wib. | Use Case

Shadow & Zombie APIs

Smart energy IoT manufacturer

Shadow and Zombie APIs refer to APIs that are not officially supported or documented by an organization but still exist within the API estate. These APIs can be created by third party developers or by in-house teams and can be used to access sensitive data or perform actions that are not intended to be publicly available.

Organizations must be aware of the existence of Shadow and Zombie APIs and implement measures to identify, monitor and secure them to prevent potential security breaches. This starts with having visibility on what they are and where they sit, and should include regular audits and reviews, enforcing access controls and monitoring usage patterns to detect any unauthorized access and potential exploits.

What is a shadow API?

Shadow APIs refer to APIs that are used within an organization but are not officially supported, tracked, or documented. These APIs are still active but may not have gone through the same level of security, quality and performance testing as officially supported APIs, and as a result pose a risk to the stability and security of the systems that use them.

Shadow APIs are needed and often used by developers to quickly get access to specific data or functionality. They are not a risk in themselves but become a vulnerability if not properly managed and maintained and can be easily exploited by attackers.

Zombie APIs

Zombie APIs are APIs that were once in use but are no longer active and therefore not maintained or supported. They may still be present in the codebase and may continue to be used by some systems but are essentially 'dead, meaning they are no longer being updated, improved, or secured.

Typically, zombie APIs arise when multiple versions of the same API are in use i.e. older versions are still 'connected' even though they have been superseded by newer versions. It is essential to identify and retire any Zombie APIs within the API ecosystem to ensure your organization's security hygiene once those have been investigated and identified as redundant.

Case example: smart energy IoT manufacturer

Wib's attack research team were challenged to evaluate the API security of a smart energy IoT manufacturer.

Objective

We were issued with details of known APIs and user credentials for testing purposes. This process uncovered several vulnerabilities for the organization to address.

We also dedicated a branch of our testing on scanning the APIs and application infrastructure using multiple word lists and other fuzzing tools. Through this we discovered several undocumented, shadow APIs.

What we found

During the test we discovered **multiple Shadow APIs**. One of these APIs – externally exposed – allowed us to send internal emails to all company employees. This is a particularly dangerous exploit which would potentially enable an attacker to bypass all security defences by virtue of using an internal rather than an external email as the attack vector.

We demonstrated to the organization how this position could be used to send a general phishing email to spread malware among employees, or to launch a specific spear-phishing attack spoofing an email from the company COO to the finance department requesting a money transfer.

As well as discovering the shadow APIs, we were able to show the business impact of shutting them down.

In another instance we discovered **multiple Zombie APIs.** Four out of the five discovered were a different version of the same API which were simply not shut down, unnecessarily exposing the business vulnerability.

By removing those the organization has **reduced their attack surface by** **80%**

Simply by having the right visibility and actioning the right security protocol.

How to minimise the risk

By discovering Shadow and Zombie APIs and retiring them at the right time, organizations can reduce the attack surface and decrease the potential security risks associated with them.

Similarly by discarding multiple Zombie APIs, organizations can reduce the attack surface and lower the risk of security vulnerabilities, eliminating outdated and unmaintained APIs.

Document all APIs regularly and through the full API lifecycle.

Create and implement an update/change process for APIs and their documentation.

Constantly review API code and traffic to identify unnecessary APIs or endpoints and remove them.

Proper API management and maintenance will help your organization shrink your attack surface significantly and protect your sensitive data.

The Wib holistic approach

Wib advanced API Security Platform ('Fusion Platform') is comprehensive, holistic solution for securing APIs across an organization's entire ecosystem. It utilizes a comprehensive, multi-lens approach, powered by Wib's proprietary Fusion Engine – to assess the security posture of APIs, minimize risk, and quickly address cybersecurity incidents throughout the entire development process. From code to testing and production – further enabling incident response and vulnerability management via Wib Fusion Defense.

It focuses on three engines – code analysis, traffic inspection and attack simulation – provide advanced perspectives to better gain a holistic view of each organization's unique API gaps and flaws.

The code analysis engine maps all endpoints, APIs, patterns, and designs in the code by connecting to the API repositories and inventories.
At this point, we can identify the APIs we expect to see. The engine will identify any endpoints unable to properly validate the authentication tokens.

The traffic inspection engine harnesses the code analysis data to verify and compare. This avoids false positives and can identify where mitigation controls may be in place if there is no authentication enforcement. It also enables other potentially hidden APIs to be inspected for similar defects

The attack simulation engine allows us to 'red team' various attacks against the endpoints and APIs. A human dimension is critical here as there is no automated tool capable of exploiting business logic. Some attacks are used to eliminate false positive feedback.

Through this approach, Wib's Fusion Platform is uniquely equipped to optimize defence against API logic attacks and effective detection of potential blind spots where traditional rule base detection will fail.

Secure. Liberate. Innovate.

API Penetration Testing as a Service (PTaaS)

APIs expose more attack surface than User Interfaces, but most penetration testing lacks rigorous testing of APIs by experienced offensive API attackers.

Our industry-first API penetration testing service is a quick and simple way to ensure visibility, protection, and compliance by providing full pen testing capabilities or augmenting your existing pen testing solution with our API-specific security expertise.

What you get:

- **Full risk and vulnerability assessment of your critical APIs (can include black, grey, or white box testing)**
- **A risk severity score based on NIST cyber matrix calculator**
- **Contextual remediation report for all identified vulnerabilities**
- **Consultancy and remediation roadmap plan with Wib's security team experts**

Testing tailored to PCI DSS 4.0, GDPR, CCPA, SOC-2, ISO, NIST 800-30, HIPAA, CMA and other regulatory Frameworks