombie APIs. Proper documentation is key to understanding their presence.
2. Regular Audits : Conduct regular security audits to identify Shadow APIs, assess their risks, and either secure or eliminate them.
3. Secure Retirement : When APIs become Zombie APIs, ensure that they are securely retired, and any potential security vulnerabilities are addressed before they are decommissioned.
4. API Management Platforms : Implement API management platforms that offer governance and visibility into API usage, ensuring better control over API ecosystems.
5. Educate Teams : Train IT and development teams to recognize the risks associated with Shadow and Zombie APIs and the importance of proper documentation.

How EASM can Help

1. Comprehensive Asset Discovery: EASM solutions employ extensive scanning and monitoring capabilities to unveil both documented and undocumented APIs, making it easier to identify Zombie and Shadow APIs within an organization’s digital infrastructure.
2. Continuous Monitoring: EASM solutions provide continuous visibility into an organization’s digital footprint, ensuring that even inactive APIs, such as Zombie APIs, are promptly detected when they resurface, thus preventing potential security vulnerabilities.
3. Data Correlation: By correlating data from various sources, including passive reconnaissance and traffic analysis, EASM solutions can piece together the puzzle of APIs, identifying anomalies and discrepancies that may indicate the presence of Shadow APIs.
4. Security Assessments: EASM tools can conduct security assessments on APIs, allowing organizations to not only discover Zombie and Shadow APIs but also assess their potential security risks and take the necessary steps to secure or decommission them.

Conclusion

In conclusion, Shadow and Zombie APIs may lurk in the dark corners of an organization's digital infrastructure, posing significant risks. Understanding and addressing these hidden entities is crucial to maintaining a secure and compliant digital environment. By shedding light on these hidden APIs, organizations can bolster their security measures and reduce the chances of falling victim to data breaches and vulnerabilities that often go unnoticed.

THINGS RECON

thingsrecon.com